HERZOG, Felix. "Straftaten im Internet, Computerkriminalität und die Cybercrime Convention". *Polít. crim.*, Vol. 4, Nº 8 (Diciembre 2009), Doc. 1, pp. 475-484 (1-10). [http://www.politicacriminal.cl/Vol_04/n_08/Vol4N8D1.pdf]

Straftaten im Internet, Computerkriminalität und die Cybercrime Convention[1]

Professor Dr. Felix Herzog, Universität Bremen
felix.herzog@uni-bremen.de

In den folgenden Ausführungen möchte ich zunächst eine phänomenologische Definition dessen geben, was man unter Computerkriminalität und Straftaten im Internet verstehen kann. In einem zweiten Schritt werde ich diese Kriminalitätsformen zu den Regelungen der europäischen Cybercrime Convention[2] in Beziehung setzen.

Sodann gehe ich der Frage nach, ob sich Computerkriminalität und Straftaten im Internet in den Tatbegehungsstrukturen und der Struktur der Täterpopulation wesentlich von der bislang bekannten Kriminalität unterscheidet. Weiter wird es um die Frage gehen, ob die Struktur des „Tatortes" Internet und Computerwelt besondere Formen der Ermittlungen notwendig macht.

Abschließend werde ich die beiden Themen Prävention und Selbstregulierung behandeln.

1. Phänomene der Computerkriminalität und Kriminalität im Internet

Unter Computerkriminalität versteht man im weitesten Sinne die Begehung von Straftaten unter Einsatz von elektronischer Datenverarbeitung, häufig an einem diffusen Tatort, den ich hier der Einfachheit halber einmal „Computerwelt" nennen möchte. Bei den entsprechenden Taten handelt es sich beispielsweise um Fälle des Computerbetrugs, der Computersabotage und der Softwarepiraterie. [3] Bei diesen Delikten wird der Computer als Tatmittel eingesetzt und ist auch das Medium, mit dem die Früchte der Taten geerntet und weiter verarbeitet werden können. Als spezifische computerbezogene Begehungsweisen von Betrug gehören in den Bereich dieser Delikte auch der Missbrauch elektronischer Plattformen wie z.B. Online-Banking, ebay oder andere Handelsplattformen zu vielerlei Varianten üblicher Täuschungs- und Schädigungsstrategien.[4]

Straftaten im Internet unter der Nutzung von Computertechnologie finden darüber hinaus in der Weise statt, dass das Kommunikationsmedium zur Verabredung zu Straftaten, zur Organisation von Beihilfetaten und allgemein als eine logistische Struktur genutzt wird. Dies gilt für Taten aus dem Bereich der organisierten Kriminalität (wie Rauschgifthandel, illegaler Waffenhandel, Geldwäsche etc.) ebenso wie für alle möglichen Spielarten des politisch oder religiös motivierten Terrorismus.[5]

Die Erfahrungen der letzten Jahre zeigen weiterhin, dass das Medium des Internets zur Anbahnung von Kontakten genutzt wird, die in der Gesellschaft als moralisch fragwürdig oder gar kriminell gelten – so etwa zur Verabredung zu abweichenden Sexualpraktiken, zur Kontaktaufnahme mit

1 Este Trabajo ha sido realizado dentro del marco Proyecto Fondecyt N° 1060410 titulado "Los nuevos desafíos que las nuevas estructuras sociales imponen al Derecho Penal", que dirige el prof. Dr. Raúl Carnevali y tiene su base en la ponencia presentada en el Segundo Seminario Política Criminal: "Nuevas tecnologías y desafíos actuales del Derecho Penal", en noviembre de 2007.

2 Convention on cybercrime, CETS No. 185, 23.11.2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Stand: 21.12.2008)

3 Vgl. Bär, Wolfgang, Strafrecht in der digitalen Welt, Beitrag zur BKA-Herbsttagung in Wiesbaden, 20.-22.11.2007, http://www.bka.de

4 Vgl. Bär, a.a.O.

5 Griesbaum, Rainer, Probleme bei der Bekämpfung, Beitrag zur BKA-Herbsttagung in Wiesbaden, 20.-22.11.2007, http://www.bka.de

Kindern mit dem Ziel ihres sexuellen Missbrauchs[6] oder zur Bildung von Kommunikationszusammenhängen (Foren und Chats) zwischen Personen, die beispielsweise an Satanismus oder Kannibalismus interessiert sind.[7]

Schließlich sind Straftaten im Internet der Natur des Mediums gemäß Kommunikationsdelikte, die beispielsweise Pornografie, Gewaltverherrlichung, Aufforderungen zur Diskriminierung, Werbung für extremistische und terroristische Aktivitäten und jede Art von Hate-Speech umfassen.[8]

2. Einige Details der gerade genannten Phänomene

Im Folgenden möchte ich auf einige der Phänomene näher eingehen und einen Bezug zu den Regelungen der so genannten Cybercrime Convention herstellen. Dabei handelt es sich um ein auf Initiative des Europarates zurück gehendes Abkommen im Kampf gegen die Computer- und Internetkriminalität, das neben Instrumenten zur Koordinierung der internationalen Zusammenarbeit einen Normkatalog enthält, der bestimmte Formen von Cybercrime zu systematisieren versucht. Mittlerweile sind der Cybercrime Convention 46 Staaten beigetreten, außerhalb Europas gehören hierzu Japan, die USA, Kanada und Südafrika.[9] Allerdings hat bisher nur die Hälfte der Unterzeichner das Abkommen auch ratifiziert.

Nach den Vorgaben der Cybercrime Convention sind im Bereich des materiellen Strafrechts folgende Taten zu kriminalisieren und mit besonderer Aufmerksamkeit zu verfolgen:

2.1. „Hacking“ und der Schutz der „Integrität informationstechnischer Systeme“

Nach Art. 2 der Konvention haben die Vertragsparteien alle vorsätzlichen Formen des unrechtmäßigen Zugriffs auf Computersysteme unter Strafe zu stellen. Die damit angezielten Verhaltensweisen befinden sich häufig im Vorfeld weiterer Rechtsgüterverletzungen. Die Konventionsstaaten sind der Meinung, dass es angesichts der damit verbundenen Gefahren erforderlich ist, bereits das bloße Eindringen in Computersysteme („Hacking“) zu kriminalisieren, da es einerseits bereits eine Verletzung der Rechtssphäre der rechtmäßigen Nutzer darstelle und andererseits mit „Hacking“ auch ein massives Gefährdungspotenzial für weitere Rechtsgüter verbunden sei, das eine Vorfeldkriminalisierung rechtfertige. In Deutschland wurde diese Anforderung durch das im August 2007 in Kraft getretene 41. Strafrechtsänderungsgesetz umgesetzt und der sog. „virtuelle Hausfriedensbruch“ durch den § 202 a StGB als strafbare Handlung definiert. Unter den Tatbestand fällt jede konkrete Gefährdung der Vertraulichkeit von Daten, die bereits dann gegeben ist, wenn der Täter durch seine Handlung die Möglichkeit eröffnet hat, auf Daten zuzugreifen.[10]

Das Universalrechtsgut von Art. 2 der Cybercrime Convention wäre damit als „Integrität von Computersystemen“ zu beschreiben und würde einen bunten Strauß von Individualrechtsgütern von einer Art „Hausrecht“ am eigenen Computersystem bis hin zu einem erweiterten Eigentumsschutz enthalten.

6 Bliesener, Thomas, Die digitale Welt und ihre Opfer, Beitrag zur BKA-Herbsttagung in Wiesbaden, 20.-22.11.2007, http://www.bka.de

7 Bliesener, a.a.O.

8 Vassilaki, Irini E., Kriminalität im World Wide Web – Erscheinungsformen der „Post-Computerkriminalität“ der zweiten Generation, MMR 2006, 212

9 http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=12/14/2008&CL=ENG (stand: 21.12.2008)

10 Vgl. Bär, a.a.O.; Gröseling, Nadine, Höfinger, Frank Michael, Hacking und Computerspionage – Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, 549, 551

Das deutsche Bundesverfassungsgericht hat jüngst im Zusammenhang mit der Frage nach den Voraussetzungen für eine (heimliche) Zugriffsbefugnis staatlicher Ermittlungsbehörden auf private Computer („Online-Durchsuchung") aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art.1 Abs. 1 GG) ein Grundrecht „auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" abgeleitet.[11] Der Sammelbegriff „informationstechnische Systeme" wird von dem Verfassungsgericht durch Beispiele konkretisiert. Umfasst sind das Internet insgesamt, Rechnersysteme, Personalcomputer, andere Telekommunikationsgeräte wie z. B. Mobiltelefone, elektronische Geräte in Wohnungen wie z.B. Steuerungsanlagen der Haustechnik, elektronische Geräte in Kraftfahrzeugen und elektronische Terminkalender.

2.2. „Abfangen von Daten"

Art. 3 der Cybercrime Convention stellt unter dem Titel „Rechtswidriges Abfangen" das mit technischen Mitteln bewirkte Abfangen nicht öffentlicher Computerdatenübertragungen einschließlich elektromagnetischer Abstrahlungen unter Strafe. Dieses Delikt ist durch die rasante Verbreitung von Wireless Lan in den Fokus der Aufmerksamkeit gerückt. Auch hier handelt es sich – wie beim Hacking – um eine Vorfeldkriminalisierung, da man aus kriminalistischer Erfahrung weiß, dass das Abfangen von Computerdaten häufig die Vorstufe von weiteren Integritätsverletzungen von Computersystemen und für vermögensbezogene Taten im Netz bildet.[12]

2.3. „Datenmanipulation"

In Art. 4 der Konvention geht es um den Eingriff in Daten. Die Vertragsparteien verpflichten sich in diesem Artikel der Konvention, das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten unter Strafe zu stellen. Mit dieser Regelung wird der klassische Tatbestand der Sachbeschädigung an die Erfordernisse des modernen Lebens angepasst – das Ziel der Regelung ist es, Computerdaten ähnlich wie bewegliche Sachen umfassend gegen Beeinträchtigungen zu schützen. Nach den beiden Vorfelddelikten des Eindringens in Computersysteme und des Abfangens von Daten ist man mit diesem Deliktsbereich bei klassischen strafrechtlichen Verletzungsdelikten angelangt.[13]

2.4. „Systemeingriffe"

Ähnlich verhält es sich bei der Regelung des Art. 5 Cybercrime Convention, die unter dem Titel „Eingriff in ein System" die schwere Behinderung der Funktion eines Computersystems durch Eingeben, Übertragen, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten unter Strafe stellt. Es handelt sich insofern um eine Klarstellung, dass unter den Bedingungen des modernen Lebens Eingriffe in das Eigentum nicht mehr an die Beeinträchtigung von Gegenständen gebunden sind. Natürlich ist das Zertrümmern oder Verbrennen von Hardware schon immer strafbar; nichts anderes kann für vergleichbare Angriffe auf die Software gelten.

2.5. Missbrauch von Tools

Einen etwas unklaren Status hat die Regelung des Art. 6 Cybercrime Convention, der den Vertragsparteien aufgibt, den „Missbrauch von Vorrichtungen" zur Sicherung von Computersystemen unter Strafe zu stellen. Im Internet kursieren unzählige Programme, die es ermöglichen, bestimmte Strukturen der Systemsicherheit zu umgehen, zu verändern oder ganz lahm

11 1 BvR 370/07, 1 BvR 595/07; http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
12 Vgl. Bär, a.a.O.
13 Vgl. Gercke, Marco, Analyse des Umsetzungsbedarfs der Cybercrime Konvention – Teil 1: Umsetzung im Bereich des materiellen Strafrechts, MMR 2004, 728

zu legen. Ihr Einsatz soll den Tatbestand des Missbrauchs von Vorkehrungen erfüllen, was bedeutet, dass Art. 6 der Sache nach ein strafrechtliches Verbot der Herstellung von Software, die für kriminelle Zwecke genutzt werden könnte, bedeutet. Eine Kriminalisierung in diesem Bereich wurde in Deutschland im Kontext des neuen Straftatbestands § 202 c StGB, welcher den Gedanken des Art. 6 umsetzt, scharf kritisiert. Der Einsatz entsprechender Programme sei dringend erforderlich, um digitale Systeme sicherer zu machen, indem sie zum Finden von Schwachstellen genutzt werden. Dafür sei der Besitz von sog. „Hacker-tools“, ihre Weiterentwicklung sowie die Möglichkeit eines öffentlichen fachlichen Austauschs über Stärken und Schwächen unabdingbar. Eine Kriminalisierung gefährde die Sicherheit von Computersystemen.[14] Zudem gebe es zahlreiche Programme, die nach ihrer objektiven Zweckbestimmung sowohl für kriminelle als auch für legale Zwecke eingesetzt werden können („Dual-use“). Um einer über das (verfassungsgemäße) Ziel hinaus schießenden Pönalisierung entgegenzuwirken, bleibt nur die enge Auslegung der Tatbestandsmerkmale, vor allem in Bezug auf den Schwerpunkt der Zweckbestimmung eines Programms.[15] Grundsätzlich stellt sich aber auch hier die Frage, wie weit man die Vorfeldkriminalisierung im Interesse der Sicherheit im Internet und der Integrität von Computersystemen ziehen möchte. Diese kritische Frage hat deswegen ein besonderes Gewicht, da die vorgelagerte Strafbarkeit an Delikte geknüpft wird, deren Schutzgüter nicht von höchstem Rang sind.[16]

2.6. „Fraud“

Die Regelungen der Art. 7 und 8 der Cybercrime Convention sind dagegen kriminalpolitisch unbedenklich, da sie letztlich alt bekannte Delikte auf die Bedingungen der modernen Kommunikationsmedien umsetzen.

In Art. 7 unter dem Titel „Computergestützte Fälschungen“ geht es der Sache nach darum, dass mit Täuschungsabsicht vorgenommene Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten, das dann zu manipulierten Datenverarbeitungsergebnissen führt, unter Strafe zu stellen. Es handelt sich also um eine Art modernen Tatbestand der Urkundenfälschung.

Bei Art. 8 unter dem Titel „Computergestützter Betrug“ ist schon durch den Titel klar, dass es um moderne Begehungsformen des klassischen Delikts geht: Die Vertragsparteien haben gemäß Art. 8 die in betrügerischer oder unredlicher Absicht der Bereicherung erfolgende Beschädigung des Vermögens eines anderen durch Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten oder Eingriffe in die Funktionsweise eines Computersystems unter Strafe zu stellen. Dieses Delikt der Datenmanipulation ist das Pendant zum klassischen Delikt der betrügerischen Kommunikationsmanipulation unter Menschen in der Absicht, sich Vermögensvorteile zu verschaffen.

2.7. Verbreitung von Kinderpornographie

Art. 9 der Cybercrime Convention greift das Problem der flutwellenartigen Verbreitung von Kinderpornografie über das Internet auf. Die umfassende Kriminalisierung soll einerseits verdeutlichen, dass es der Respekt vor der Würde von Kindern verbietet, eine unkontrollierte Verbreitung derartiger Materialien zu dulden, andererseits liegt der Kriminalisierung die Annahme zu Grunde, dass ein ungebändigter Austausch von kinderpornografischem Bildmaterial dazu

14 Vgl. Stellungnahmen des Chaos Computer Clubs v. 25.9.2006, http://www.ccc.de/press/releases/2006/20060925/ und v. 15.7.2008, http://www.ccc.de/202c/202cStellungnahme.pdf?language=de

15 Gröseling, Nadine, Höfinger, Frank Michael, Computersabotage und Vorfeldkriminalisierung – Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, 626, 628 f.

16 Gröseling/Höfingera.a.O., 628

beiträgt, den realen sexuellen Missbrauch von Kindern zu unterstützen oder zu erleichtern.[17]

2.9. Illegale downloads

In Art. 10 der Cybercrime Convention geht es schließlich um die allgegenwärtigen Verletzungen des geistigen Eigentums und von Urheberrechten durch Downloads im Internet. Hier trifft die Konvention keine kategorische Regelung; vielmehr legt sie den Vertragsparteien nur auf, solche Verstöße zu kriminalisieren, die einen gewerbsmäßigen Umfang annehmen.

2.10. Hate speech im Internet

Ein Zusatzprotokoll zur Cybercrime Convention „On the criminalisation of acts of racist or xenophobic nature through computernetworks"[18] wurde von zahlreichen Vertragsparteien angestrebt, stieß aber bei anderen Vertragsparteien im Hinblick auf die dortigen Regelungen und Traditionen zur Meinungsfreiheit auf Widerstand. Das Zusatzprotokoll wurde schließlich von 34 Staaten unterzeichnet.[19] Auch wenn der Text der Cybercrime Convention selbst vor dem geschilderten Hintergrund keine entsprechenden Regelungen enthält, ist darauf hinzuweisen, dass durch einen Rahmenbeschluss der Europäischen Union[20] aus dem Jahr 2008 jedenfalls alle Mitgliedsstaaten der Europäischen Union dazu verpflichtet sind, die Verbreitung von rassistischer und neonazistischer Hate-Speech im Internet strafrechtlich zu verfolgen. Der Rahmenbeschluss sieht vor, dass jede öffentliche Aufstachelung zu Gewalt und Hass gegen Menschen anderer Rasse, Hautfarbe, Religion oder nationaler wie auch ethnischer Abstammung unter Strafe gestellt werden muss. Eingeschlossen ist auch die Anstiftung oder Beihilfe zu einer solchen Handlung.

2.11. Missbrauch von Handelsplattformen und Phishing

Außerhalb der Regelungen der Cybercrime Convention bildet der Missbrauch elektronischer Handelsplattformen im Internet einen relevanten, rasant steigenden Anteil an der Computerkriminalität. In Europa und den Vereinigten Staaten nimmt die Zahl der Menschen stetig zu, die online Waren und Dienstleistungen kaufen. Natürlich versuchen auch Kriminelle, dieses Wachstum zu ihren Gunsten zu missbrauchen, indem sie auf Internetplattformen betrügerisch tätig werden. So werden Opfer ganz klassisch betrogen, indem sie zu Zahlungen veranlasst werden und die entsprechenden Waren oder Dienstleistungen nicht erhalten. Die elektronischen Plattformen dienen aber auch als Marktplätze, über die Produktfälschungen angeboten werden. Und Opfer werden in dubiose Geschäftsbeziehungen verstrickt – wie z.B. Partnerschaftsagenturen –, deren Kosten rasch einen ruinösen Umfang annehmen.

In diesen Zusammenhang gehört auch die missbräuchliche Nutzung von Kommunikationsweisen des Internets, wie z.B. der E-Mail oder der Kontaktformulare („Phishing"). Eine Variante des Phishings ist das Versenden von E-Mail- oder Chatnachrichten unter Vortäuschung eines vertrauenswürdigen Urhebers. Der Internetnutzer wird so dazu veranlasst, sensible persönliche

17 Ludvigsen, Björn-Erik, Kinderpornografie im Internet (Kurzfassung), Beitrag zur BKA-Herbsttagung in Wiesbaden, 20.-22.11.2007, http://www.bka.de

18 Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, CETS No.: 189, 28.1.2003, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=12/23/2008&CL=ENG

19 http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=12/23/2008&CL=ENG (stand: 21.12.2008)

20 2008/913/JI, 28. November 2008, Rahmenbeschluss zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit, http://eurocrim.jura.uni-tuebingen.de/cms/de/doc/1045.pdf **(**Stand**:** 21.12.2008**)**

Daten wie z. B. Passwörter für die Nutzung von Online-Banking oder ebay preiszugeben. In diesem Zusammenhang werden auch ganze Internetpräsenzen z. B. von Banken kopiert. Gibt ein Nutzer auf einer derart gefälschten Seite seine login-Daten ein, werden diese gespeichert und können dann für kriminelle Handlungen weiterverwendet werden. Diese Form des Phishing ist die Übertragung der Vorgehensweise von klassischen Trickbetrügern auf die Kommunikationswege der virtuellen Welt. Der sog. „Enkeltrick“ - das Vertrauen von alten Menschen wird an der Haustür oder via Telefon unter Vorspiegelung falscher Tatsachen gewonnen und diese werden schließlich bestohlen – funktioniert nach dem selben Grundprinzip.

Eine zweite, effizientere Variante des Phishing bedient sich hingegen bestimmter Hilfssoftware (Viren, Trojaner). Diese werden zwischen den Internetnutzer und beispielsweise seine Bank geschaltet und die persönlichen Informationen werden so abgefangen. Neben Banken sind auch Bezahlsysteme (z. B. Paypal), Online-Auktionshäuser, Versandhäuser, Online-Beratungen und Single-Börsen beliebtes Ziel der Daten-Fischer. Mit den erlangten Daten bzw. virtuellen Identitäten werden beachtliche Vermögens- und Rufschäden angerichtet.[21]

Die Frage der Strafbarkeit des Phishing ist umstritten – insbesondere in Bezug auf den ersten Schritt des Versendens einschlägiger, d.h. zur Preisgabe von Daten lockender E-Mails. Im deutschen Strafrecht scheitert hier eine Strafbarkeit wegen Betruges an einer kausal bewirkten Vermögensverfügung – das bloßes Versenden einer Phishing-Mail ist an eine solche nicht unmittelbar gebunden, zumal auch später eben gerade nicht der Kontoinhaber selbst Geld abhebt. Auch die §§ 263 a Abs. 3 StGB (Computerbetrug) und 202 a StGB (Ausspähen von Daten) scheitern auf der Tatbestandsebene.[22] Eine Strafbarkeit kommt allein nach § 269 StGB (Urkundenfälschung) in Betracht. Dies setzt voraus, dass die Übersendung der E-Mail eine Fälschung beweiserheblicher Daten darstellt. Dabei kommt es im Einzelfall darauf an, ob die Verbindlichkeit der Mail auch ohne digitale Signatur einem Schreiben mit Unterschrift entsprach.[23]

3. Neue Qualität der Computer-/Internet-Kriminalität?

Die Kriminalität der Computerwelt und im Internet erzeugt schon auf den ersten Blick deswegen ein besonderes Bedrohungsgefühl, da sie keinen klaren Tatort aufweist, die Täter nicht sichtbar sind und es häufig schwer fällt, die Tathandlungen rechtzeitig oder überhaupt zu erkennen. Die (empfundene) Gefährlichkeit dieser Kriminalität ergibt sich also zunächst einmal aus ihrer Ubiquität, zum anderen aus ihrer Anonymität und weiterhin aus ihrer Diffusität. Hinzu tritt, dass eine Häufung von Vorfällen oder jedenfalls die durch die Medien verbreitete Nachrichtenlage den Eindruck entstehen lässt, dass man in der Computerwelt und im Internet nirgendwo sicher und demzufolge immer massiv bedroht ist.[24]

Im Internet können zahlreiche Rechtsgüter verletzt bzw. gefährdet werden: Die Sicherheit und die Zuverlässigkeit des Rechtsverkehrs, das Vermögen, der persönliche Geheimnisbereich, die sexuelle Selbstbestimmung, die Pietät gegenüber Toten, die Ehre und der öffentliche Friede. Damit betrifft Kriminalität im Internet letztlich alle gesellschaftlichen Bereiche und auch alle Menschen als Individuen, soweit sie sich im Internet bewegen – was in der Informationsgesellschaft kaum mehr zu vermeiden ist. Es fällt also sehr schwer, der Gefahr, Kriminalitätsopfer zu werden, auszuweichen – es ist unmöglich, das Internet wie eine „schlechte Gegend“ zu meiden. Die Abhängigkeit des persönlichen und wirtschaftlichen Lebens von Computern und dem Internet löst zudem etwa

21 http://de.wikipedia.org/wiki/Phishing (Stand: 21.12.2008)
22 Vgl. Bär, a.a.O.
23 Vgl. Bär, a.a.O., AG Euskirchen, Urt. v. 19.6.06 (Az. 5 Ds 279/05), LG Bonn, Urt. v. 13.10.2006 (Az. 36 B 24/06); Ernst, Stefan, Das neue Computerstrafrecht, NJW 2007, 2661, 2665
24 Schäuble, Wolfgang, Eröffnungsansprache zur BKA-Herbsttagung, 20.-22.11.2007, http://www.bka.de

hinsichtlich von Computersabotage die berechtigte Befürchtung aus, mit mächtigen Instrumenten könnten dort schnell und aus dem „Hinterhalt" ungeahnte Schäden angerichtet werden.[25]

Als Hintergrund der ubiquitären Gefahr, Opfer von Straftaten im Internet und im Zusammenhang mit Computern zu werden, lässt sich feststellen, dass es sich um eine Form von Massenkriminalität handelt, so dass eine auf bestimmte soziale Gruppen fokussierte Präventionspolitik aussichtslos erscheint. Als „Hacker" versuchen sich schon Kinder, „Virusschreiber" gibt es im Bereich der organisierten Kriminalität, aber auch unter intellektuellen Computerfreaks; Kinderpornografie findet quer durch alle Bevölkerungsschichten Interesse; Betrügereien in Europa können von Asien, Afrika oder Lateinamerika aus gesteuert werden, z.T. konkurrieren russische Tätergruppen mit solchen aus dem asiatischen Raum usw.

Die Internationalität und Ubiquität der Straftaten im Internet stellt eine Verbindung zu den verfahrensrechtlichen Besonderheiten her. Die Täter der Internetkriminalität sind häufig gar nicht im klassischen Sinne zu verorten oder befinden sich irgendwo in „rechtsfreien Räumen". So ist häufig unklar, wer wo eigentlich Ermittlungsmaßnahmen durchführen, wer wen auf welcher Rechtsgrundlage wohin ausliefern oder wo eine tatortbezogene Bestrafung von Internetkriminalität stattfinden könnte. Dem Strafrecht kommt bei der Bekämpfung der Internetkriminalität gewissermaßen der nationale und territoriale Bezugsrahmen abhanden und damit auch die Basis für die Durchsetzung eines staatlichen Strafanspruchs gegenüber entsprechenden Tätern.

4. Besondere Herausforderungen für die Strafverfolgung?

Aus der Sicht der staatlichen Strafverfolgungsbehörden ergeben sich mit der Entwicklung der Computerkriminalität neue Herausforderungen bei der Verfolgung von Cybercrime. Dies beginnt schon mit der enormen Geschwindigkeit, mit der Daten über das Internet ausgetauscht werden können, der enormen Flut von Verbindungsdaten, die dabei anfallen und effektiven Anonymisierungs- und Verschlüsselungsdiensten, welche die Verfolgung erschweren. Die für die Ermittlung von Tätern notwendigen Daten sind für die Strafverfolgungsbehörden meist nur für kurze Zeit und schwer zugänglich.

Am 1. Januar 2008 ist in Deutschland ein Gesetz über die sog. Vorratsdatenspeicherung in Kraft getreten. Demnach werden über einen Zeitraum von sechs Monaten sämtliche E-Mail- und Telekommunikationsverbindungsdaten aller Bürger gespeichert. Für die Verfolgung bestimmter Katalogtaten können diese dann durch die Strafverfolgungsbehörden abgefragt werden. Diese neue Befugnis der Ermittler sei inzwischen unverzichtbar zur Aufklärung von Straftaten im Bereich des internationalen Terrorismus und der organisierten Kriminalität, heißt es in der Begründung des Regierungsentwurfs.[26] Kritiker sehen in der Gesetzesreform einen unverhältnismäßig schwerwiegenden Eingriff in die Privatsphäre und bezweifeln die Effektivität der riesigen Datensammlung. Die Speicherung von Verbindungsdaten sei in Bezug auf die Eingriffsintensität auch nicht schwächer als die Erfassung von Kommunikationsinhalten, da durch die Erstellung von Kontakt- und Bewegungsprofilen weit reichende Informationen über die überwachte Person erlangt werden könnten.[27] Derzeit ist die Herausgabebefugnis der gespeicherten Daten wegen einer einstweiligen Anordnung des Bundesverfassungsgerichts eingeschränkt. Grund ist eine noch nicht

25 Vgl. Bär, a.a.O.

26 Begründung des Entwurfs eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG v. 27.4.2007, S. 31, http://dip21.bundestag.de/dip21/btd/16/058/1605846.pdf

27 Vgl. http://www.vorratsdatenspeicherung.de/ mit zahlreichen weiteren Verweisen

entschiedene Verfassungsbeschwerde von über 34.000 Beschwerdeführern.[28] Auch wenn der Ruf der Strafverfolgungsbehörden nach zeitgemäßen Ermittlungsinstrumenten nachvollziehbar ist, stellt sich die Frage, ob es sich tatsächlich nur um eine Modernisierung des strafprozessualen Repertoires handelt oder um eine Erweiterung auf digitaler Ebene. Eine präventive Speicherung aller Absender und Adressaten von Briefen wäre wohl das analoge Pendant zur Vorratsdatenspeicherung.

In diesen Zusammenhang gehört auch eine Debatte darüber, ob Voraussetzungen für die Durchsuchung von Computersystemen mit Online-Instrumenten geschaffen werden sollten. Die normale Durchsuchung und Beschlagnahme von Räumen und den dort stehenden Computern macht in vielen Kriminalitätsbereichen überhaupt keinen Sinn, weil die Standorte der Hardware nicht bekannt sind und verdächtige Daten fortlaufend gelöscht werden. Dies hat unter Strafverfolgern zu der Forderung geführt, es müsse möglich sein, mit den auch von der Kriminalität genutzten Mitteln wie Hacking und Trojanern in Computersysteme und auf Datenträger vorzudringen, um in den Besitz von Beweismitteln zu gelangen. In diesem Zusammenhang stellen sich erhebliche Probleme des Datenschutzes und des Schutzes der Kommunikationsfreiheit. In der Bundesrepublik bezieht sich die Diskussion unter dem Stichwort „Online-Durchsuchung“ auf den Einsatz solcher Mittel zum Zwecke der polizeirechtlichen Gefahrenabwehr und im Strafverfahren. Auf der Ebene des Polizeirechts war zunächst das Nordrhein-Westfälische Verfassungsschutzgesetz, das als erstes eine Online-Durchsuchung vorsah, vor dem Bundesverfassungsgericht gescheitert. Viren und Trojaner der Polizeibehörden würden in das an dieser Stelle neu entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreifen. Ein solcher Grundrechtseingriff sei zwar grundsätzlich rechtfertigbar, die Grenzen müssten jedoch eng gezogen werden. Es bedarf tatsächlicher Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut wie Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Zudem muss die Online-Durchsuchung unter einem Richtervorbehalt stehen und Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung enthalten.[29] Unter Berücksichtigung der verfassungsgerichtlichen Vorgaben wurde nun im Dezember 2008 das BKA-Gesetz reformiert. Die Novelle enthält unter anderem die Ermächtigung zur Online-Durchsuchung.

Auf der Ebene der strafprozessualen Zwangsmittel hat der Bundesgerichtshof am 31.1.2007[30] festgestellt, dass die „Online-Datenabfrage“ nicht unter die Bestimmungen über die traditionelle Durchsuchung subsumiert werden könne, da sie sich wegen ihrer Heimlichkeit grundlegend davon unterscheide. Auch eine Anwendung der Bestimmungen über Eingriffe in die Telekommunikation komme nicht in Frage, da es gerade darum gehe, Daten, die der Beschuldigte auf dritten Rechnern gespeichert hat, unabhängig von seinen Zugriffen zu erlangen. Um die Online-Durchsuchung in das Instrumentarium der Strafverfolgungsbehörden zu integrieren bräuchte es in der Bundesrepublik eine Gesetzesänderung. Die Praxis ruft danach.[31]

Neben den grundsätzlichen Fragen nach den Voraussetzungen für die Zulässigkeit von Online-Durchsuchungen ergibt sich ein weiteres Problem, sobald die zu durchsuchenden Computer sich im Ausland befinden und ein Zugriff eine Verletzung der Souveränität des Standortstaates bedeuten kann. Hier bedarf es Regelungen über grenzüberschreitende Ermittlungen. In den Art. 29 ff. der Cybercrime Convention finden sich Normen dieser Art. Es geht dort vor allem darum, jenseits der langwierigen Rechtshilfeverfahren einen pragmatischeren Zugang zu Daten im Hoheitsgebiet eines anderen Staates zu ermöglichen, wenn der Verfügungsberechtigte zustimmt (Art. 32 Ziff. b). Für

28 http://verfassungsbeschwerde.vorratsdatenspeicherung.de/ (Stand: 21.12.2008)

29 BVerfG, Urt. v. 27.2.2008, 1 BvR 370/07, 1 BvR 595/0, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

30 BGH NJW 2007, 930

31 Bär, a.a.O.

Fälle, in denen eine solche Zustimmung nicht vorliegt, wird die Möglichkeit einer vorläufigen Sicherung normiert.[32] Das Problem der in der Konvention vorgesehenen Instrumente ist, dass nur eine weltweite Anwendung der Möglichkeit Vorschub leisten könnte, Daten außerhalb ihres Geltungsbereichs zu speichern.

Wann immer es dann vielleicht durch Nutzung solcher problematischer Ermittlungsmethoden dazu kommen sollte, dass Täter und ihrer Standorte identifiziert werden können, werden sich komplizierte Fragen der Rechtshilfe, der Auslieferung und des anzuwendenden Strafrechts daran knüpfen. Letztlich wird es notwendig sein, neben der Harmonisierung des materiellen Strafrechts auch zu einer Harmonisierung der Strafverfolgung und konsensualen Regelungen über den Ort der Durchführung von Strafverfahren zu kommen – ein Prozess der gegenwärtig jedenfalls in der Europäischen Union im Gange ist.[33]

Die gerade skizzierten Schwierigkeiten mit der Strafverfolgung sollten freilich überhaupt dazu Anlass geben, das Schwergewicht der Überlegungen und Initiativen nicht auf die Repression bereits vergangener Taten, sondern auf die Prävention zukünftiger Taten zu legen. Dies soll der Gegenstand meiner abschließenden Bemerkungen sein.

5. Technische Prävention als prima ratio, Strafrecht als ultima ratio der Verhinderung von Internetkriminalität

Angesichts der geschilderten Schwierigkeiten bei der Verfolgung von Computer- und Internetkriminalität und angesichts der Ubiquität und Massenhaftigkeit des Phänomens erscheint es klüger, nicht nur auf die Karte des Strafrechts zu setzen, um dieses Phänomen einzudämmen. Ohnehin steht die generalpräventive Wirkung des Strafrechts i.S. von Abschreckung sehr in Frage – was in diesem Bereich noch virulenter ist, weil es an einem klar definierten Adressatenkreis für die Strafdrohungen fehlt und die Entdeckungswahrscheinlichkeit relativ gering ist. Strafrecht könnte in diesem Bereich lediglich eine Funktion i. S. der positiven Generalprävention haben und bestimmte unverzichtbare Normen bekräftigen. Auch für diese Wirkung des Strafrechts muss man freilich einen definierten und erreichbaren Adressatenkreis voraussetzen, was aus den genannten Gründen keine Selbstverständlichkeit sein dürfte.

Betrachtet man die die Kerndelikte von Computerkriminalität wie Computersabotage und Computerbetrug, dann liegt es in der Natur der Sache dieser Delikte, dass der Ausbau technischer Maßnahmen im Sinne einer ständigen Innovation der Sicherheitstechnologien Angriffe dieser Art verringern, wenn nicht sogar in bestimmten Bereichen blockieren kann. Hier ist natürlich die Erfahrung zu berücksichtigen, dass der Einsatz von Filterungssystemen, Virus- oder Firewall-Software offenbar geradezu eine Herausforderung für Saboteure darstellt, immer neue Methoden zu entwickeln, um gleichwohl in Computersysteme eindringen zu können.

Trotz des dargelegten diffusen Bedrohungsgefühls angesichts der Kriminalität im Netz, erleichtert nach wie vor die Unvorsichtigkeit von Computerbenutzern und Internetsurfern Tätern das Eindringen in Computersysteme und daran geknüpfte Taten. Es ist deswegen statt Angstmache eine früh einsetzende und breit angelegte Sensibilisierung der Gesellschaft für die Risiken moderner Kommunikationstechnologie notwendig. Bereits in der Schule sollte eine Aufklärung über die Gefahren des Internets und die möglichen Strategien, sich zu schützen, erfolgen. Denkbar erscheint es auch, eine Art von Prüfung und Zertifikat, ähnlich dem Führerschein im Straßenverkehr, für die

32 Bär, a.a.O.
33 Hecker, Bernd, Europäisches Strafrecht, 2. Aufl., Berlin 2007, S. 15 f.

Nutzung des Internets zu verlangen.

In die Präventionsmaßnahmen ist neben den Nutzern auch die IT-Industrie einzubinden. Dies kann in der Weise geschehen, dass ein Wissenstransfer zwischen Strafverfolgungsbehörden und der IT-Industrie stattfindet, der es beiden Seiten ermöglicht, die richtigen Schlüsse aus neuen Phänomenen der Internetkriminalität sowohl in ermittlungstaktischer als auch in technopräventiver Richtung zu ziehen.[34]

Weiterhin erscheint in diesem Kontext der Einsatz von soft law und Selbstregulierungsmechanismen viel versprechend. Die „Community“ der Internetnutzer hat ganz überwiegend ein Interesse daran, dass das Medium gerade nicht für Kriminalität missbraucht wird. Es hat sich – etwa in der Verwaltung von Foren und Chatrooms – gezeigt, dass „Codes of Conduct“ und informelle Durchsetzungsmechanismen wie die Ermahnung von Normverletzern („blame them and shame them“) und deren Ausschluss von bestimmten Foren eine erhebliche Wirkung zeigen können. Die Benutzer des Internets reagieren sehr sensibel und sehr schnell auf bestimmte Formen des Missbrauchs des Mediums und sind in der Entwicklung von Abwehrstrategien außerordentlich kreativ, weil sie dabei nicht an feste Regeln der Sanktionierung und ein formalisiertes Verfahren gebunden sind. Natürlich bringt dies auch Gefahren mit sich, die man jedoch in einem Bereich der Internet-Bagatellkriminalität durchaus hinnehmen kann.

Statt nach mehr Polizei im Netz, nach unerbittlicher staatlicher Verfolgung und Bestrafung des Bösen im Netz zu rufen, sollten uns die dort anzutreffenden Phänomene ohnehin Anlass sein, über deren gesellschaftliche Entstehungsbedingungen nachzudenken und die Hoffnung nicht aufzugeben, dass soziale Kontrolle auch durch gesellschaftliche Aufklärung und Selbstregulation gelingen kann. Strafe muss sein, wo es um gravierende Rechtsgutsverletzungen im und durch das Medium des Internets geht. Die Normen, die wir für unser friedfertiges Zusammenleben als unverzichtbar ansehen, müssen auch hier behauptet und gesichert werden. Dies kann dazu beitragen, dass i. S. von positiver Generalprävention dafür gesorgt wird, dass die Nutzer des Internet einen inneren moralischen Kompass entwickeln und nicht unkontrolliert von den dunklen Seiten des Internet angezogen werden.

Über die Wirkungsweise strafrechtlicher Sozialkontrolle gibt es allerdings nur wenige verlässliche empirische Erkenntnisse. Als gesichert kann jedoch gelten, dass ein wesentlicher Faktor für eine solche sittenbildende Kraft des Strafrechts die Kontrolldichte und die Verfolgungsintensität ist. Dies ist eine wichtige Erkenntnis für die strategische Ausrichtung von Kontrolle im Internet, bedeutet aber zugleich eine Warnung: eine wirklich flächendeckende Kontrolle des Netzes und seiner Nutzer wird technisch nur schwer möglich sein und steht überdies in Gefahr, totalitäre Züge anzunehmen. Cyber-Policing an allen Ecken des Internets hätte einen hohen Preis für die Freiheit der Kommunikation.

In diesem Zusammenhang dürfen wir nicht vergessen, dass das Medium des Internets vielen Menschen die Möglichkeit der Bildung und Kommunikation überhaupt erst eröffnet hat und dass das Internet etwa auch eine wichtige Rolle in den Kampagnen für den Schutz von Menschenrechten spielt. Dass das Internet zugleich ein Ort ist, an dem das Böse, Schmutz und Gewalt wachsen und gedeihen, darf nicht dazu führen, dass eine populistische Kriminalpolitik betrieben wird und bei der Strafverfolgung „chinesische“ Methoden der Kontrolle verwendet werden.

Auch in diesem Bereich von Kriminalität gilt es, den Gegensatz von Sicherheit und Freiheit rational zu diskutieren und ausgewogene Lösungen des Rechtsgüterschutzes zu finden.

34 Vgl. Vassilaki, a.a.O., 216 f.