Prof. Dr. Dr. Eric Hilgendorf
Universität Würzburg

Kurze Stellungnahme zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (BT-Drucksache 16/3656 vom 30.11.2006) für die öffentliche Anhörung im Rechtsausschuss des Deutschen Bundestages am Mittwoch, dem 21. März 2007

I. Einleitung

Bis Mitte der 80er Jahre war die private Nutzung eines Computers noch eine seltene Ausnahme. Heute dagegen findet sich in fast jedem deutschen Privathaushalt mindestens ein Rechner. Gleichzeitig werden immer mehr Haushaltsgeräte mittels digitaler Technik betrieben. Die Nutzung des Internet zu privaten wie beruflichen Zwecken ist eine Alltäglichkeit geworden. Das Internet ist heute ein fast ebenso unverzichtbarer Bestandteil der öffentlichen Infrastruktur wie das Straßennetz. Ohne Übertreibung lässt sich daher von einer *umfassenden Digitalisierung* unserer Lebenswelt sprechen.

Mit dem Siegeszug der neuen Informations- und Kommunikationstechnologien sind auch neue sozialschädliche und kriminelle Verhaltensweisen auf den Plan getreten. Der deutsche Gesetzgeber hat früh reagiert und 1986 das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität erlassen. Die damals eingeführten Bestimmungen des Computerstrafrechts sind noch heute in Geltung. Auf europäischer Ebene wurden in den vergangenen Jahren neue Vorgaben für das Computer- und Internetstrafrecht entwickelt.[1] Die beiden wichtigsten sind das Übereinkommen des Europarats über Computerkriminalität vom 23.11.2001[2] und der Rahmenbeschluss des Rates vom 24.2.2005 über Angriffe auf Informationssysteme.[3]

Mit dem vorliegenden Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität sollen die Vorgaben der Cybercrime-Konvention und des Rahmen-

[1] Überblick bei E. Hilgendorf, Tendenzen und Probleme einer Harmonisierung des Internetstrafrechts auf Europäischer Ebene, in: Ch. Schwarzenegger, O. Arter und F.S. Jörg, Internet-Recht und Strafrecht, 4. Tagungsband 2004, 2005, S. 257 ff.

[2] ETS Nr. 185.

[3] Rahmenbeschluss 2005/222/JI, ABl. EU Nr. L 69 S. 67.

beschlusses in das deutsche Recht umgesetzt werden.[4] Der zu diesem Zweck von der Bundesregierung ausgearbeitete Entwurf ist in seinen Leitmotiven ebenso wie in den meisten Details trotz des großen Zeitdrucks, unter dem die Umsetzung stand, überzeugend. Besonders positiv hervorzuheben ist, dass der Entwurf mehrfach auf die Gefahren einer Überkriminalisierung aufmerksam macht und deshalb grundsätzlich einer engen Fassung der Straftatbestände den Vorzug gibt. Die Digitalisierung unseres Alltags ist so weit fortgeschritten, dass das computerspezifische Unrecht klar und trennscharf umschrieben werden muss, will man nicht Gefahr laufen, den Anwendungsbereich des Computer- und Internetstrafrechts inflationär auszudehnen.

II. Ausspähen von Daten, § 202a

§ 202a Abs. 1 soll folgende Fassung erhalten:

> „Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

Die Tathandlung soll nicht mehr darin bestehen, dass der Täter sich oder einem anderen Daten verschafft, sondern darin, dass er sich oder einem anderen Zugang zu Daten verschafft. Damit soll das einfache Hacken, also das Eindringen in ein fremdes Computersystem, strafrechtlich erfasst werden.

Diese Änderung ist grundsätzlich positiv zu bewerten. Die vielfältigen Probleme, die die alte Tathandlung der Datenverschaffung aufwarf,[5] fallen fort. Zu Recht hält der Entwurf an dem Erfordernis einer besonderen Sicherung fest. Damit wird ausgedrückt, dass nicht beliebige Daten durch § 202a geschützt werden, sondern nur solche, deren Schutzbedürftigkeit vom Berechtigten durch eine besondere Sicherung festgelegt wurde. Im Gegenschluss kann man festhalten, dass ungesicherte Daten nicht durch § 202a geschützt werden.

Überzeugend ist auch, dass die Tat lediglich dann strafbar sein soll, wenn sich der Täter den Zugang „unter Überwindung der Zugangssicherung" verschafft hat. Damit werden nur Fälle erfasst, in denen der Täter eine besondere kriminelle Energie an den Tag legt. Gleichzeitig kann Nachlässigkeit im Umgang mit den eigenen Daten dazu führen, dass der strafrechtliche Schutz entfällt, etwa wenn eine sehr leicht umgehbare Sicherung gewählt wurde. Da das

---

[4] Näher M. Gercke, Analyse des Umsetzungsbedarfs der Cybercrime-Konvention – Teil 1: Umsetzung im Bereich des materiellen Strafrechts, in: MMR 2004, S. 728 ff. Nur angemerkt sei, das die Umsetzung der auch in der Gesetzesbegründung (Bundestagsdrucksache 16/3665, S. 6) angesprochenen Europarats-Konvention zur Kinderpornographie zügig erfolgen sollte.

[5] E. Hilgendorf, Th. Frank, B.Valerius, Computer- und Internetstrafrecht, 2005, Rn. 683 ff.

Gesetz ausdrücklich von der Notwendigkeit einer „Überwindung“ der Zugangssicherung spricht, wird man, wie beim bisherigen § 202a auch, zu verlangen haben, dass es sich um eine nicht völlig belanglose, für jedermann ohne Weiteres zu überwindende Sicherung handelt.

Der Bundesrat hat in seiner Stellungnahme vom 3.11.2006 kritisiert, dass der Tatbestand zu weit geraten sei, da kaum noch elektronische Geräte ohne Datenspeicherung und Datenverarbeitung existierten. So könne sich nach dem Entwurf strafbar machen, wer sich unbefugt Zugang zu einem verschlossenen MP3-Player verschafft, um die abgespeicherte Musik anzuhören, oder wenn sich ein Jugendlicher heimlich ein Passwort für bestimmte TV-Sendungen besorgt, die ihm von den Eltern verboten wurden, und dann die Sendung anschaut.

Damit wird in der Tat ein problematischer Punkt angesprochen. Die Gegenäußerung der Bundesregierung, die fraglichen Fälle würden durch das Tatbestandsmerkmal der besonderen Zugangssicherung aus dem Anwendungsbereich des § 202a herausgefiltert, überzeugt nicht, da in beiden Fällen (Verschluss des MP3-Players, Passwort) besondere Zugangssicherungen existieren und durch die Handlungen des Täters überwunden werden. Das Problem stellt sich im Grundsatz schon bei § 202a a.F., ist dort aber weniger virulent, weil der Täter sich dort nicht bloß Zugang zu den Daten verschaffen musste, sondern die Daten selbst.

Das Problem rührt daher, dass der deutsche Gesetzgeber, aber auch die Verfasser der einschlägigen europäischen Vorgaben noch vom alten, im Wesentlichen in den 60er Jahren des vergangenen Jahrhunderts entstandenen Leitbild des „Hackens“ ausgingen. Damals war noch nicht daran zu denken, dass Rechnerfunktionen in fast alle Alltagsgeräte eingebaut werden würden. Der klassische „Hacker“ greift komplexe Computersysteme an, nicht MP3-Player, Fernseher oder hochgerüstete Bügeleisen.

Eine Lösung könnte sein, nicht eine beliebige Zugangsverschaffung ausreichen zu lassen, sondern nur solche Fälle zu erfassen, in denen der Täter sich den Zugang *zu einem Datenspeicher* verschafft. Dementsprechend ließe sich daran denken, § 202a Abs. 1 wie folgt zu fassen:

> „Wer unbefugt sich oder einem anderen Zugang zu *auf einem Datenträger gespeicherten oder an einen solchen übermittelten* Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.“

Durch die Einfügung des Merkmals „auf einem Datenträger gespeichert oder an einen solchen übermittelt“ würde der Gesetzgeber der Rechtsprechung die Möglichkeit geben, das

neue Leitbild des „Hackens“ und damit des § 202a schärfer herauszuarbeiten und die unerlaubte und unter Überwindung einer Zugangssicherung erfolgende Nutzung von Musikabspielgeräten, Fernsehern und anderen Alltagsgeräten mit Datenvermittlungsfunktion aus dem Tatbestand auszugrenzen. Leitgedanke könnte sein, nur solche Geräte mit Datenspeicherfunktionen als Tatobjekte des „Hackens“ zuzulassen, bei deren das Speichern von Daten ein wesentliches Element der Gesamtfunktionen des Gerätes ausmacht.

Dagegen spricht aber, dass die Abgrenzung zwischen Geräten, die spezifisch dem Speichern von Daten dienen, und solchen Geräten, bei denen das Speichern von Daten nur eine Nebenfunktion des Gerätes darstellt, nur schwer durchzuführen ist. In der Praxis kommt es mehr und mehr zu einer *Verschmelzung der Endgeräte*, so dass sich z.B. Fernseher (mit Datenspeicherung als Nebenfunktion) und Computer (mit Datenspeicherung als Hauptfunktion) bald nicht mehr klar trennen lassen. Ähnlichen Bedenken begegnet die Möglichkeit, nur die in einem Computer gespeicherten bzw. an einen solchen übermittelten Daten zu schützen.

Es spricht deshalb mehr dafür, das Gesetz wie vorgeschlagen zu beschließen und der Rechtsprechung (und Rechtswissenschaft) die Aufgabe zu übertragen, durch eine angemessene Interpretation der Norm (teleologische Reduktion) für eine Gesetzesanwendung zu sorgen, die dem Leitbild des „Hackens“ entspricht.

III. Abfangen von Daten, § 202b

§ 202b soll folgende Fassung erhalten:

> „Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.“

Der Auffangtatbestand dient dem Schutz des formellen Geheimhaltungsinteresses des Verfügungsberechtigten an „seinen“ Daten. Durch die Aufnahme des Merkmals „sich oder einem anderen Daten verschaffen“ werden die ungelösten Interpretationsschwierigkeiten dieser Handlungsumschreibung aus § 202a a.F.[6] in den neuen § 202b übertragen.

Das Verschaffen von Daten aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage kann nach dem Wortlaut der Norm auch Daten betreffen, die nicht gerade übermittelt werden, sondern bereits im System gespeichert sind. Die

---

[6] Vgl. oben Fn. 5.

Gesetzesbegründung ist insofern missverständlich[7] Die Weite des Gesetzeswortlauts ist zweckmäßig, um auch sog. „side-channel-Angriffe“ zu erfassen, bei denen sich der Täter die Daten nicht durch einen Eingriff in das System verschafft, sondern auf andere Weise (wie z.B. durch Aufzeichnung der elektromagnetischen Abstrahlung).[8]

Auffällig ist, dass der (deutsche wie europäische) Normgeber hier anders als bei § 202a auf das Erfordernis einer besonderen Zugangssicherung verzichtet. Der Grund hierfür ist nicht ganz klar. An den technischen Gegebenheiten allein kann es nicht gelegen haben. Nichtöffentliche Datenübermittlungen lassen sich z.B. durch Verschlüsselung sichern, elektromagnetische Abstrahlungen durch entsprechende technische Schutzvorrichtungen hemmen. Dem Gedanken der Selbstverantwortung für die eigenen Daten, der in § 202a n.F. einen überzeugenden Ausdruck gefunden hat, scheint § 202b auf den ersten Blick nicht gerecht zu werden, weil der leichtfertige Datenberechtigte genauso geschützt wird wie der vorsichtige. Man könnte deshalb daran denken, vor das Wort „verschafft“ die Formulierung „unter Überwindung einer besonderer Sicherung“ aufzunehmen.

Es erscheint allerdings fraglich, ob dies mit den europäischen Vorgaben noch vereinbar wäre. Außerdem sind Daten, die sich im Zustand der Übermittlung befinden, eher angreifbar als gespeicherte Daten, weshalb ein besonderer strafrechtlicher Schutz auch vom Berechtigten ungesichert gelassener Datenübermittlungen vertretbar erscheint. In vielen Fällen wird die Nutzung technischer Schutzmaßnahmen mit einem unzumutbaren Aufwand verbunden sein. Eine gewisse Einschränkung des Tatbestandes wird im Übrigen schon dadurch erreicht, dass nur die nichtöffentliche Übertragung von Daten, die nicht für den Täter bestimmt sind, vom geplanten § 202b erfasst wird. Dagegen dürfte das Tatbestandsmerkmal „unter Anwendung technischer Mittel“ funktionslos sein, denn ein Zugriff auf übermittelte Daten oder gar auf die elektromagnetische Abstrahlung einer Datenverarbeitungsanlage ist ohne Anwendung technischer Mittel nicht möglich.

IV. Vorbereiten des Ausspähens und Abfangens von Daten, § 202c

§ 202c soll folgende Fassung erhalten:

> „(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
>
> 1. Passworte oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
> 2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

---

[7] Vgl. BT-Drucksache 16/3656, S. 17, wonach gespeicherte Daten nicht Tatobjekt der Vorschrift sein sollen.

[8] Näher Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht (Fn. 5), Rn. 693.

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend."

Ziel der Neunormierung ist es, bestimmte besonders gefährliche Vorbereitungshandlungen im Bereich des Computerstrafrechts zu erfassen. Dass der Gesetzgeber von der Kriminalisierung des bloßen Besitzes abgesehen hat,[9] verdient Zustimmung.

§ 202c scheint mir zu weit geraten zu sein. Der objektive Tatbestand umschreibt keinen klaren Unrechtstypus, sondern erfasst z.B. auch die Tätigkeiten von Systemadministratoren (Herstellen bzw. Festlegung von Passwörtern und Sicherungscodes) sowie von Sicherheitsfirmen, die Software zum Testen der Schutzvorrichtungen von IT-Systemen entwickeln. Auch die Gesetzesformulierung „wer eine Straftat nach § 202a oder § 202b vorbereitet" ist sehr weit geraten, da unter „Vorbereitung" jede (u.U. auch weit entfernte) Hilfeleistung vor der Tat verstanden werden kann. Da für die Vorbereitung einer Straftat nach § 303a Abs. 1 oder § 303b Abs. 1 der § 202c entsprechend gelten soll, tauchen diese Probleme auch dort auf.

Die angesprochenen Schwierigkeiten wurden bereits vom Bundesrat gesehen. In der Stellungnahme des Bundesrates vom 8.11.2006 findet sich folgender Beispielsfall: „Der besonders vergessliche und auch etwas nachlässige „Täter" (Angehöriger einer Behörde oder eines Unternehmens) vermerkt sein Passwort im Nahbereich seines Computers. Er rechnet damit und nimmt in Kauf, dass etwa eine Reinigungskraft das Passwort findet und sich damit einloggt (was sie dann nicht tut)."[10] In ihrer Gegenäußerung argumentiert die Bundesregierung, es fehle in derartigen Fällen an einer Computerstraftat i.S.d. § 202a, weil es nicht zur Überwindung einer besonderen Zugangssicherung gekommen sei.[11] Dies überzeugt jedoch nicht: der Reinigungskraft wird durch den Täter die Möglichkeit gegeben, die Passwortsicherung des Computers zu überwinden. Damit wird der Tatbestand von § 202a n.F. erfüllt. Wollte man dies anders sehen, würde die Herstellung von Passwörtern zur Vorbereitung eines Eindringens in fremde Rechenanlagen niemals den § 202c Abs. 1 Nr. 1 erfüllen.

Als Korrektiv für die zu weit geratene Fassung des subjektiven Tatbestandes dient in der derzeitigen Gesetzesfassung allein der subjektive Tatbestand. Dieses Korrektiv ist jedoch

---

[9] BT-Drucksache 16/3656, S. 20 f.

[10] BT-Drucksache 16/3656, S. 29.

[11] BT-Drucksache 16/3656, S. 32.

kaum ausreichend. § 202c lässt dolus eventualis genügen. Dies bedeutet, dass sich z.B. ein Systemadministrator, der Passworte vergibt oder Sicherungscodes festlegt, schon dann strafbar machen kann, wenn er dabei mit der Möglichkeit rechnet, dass diese Passworte bzw. Sicherungscodes in einem Hacker-Angriff benutzt werden, und sich damit abfindet. Diese Situation dürfte durchaus häufig auftreten. § 202c in seiner jetzigen Fassung könnte deshalb die Arbeit von Systemadministratoren und IT-Sicherheitsfirmen unangemessen behindern.

Um § 202c enger zu fassen, könnte man im subjektiven Tatbestand ansetzen und formulieren: „Wer *in der Absicht*, eine Straftat nach § 202a oder § 202b vorzubereiten, …". Durch das Erfordernis einer kriminellen (auf Begehung der Straftaten § 202a oder 202b bezogenen) subjektiven Tatseite wird zumindest in der Person des Täters der Unrechtstypus klarer herausgearbeitet. Allerdings ist zu bedenken, dass subjektive Tatbestandselemente stets Nachweisschwierigkeiten verursachen können.

Vorzugswürdig erscheint es deshalb, den objektiven Unrechtstypus deutlicher herauszustellen. Dies könnte etwa mittels folgender Formulierung geschehen: „Wer *gezielt* eine Straftat nach § 202a oder § 202b vorbereitet, indem er …". Das Wort „gezielt" wird dabei objektiv verstanden und meint solche Handlungen, die objektiv erkennbar auf die Begehung einer Straftat nach §§ 202a oder 202b abzielen. Statt des Wortes „gezielt" ließe sich auch der (allerdings blassere) Ausdruck „unmittelbar" verwenden.

Derselbe Ansatz findet sich schon in der Nr. 2, wo von einem (objektiv zu verstehenden) „Zweck" die Rede ist. Allerdings sind die Ausführungen gerade zu „dual-use-Werkzeugen" nicht ganz eindeutig. Einerseits verweist die Bundesregierung darauf, dass es ausreicht, dass die objektive Zweckbestimmung des Tools *auch* die Begehung einer Straftat ist,[12] behauptet aber später, dass bei dual-use-tools bereits der objektive Tatbestand nicht erfüllt sei.[13] Es bietet sich an, das Erfordernis einer objektiven Tatbestandseinschränkung deutlicher hervorzuheben, etwa indem man von Computerprogrammen spricht, „deren *offensichtlicher* Zweck" oder „deren *überwiegender* Zweck" die Begehung einer Straftat ist.

V. Datenveränderung, § 303a

In der Stellungnahme des Bundesrates wird gerügt, dass § 303a StGB vielfach wegen seiner erheblichen Unbestimmtheit kritisiert wird.[14] Die Unbestimmtheit bezieht sich z.B. auf die Frage, woran die Verfügungsberechtigung über Daten festzumachen ist. Gerade bei Daten in

[12] BT-Drucksache 16/3656, S. 20.

[13] BT-Drucksache 16/3656, S. 33.

[14] BT-Drucksache 16/3656, S. 29.

vernetzten Systemen ist dieses Problem weitgehend ungeklärt. Daraus lassen sich Bedenken hinsichtlich der Verfassungsmäßigkeit der Norm herleiten. Allerdings erscheint fraglich, ob der Gesetzgeber derzeit in der Lage ist, das Problem zu lösen. In der rechtswissenschaftlichen Literatur hat sich bislang kein Lösungsansatz eindeutig durchsetzen können, und für die Rechtspraxis scheint das Problem keine große Rolle zu spielen. Es erscheint deshalb vertretbar, im vorliegenden Entwurf von einer durchgreifenden Reform des § 303a abzusehen. Dies gilt auch hinsichtlich des Tatbestandsmerkmals „unterdrückt", das in einer neueren Entscheidung des OLG Frankfurt entgegen der ganz h.M. so interpretiert wurde, dass ein nur kurzfristiges Vorenthalten der Daten nicht ausreichen soll.[15] Es ist nicht zu erwarten, dass diese Ansicht in der Rechtsprechung weitere Gefolgschaft findet.

VI. Computersabotage, § 303b

§ 303b soll wie folgt geändert werden:

„(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitung oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend."

---

[15] OLG Frankfurt MMR 2006, S. 547 mit Anm. Hilgendorf, jurisPraxisreport IT-Recht 10/2006, Anm. 5.

Der neue § 303b weitet den strafrechtlichen Schutz gegen Computersabotage in Absatz 1 auf grundsätzlich alle Datenverarbeitungen aus. Angesichts der Tatsache, das der Computer inzwischen für fast jedermann zum Alltag gehört und die meisten Privathaushalte über einen eigenen Rechner verfügen, verdient diese Ausweitung des strafrechtlichen Schutzes Zustimmung. Durch das einschränkende Korrektiv der Datenverarbeitung von „wesentlicher Bedeutung" soll einer Inflationierung des staatlichen Strafanspruchs begegnet werden. Dies ist überzeugend. Die Aufgabe einer Angrenzung von „wesentlicher" zu „unwesentlicher" Bedeutung einer Datenverarbeitung wird von der Rechtsprechung zu lösen sein (vgl. auch schon § 303b a.F.).

§ 303b Abs. 1 Nr. 2 dient der strafrechtlichen Erfassung von DoS-Angriffen. Der objektive Tatbestand (Dateneingabe und -übermittlung) ist weit gefasst und wird nur durch das Absichtserfordernis des subjektiven Tatbestandes eingeschränkt. Diese Gesetzgebungstechnik führt dazu, dass der – prinzipiell schwierigen – Feststellung der subjektiven Tatseite besonderes Gewicht zukommt. Zur Erfassung der besonderen Situation von DoS-Angriffen dürfte aber kaum eine andere Lösung möglich sein.

Auch § 303b n.F. wirft das Problem auf, dass infolge der fortschreitenden Digitalisierung unserer Lebenswelt kaum noch elektronische Geräte ohne Datenverarbeitung existieren, so dass grundsätzlich auch die Beschädigung solcher Geräte unter § 303b subsumiert werden könnte. Der Bundesrat erwähnt in seiner Stellungnahme die Störung von Videorekordern, Hifi-Anlagen, Fernsehgeräten, Navigationsgeräten, Wasch- und Spülmaschinen und programmierbare Elektroherde. Allerdings wird es sich bei in derartigen Geräten ablaufenden „Datenverarbeitungen" kaum je um Datenverarbeitungen von „wesentlicher Bedeutung" für den Betroffenen handeln, wie dies § 303b Abs. 1 erster Halbsatz voraussetzt.

VII. Zur Erfassbarkeit des „Phishing"

Fortlaufend tauchen im Internet neue Formen von sozialschädlichem Verhalten auf, deren Erfassbarkeit durch die etablierten Tatbestände des Computerstrafrechts problematisch erscheint. In jüngerer Zeit hat vor allem dass „Phishing" (zusammengesetzt aus „password" und „fishing") für Aufmerksamkeit gesorgt.[16] Beim „Phishing" versucht der Täter, per email (oder über ein anderes Medium) den Empfänger dazu zu veranlassen, Passwörter und andere relevante Zugangsdaten herauszugeben. Die Idee derartige Vorgehensweisen im Internet ist alt und wurde bereits vor über 10 Jahren unter der damals gebräuchlichen Bezeichnung

[16] J.-P. Graf, „Phishing" derzeit nicht generell strafbar, in: NStZ 2007, S. 129 – 132; Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht (Fn. 5), Rn. 760 ff.; ausführlich C.F. Stuckenberg, ZStW 118 (2006), S. 878 ff.; vgl. auch G. Borges, Rechtsfragen des Phishing, in: NJW 2005, S. 3313 ff.

„man-in-the-middle-Angriff“ diskutiert. Für die heutigen Formen des Phishing ist festzustellen, dass sie de lege lata strafrechtlich nicht vollständig erfassbar sind:[17]

Der Tatbestand des § 263 StGB kann daran scheitern, dass zwar eine Täuschungshandlung des Täters und eine entsprechende Irrtumserregung beim Opfer vorliegen, nicht dagegen eine unmittelbar vermögensschädigende oder auch nur „schadensgleich“ vermögensgefährdende Verfügung des Opfers über sein Vermögen.[18] In der bloßen Preisgabe des Passworts oder anderer Zugangsdaten kann zwar oft, aber keineswegs immer eine schadensgleiche Vermögensgefährdung gesehen werden. Eine unmittelbare Vermögensgefährdung fehlt etwa in den Fällen, in denen es sich der Täter vorbehält, die in großem Stil „gephishten“ Zugangsdaten erst einmal zu sammeln und nur besonders aussichtsreich erscheinende unerlaubte Transaktionen vorzunehmen.

§ 202a liegt meist deshalb nicht vor, weil der Täter sich die Zugangsdaten nicht unter Überwindung einer besonderen Sicherung verschafft. § 269 schließlich, der in einer Vielzahl von Fällen einschlägig sein kann, scheidet dann aus, wenn die Absenderangabe fehlt oder so diffus ist, das von der Angabe eines konkreten Absenders und damit von einer „Garantiefunktion“ der digitalen Urkunde nicht gesprochen werden kann. Gerade die Fälle, in denen § 269 wegen unklarer oder gänzlich fehlender Absenderangaben nicht in Frage kommt, zeichnen sich in der Regel durch eine nicht unerhebliche Nachlässigkeit des Opfers aus, so dass man, ausgehend von einem viktimodogmatischen Ansatz, die Angemessenheit eines strafrechtlichen Schutzes in Frage stellen könnte. Gerade diese Form sozialschädlichen Verhaltens im Internet zeigt wieder einmal deutlich, dass die beste, weil wirkungsvollste Art der Prävention nicht das Strafrecht, sondern eine verbesserte Medienkompetenz der Nutzer darstellt.

Angesichts des Gefährlichkeitspotentials des „Phishing“ und der hohen Kosten, die durch diese neue Form betrügerischen Verhaltens im Internet entstehen, erscheint es jedenfalls nicht abwegig, über eine vollständigere Kriminalisierung des Phishing nachzudenken.

Erstaunlicherweise wird in der Gesetzesbegründung nicht näher thematisiert, dass § 202c Abs. 1 Nr. 1 (Sich-Verschaffen von Passwörtern) bereits die meisten Fälle des Phishing erfassen dürfte. Im Sich-Verschaffen von Passwörtern oder sonstigen Zugangscodes liegt der Kern des „Phishing“. Eine gewisse Einschränkung bewirkt die Voraussetzung, dass durch die Passwortverschaffung eine Straftat nach § 202a oder § 202b vorbereitet werde müsse. Ein

---

[17] Graf, NStZ 2007 (Fn. 16), 129, 132.

[18] Im Regelfall des „Phishing“ wird allerdings ein Betrug gem. § 263 vorliegen, vgl. Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht (Fn. 5), Rn. 765.

„Phisher“, der sich durch Täuschung im Internet Passwörter oder sonstige Zugangsdaten zu Konten oder anderen attraktiven geschützten Bereichen verschafft hat, wird, wenn er die „gephishten“ Daten verwendet, in aller Regel den § 263a Abs. 1 Var. 3 oder Var. 4 verwirklichen. Um das „Phishing“ noch zuverlässiger zu erfassen, bietet es sich deshalb an, in § 202c zu formulieren „Wer eine Straftat nach § 202a, 202b *oder 263a* vorbereitet, …“ bzw. „Wer *in der Absicht*, eine Straftat nach § 202a, 202b *oder 263a* vorzubereiten, …“.
Denkbar erscheint es aber auch, das „Phishing“ wegen seiner besonderen Bedeutung in einem eigenen Straftatbestand (§ 202d) zu erfassen. Eine entsprechende Strafnorm könnte folgenden Wortlaut haben:

> *„Wer es in der Absicht, einem anderen Nachteil zuzufügen, unternimmt, in den Kommunikationsdiensten des Internet den Empfänger durch unzutreffende Angaben zur Preisgabe von Passwörtern oder anderer Zugangsdaten zu bewegen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.“*

Eine solche Vorschrift wäre weit genug, um alle strafwürdig erscheinenden Formen des „Phishing“ zu erfassen. Will man nur das Vermögen vor den Aktivitäten von „Phishern“ schützen, könnte man statt der Nachteilszufügungsabsicht die Formulierung verwenden „*sich oder einem anderen/Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen*“.

VIII. Empfiehlt sich eine Pönalisierung von Leichtfertigkeit im Netzverkehr?

Mit der Digitalisierung des Alltags wird die Verwendung des Computers mehr und mehr zur Selbstverständlichkeit. Bürgerinnen und Bürger nutzen das Internet in vielfältigster Weise etwa zur Kommunikation, zur Informationsgewinnung, im Berufsleben und zur Freizeitgestaltung. Der Verkehr im Internet wird deshalb mehr und mehr zur Selbstverständlichkeit. In Parallele zum Straßenverkehr sollte deshalb darüber nachgedacht werden, den Internetnutzern grundlegende Sicherungsmaßnahmen abzuverlangen, um nicht sich und andere zu gefährden. So wie z.B. die §§ 315c, 316 im Straßenverkehr sicherstellen sollen, dass nicht von Verkehrsteilnehmer nicht mehr sozialadäquate Gefahren ausgehen, so ließe sich an Vorschriften denken, die entsprechende Sicherungen für PC-Nutzer fordern und ihre Unterlassung unter Strafe stellen.[19] Man sollte bedenken, dass die massenhafte Verbreitung von Viren und anderer Formen von Schadsoftware nur möglich ist, weil viele Nutzer elementare Sicherungsmaßnahmen unterlassen. Desgleichen werden DDoS-Angriffe

[19] E. Hilgendorf, Aktuelle Fragen des materiellen Computer- und Internetstrafrechts im Spiegel neuerer Gesamtdarstellungen, in: ZStW 118 (2006), S. 202 (204).

oft über gekaperte Rechner durchgeführt, deren nichts ahnende Nutzer entsprechende Sicherungsmaßnahmen vernachlässigt haben.

Mangels Gehilfenvorsatz kommt eine Beihilfe-Strafbarkeit (§ 27) in derartigen Fällen in der Regel nicht in Betracht. Um diese Lücke zu schließen, ließe sich an eine Strafnorm denken, die das leichtfertige Unterlassen zumutbarer Sicherungen des PC unter Strafe stellt, sofern dadurch Straftaten nach §§ 202a, 202b, 303a oder 303b ermöglicht werden. Mit Blick auf das ultima-ratio-Prinzip erscheint es jedoch angebracht, zunächst nicht-strafrechtliche Möglichkeiten einer Problemlösung zu prüfen. Wirkungsvoll könnte insbesondere die Einführung einer zivilrechtlichen Gefährdungshaftung sein. Langfristig scheint mir die Einführung eines entsprechenden Fahrlässigkeitstatbestandes aber nicht ausgeschlossen zu sein.

IX. Zusammenfassung

Der Gesetzentwurf erscheint insgesamt gelungen. Folgende Punkte verdienen eine neuerliche Prüfung:

1. Das Merkmal „unter Anwendung technischer Mittel“ in § 202b dürfte überflüssig sein, da sich Daten i.S.v. § 202a stets nur mit technischen Mitteln verschaffen lassen.
2. § 202c ist zu weit geraten. Eine Einschränkung kann auf der Ebene des subjektiven Tatbestandes („Wer in der Absicht …“) oder, was vorzugswürdig erscheint, auf der Ebene des objektiven Tatbestandes („gezielt … vorbereitet“) erfolgen.
3. Um das „Phishing“ noch besser zu erfassen, kann im objektiven Tatbestand des § 202c die Formulierung gewählt werden: „Wer eine Straftat nach § 202a, 202b oder § 263a vorbereitet, …“. Denkbar ist aber auch ein gänzlich neuer Straftatbestand mit folgendem Wortlaut: *„Wer es in der Absicht, einem anderen Nachteil zuzufügen, unternimmt, in den Kommunikationsdiensten des Internet den Empfänger durch unzutreffende Angaben zur Preisgabe von Passwörtern oder anderer Zugangsdaten zu bewegen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.“*

Würzburg, den 17.3.2006