GERCKE

Dr. Marco Gercke I Niehler Str. 35 I 50733 Köln I www.gercke.de I info@gercke.de

STELLUNGNAHME

zum Gesetzesentwurf der Bundesregierung zu einem Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (BT-Drs. 16/3656) zur Vorbereitung der öffentlichen Anhörung im Rechtsausschuss am 21.3.2007

1. Einleitung

Der vorliegende Entwurf des Strafrechtsänderungsgesetzes bezweckt die Umsetzung des EU-Rahmenbeschlusses über Angriffe auf Informationssysteme[1] und die (teilweise) Umsetzung der Cybercrime Konvention des Europarates[2] in nationales Recht. Gemäß Art. 12 Abs. 1 des Rahmenbeschlusses vom 24.2.2005 sind die Mitgliedstaaten verpflichtet, die im Rahmenbeschluss enthaltenen Maßnahmen waren zum 16.3.2007 umzusetzen. Der Gesetzesentwurf dient vorrangig der Umsetzung des Rahmenbeschlusses. Eine Umsetzung der Cybercrime Konvention, zu der sich Deutschland mit der Unterzeichnung im Jahr 2001 verpflichtet hat und die mittlerweile von 19 Staaten ratifiziert wurde[3], erfolgt

[1] Rahmenbeschluss 2005/222/JI des *Rates*. Vgl. dazu einleitend *Sanchez-Hermosilla*, CR 2003, 778; Ausführlich *Hilgendorf* in Schwarzenegger, Internet-Recht und Strafrecht, S. 257ff.; *Gercke* CR 2005, 468ff.

[2] Vgl. zur Cybercrime Konvention *Sannbrucker*, Convention on Cybercrime; *Gercke*, CR 2004, 782; *ders.* MMR 2004, 728ff. u. 851ff.; *ders.* ZUM 2005, 615f.; *Valerius,* KR 2004, 513ff.; *Dix*, DuD 2001, 589; *Breyer*, DuD 2001, 594 mwN.; *Schulzki-Haddouti*, Beitrag in Telepolis vom 27.6.2000, abrufbar unter www.heise.de/tp/deutsch/inhalt/te/8290/1.html (Stand Feb. 2007); *Taylor*, The Council of Europe Cybercrime Convention – A civil liberties perspective, abrufbar unter http://crime-research.org/library/CoE_Cybercrime.html

[3] Albanien (2002), Armenien (2006) Bosnien Herzegowina (2006) Bulgarien (2005), Dänemark (2005), Ehemalige jugoslawische Republik Mazedonien (2005), Estland (2003), Frankreich (2006), Island (2007), Kroatien (2002),

nur hinsichtlich ausgewählter Aspekte des materiellen Strafrechts[4]. Während die Umsetzung der Vorgaben des Rahmenbeschlusses weitgehend gelingt, gibt die zögerliche Umsetzung der Cybercrime Konvention des Europarates Anlass zur Kritik.

Zutreffend wird in der Begründung des Gesetzesentwurfs darauf hingewiesen, dass die Internetkriminalität kein nationales, sondern ein internationales Phänomen darstellt. Bislang bereitet die Bekämpfung grenzüberschreitender Straftaten im Internet erhebliche Probleme. Diese sind zum einen darauf zurück zu führen, dass in einigen Staaten weiterhin adäquate Strafnormen fehlen. Dem tragen sowohl der Rahmenbeschluss, als auch die Cybercrime Konvention Rechnung. Zum anderen resultieren die Probleme bei der Bekämpfung transnationaler Computerstraftaten aus dem Fehlen strafprozessualer Ermittlungsinstrumente und Regelungen im Bereich der internationalen Kooperation bei grenzüberschreitenden Ermittlungen. Weder der EU-Rahmenbeschluss, noch die ausgewählten und mit dem Strafrechtsänderungsgesetz umgesetzten Vorgaben der Cybercrime Konvention im Bereich des materiellen Strafrechts tragen diesem Umstand Rechnung.

Es ist vor diesem Hintergrund nicht nachvollziehbar, warum die Bundesrepublik anders als beispielsweise Frankreich, die neuen EU Mitglieder Rumänien und Bulgarien sowie 16 weitere Staaten auch 5 Jahre nach der Unterzeichnung der Konvention keine vollständige Umsetzung vorgenommen hat. Die Umsetzung der Art.2 bis 8 mag als erster Ansatz zu würdigen sein. Angesichts der internationalen Bedrohung durch weltweit agierende Internetstraftäter, erscheint jedoch zweifelhaft, ob der vorliegende Entwurf die adäquate Antwort auf die Herausforderungen der Internetkriminalität darstellt. Die große Chance, innerhalb der Umsetzungsfrist des Rahmenbeschlusses auch die Cybercrime Konvention zu ratifizieren, wurde bedauerlicherweise nicht genutzt.

Litauen (2004), Niederlande (2006), Norwegen (2006), Rumänien (2004), Slowenien (2004), Ukraine (2006), Ungarn (2003), Vereinigte Staaten von Amerika (2006) und Zypern (2005).

[4] Die Umsetzung der Vorgaben im Hinblick auf inhaltsbezogene Straftaten, das Verfahrensrecht und insbesondere des für die Verbesserung transnationaler Ermittlungen wesentlichen Bereichs der internationalen Zusammenarbeit bleibt gesonderten Gesetzesvorhaben vorbehalten. Vgl. dazu auch die Begründung des Gesetzesentwurfs, BT-Drs. 16/3656, S. 6.

2. Eingeschränkter Handlungsspielraum des Gesetzgebers

Der vorliegende Entwurf des Strafrechtsänderungsgesetzes ist auf Kritik gestoßen.[5] Weite Teile der Kritik betreffen jedoch rechtspolitische Entscheidungen, die aufgrund der verbindlichen Vorgaben des Rahmenbeschlusses und der Cybercrime Konvention der Disposition des nationalen Gesetzgebers entzogen sind. Exemplarisch sei dies an der kritisierten Kriminalisierung von Vorbereitungshandlungen zum Ausspähen und Abfangen von Daten in § 202c StGB verdeutlicht. Dem Grunde nach ist die Kritik, soweit sie die Vorverlegung der Strafbarkeit betrifft, nachvollziehbar. Betrachtet man die Gesetzesänderungen, die in den letzten Jahren verabschiedet wurden, so ist auffällig, dass insbesondere bei der Bekämpfung von Computer- und Internetstraftaten bis dahin straflose Vorbereitungshandlungen kriminalisiert wurden. Sowohl im Zusammenhang mit § 108b Abs.2 UrhG wie auch bei der Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union vom 28.05.2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln[6] zeigen sich deutliche Tendenzen zur Intensivierung der Kriminalisierung im Vorfeldbereich. So ist im Rahmen der Umsetzung des Rahmenbeschlusses eine Ergänzung des § 263a StGB um ein Verbot des Herstellens, Verschaffens, Verwahrens und Überlassen von Computerprogrammen, deren Zweck die Begehung eines Computerbetrugs ist, erfolgt. Eine vergleichbare Kriminalisierung von Vorfeldhandlungen findet sich auch in § 176 Abs.4 Nr. 3 StGB. Danach macht sich bereits wegen sexuellem Missbrauch strafbar, wer auf ein Kind durch Schriften im Sinne des § 11 Abs.3 StGB einwirkt, um es zu sexuellen Handlungen zu bewegen. Die Norm zielt aufgrund der – zu Recht als inkonsequent kritisierten Beschränkung auf Schriften[7] – insbesondere auf die in den letzten Jahren zunehmend in das Interesse der Öffentlichkeit gerückten Anbahnungen von Kindesmissbauchsfällen in Internet-Chat-Foren ab.[8] Tatsächlich bieten Chat-Foren durch die einfachen Möglichkeiten der Verschleierung von Geschlecht und Alter Pädophilen die Gelegenheit zur vermeintlich anonymen

[5] Vgl. dazu beispielsweise die Stellung der *Humanistischen Union*, abrufbar unter http://www.humanistische-union.de/themen/innere_sicherheit/verdeckte_ermittlungen/ (Stand März. 2007); Stellungnahme des *ECO Verbandes*, abrufbar unter http://www.eco.de (Stand März. 2007); Stellungnahme des *Teletrust Deutschland e.V.* vom 27.10.2006; *Schulz*, MIR Dok. 180-2006; Stellungnahme des *BITKOM e.V.* abrufbar unter www.bitkom.org. (Stand: März 2007) Stellungnahme des *Bundesrates* zum Gesetzesentwurf, BR-Drs. 676/06.

[6] ABl. EG Nr. L 149 v. 2.06.2001,1.

[7] *Duttge, Hörnle, Renzikowski*, NJW 2004, 1067f.

[8] BT-Drs. 15/350 S. 17f.

Kontaktaufnahme mit potentiellen Opfern.[9] Es fehlen aber aussagekräftige Untersuchungen über die von Chaträumen tatsächlich ausgehende Gefahr.[10] Angesichts rückläufiger Zahlen in der Polizeilichen Kriminalstatistik im Zusammenhang mit dem sexuellen Missbrauch von Kindern stellt sich aber die Frage, ob allein die Wahrnehmung der Problematik in der Öffentlichkeit es rechtfertigt, isoliert bei der Anbahnung der Kontaktaufnahme durch Schriften vom Grundprinzip, dass Vorbereitungshandlungen straflos sind, abzuweichen.[11] Diese Frage ist über das Pornographiestrafrecht auch für die übrigen Bereiche der Vorfeldkriminalisierung im Zusammenhang mit Internetstraftaten – so auch im Hinblick auf die Einführung des § 202c StGB - von Bedeutung.

Gleichwohl ist die grundsätzliche Kritik an § 202c StGB insoweit verspätet, als dem nationalen Gesetzgeber aufgrund der Vorgaben in Art. 6 der Cybercrime Konvention – von den Einschränkungsmöglichkeiten in Art. 6 Abs. 3 abgesehen – im Rahmen der Umsetzung weitgehend die Hände gebunden sind. Als Konsequenz der beschränkten Dispositionsbefugnisse des nationalen Gesetzgebers im Rahmen der Umsetzung internationaler Vorgaben lässt sich eine Einbeziehung der Kritik an Grundsatzfragen nur berücksichtigen, soweit diese bereits im Entstehungsprozess der internationalen Vorgaben erfolgen.

3. Der Gesetzesentwurf

In Ermangelung eines konkreten Fragekatalogs beschränkt sich die folgende Darstellung auf ausgewählte Bereiche des Gesetzesentwurfes, die sich als besonders problematisch erweisen.

3.1 Neufassung des § 202a StGB

Der Gesetzesentwurf sieht vor, die Vorgaben aus Art. 2 des EU-Rahmenbeschlusses und Art. 2 der Cybercrime Konvention zur Kriminalisierung des rechtswidrigen Zugangs zu

---

[9] Zur Möglichkeit der Rückverfolgung vgl. *Gercke*, DuD 2002, 477ff.

[10] Auch die Bundesregierung stützte sich nicht auf aussagekräftige Untersuchungen, sondern bemühte in der Gesetzesbegründung zu § 176 Abs.4 unter anderem einen Bericht der Süddeutschen Zeitung vom September 1999 über den „offenbar nicht seltenen Fall" dass sich amerikanische Internetnutzer in so genannten Chatrooms mit Kindern zu sexuellen Begegnungen verabreden.

[11] Gegenüber 15255 erfassten Fällen im Jahr 2004 wurden 2005 13962 Fälle in der PKS für das Jahr 20035ausgewiesen, was einen Rückgang um 8,5% bedeutet.

Informationssystemen durch eine Neufassung des § 202a StGB umzusetzen. Gemäß der Entwurfsfassung soll § 202a Abs.1 StGB-E wie folgt neu gefasst werden:

§ 202a StGB-E

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 internationalen Vorgaben erfordern ein Tätigwerden des Gesetzgebers, da das Deutsche Strafrecht keine Strafnorm beinhaltet, die einen autonomen Schutz der Integrität von Informationssystemen bietet[12]. Der Gesetzgeber hat sich im Rahmen der Gesetzesnovellierung durch das 2. WiKG dagegen ausgesprochen, das bloße Eindringen in ein Computersystem unter Strafe zu stellen[13]. Anders als in der bisherigen Fassung stellt die geplante Änderung nicht erst das Verschaffen von Daten, sondern bereits das Verschaffen des Zugangs zu Daten unter Strafe. Trotz der damit einhergehenden Vorverlagerung der Strafbarkeit werden mit der geplanten Änderung die Vorgaben der Cybercrime Konvention und des EU-Rahmenbeschlusses nicht vollständig umgesetzt.

Anders als die Cybercrime Konvention und der Rahmenbeschluss, die als Rechtsgut die Integrität der Computersysteme schützen, basiert der vorliegende Gesetzesentwurf weiterhin auf einem Schutz der Integrität von Daten.[14] Dies hat zur Folge, dass der Gesetzesentwurf nur in den Fällen eine Strafbarkeit begründet, in denen mit dem Zugriff zu einem Computersystem auch der Zugang zu Daten einhergeht. Regelmäßig ist dies der Fall, da mit dem Zugriff auf ein Computersystem in der überwiegenden Zahl der Fälle nicht nur der Zugang zum System, sondern auch zu den dort gespeicherten Daten möglich ist. Gleichwohl sind Fallgestaltungen möglich, die bedingt durch die

---

[12] Vgl. dazu im Hinblick auf die Vorgaben aus Art. 2 EU-Rahmenbeschlusses und die Notwendigkeit der Anpassung des Deutschen Rechts *Gercke*, CR 2005, 470; zu den Vorgaben aus Art. 2 Cybercrime Konvention und die Notwendigkeit der Anpassung des Deutschen Rechts vgl. *Gercke*, MMR 2004, 729.

[13] Im Rahmen der Verhandlungen zum 2. WiKG wurde die Reichweite der Kriminalisierung des Hackings intensiv diskutiert. Der Gesetzgeber hat sich gegen einen autonomen Schutz von Computersystemen entschieden und das klassische Hacking straflos belassen (vgl. BT-Drs. 10/5058, S. 28f. Kritisch dazu *Tiedemann*, JR 1986, 871; Zur Reichweite des 2. WiKG im Bereich der Zugriffe auf Datensysteme vgl. *Sieber*, Informationstechnologie und Strafrechtsreform, S. 51 ff.; *v.Gravenreuth*, NStZ 1989, 201ff.; *Haft*, NStZ 1987, 6ff.). Von § 202a StGB erfasst werden daher bislang nur die Fälle, in denen das Eindringen mit dem Ausspähen von Daten i.S.d. § 202a StGB einhergeht.

[14] Vgl. Begründung des Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität, BT-Drs. 16/3656 S. 13.

unterschiedlichen Rechtsgüter von Art. 2 der Cybercrime Konvention und Art. 2 des Rahmenbeschlusses, nicht aber von § 202a StGB-E erfasst werden.

Das Kernproblem ist insoweit die fehlende Präzisierung der Tathandlung. Während die Entwurfsbegründung ausführlich auf die Auslegung der Tatbestandsbeschränkungen eingeht, fehlt eine hinreichend klare Definition, wann ein Zugriff auf Daten verschafft wird. Die Bezugnahme auf die bisherige Regelung des § 202a StGB spricht dafür, dass ein Zugang zu Daten verschafft wurde, wenn der Täter die Möglichkeit hat, diese abzurufen. Neben den Fällen des Hacking, bei denen das Eindringen in ein System nicht Selbstzweck war, sondern der Vorbereitung einer Datenspionage diente, erfasst die Norm nunmehr auch die Fälle, in denen der Angriff mit dem Überwinden der Schutzmaßnahme abgebrochen wurde, obwohl ein Ausspähen der Daten möglich gewesen wäre.

Dass gleichwohl ein den Vorgaben entsprechender Schutz der Systemintegrität nicht erreicht wird, verdeutlicht folgendes Beispiel: Der Anbieter X betreibt einen FTP Server bei dem er zwei unterschiedliche, jeweils passwortgeschützte Zugänge eingerichtet hat. Der eine berechtigt nur zum Aufspielen von Daten, nicht aber zum Abruf gespeicherter Daten, während der zweite Zugang auch zum Abruf der Daten berechtigt. Gelingt es einem Täter, die Schutzmaßnahme des ersten Zugangs zu überwinden, so kann er durch das Hochladen von Daten die Integrität des Computersystems verletzten, ohne dass er einen Zugang zu den (gespeicherten) Daten verschaffen würde.

Diese Strafbarkeitslücke ließe sich dadurch schließen, dass man das Verschaffen des Zugangs zu Daten so weit auslegte, dass neben der Möglichkeit des Abrufens von Daten jegliche Datenveränderung erfasst wird. Doch selbst dann deckt sich die Systemintegrität nicht mit der von § 202a StGB gewährleisteten Datenintegrität.

So lassen sich bei den meisten Betriebssystemen im Rahmen der Einrichtung neuer Benutzer deren Rechte beschränken. Während die für den Consumerbereich entwickelten Betriebssysteme der Firma Microsoft oft nur eingeschränkte Skalierungen der Nutzungsrechte erlauben, lassen sich diese beispielsweise in Linuxumgebungen sehr präzise einschränken. Wird ein (passwortgeschütztes) Benutzerkonto angelegt, dass weder den Zugriff auf bestehende Daten, noch deren Veränderung erlaubt und gelingt es einem Hacker, den Passwortschutz zu überwinden, so verletzt er die von Art. 2 des EU-Rahmenbeschlusses und Art. 2 der Cybercrime Konvention geschützte Systemintegrität, ohne sich gemäß § 202a StGB-E strafbar zu machen.

Der Gesetzesentwurf ist daher insoweit nicht geeignet, die internationalen Vorgaben vollständig umzusetzen. Daher sollte eine stärker am Wortlaut der Vorgaben orientierte Entwurfsfassung in Erwägung gezogen werden.

3.2 Strafbarkeit der Vorbereitung des Ausspähens und Abfangens von Daten

Gemäß Art. 6 der Cybercrime Konvention sind die Mitgliedstaaten verpflichtet, das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten, sowie den Besitz von Vorrichtungen und Zugriffsdaten, die in erster Linie der Begehung von Straftaten gemäß Art. 3 bis 5 der Konvention dienen oder diese ermöglichen, unter Strafe zu stellen[15]. Der Gesetzesentwurf sieht vor, die Vorgaben durch das Einfügen eines § 202c StGB-E umzusetzen:

§ 202c StGB-E

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a

Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, ver-

breitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Wie oben dargestellt, ist der Entwurf des § 202c StGB-E auf erhebliche Kritik gestoßen[16]. Neben den oben genannten grundsätzlichen Bedenken gegen eine weitere Vorfeldkriminalisierung liegt das Augenmerk der Kritiker dabei auf dem Risiko, dass auch sicherheitsrelevante Handlungen zur Abwehr von Angriffen zukünftig strafbar sein könnten. Zu Recht weisen die Kritiker darauf hin, dass es für Systemadministratoren von großer Bedeutung ist, durch die Simulation von Angriffen das eigene System auf Schwachstellen zu überprüfen[17]. Sollte § 202c Abs.1 Nr. 2 StGB-E nicht zwischen den Taten Krimineller und den Sicherungsmaßnahmen berechtigter Personen differenzieren,

[15] Vgl. dazu im Hinblick auf die Vorgaben aus Art. 6 Cybercrime Konvention und die Notwendigkeit der Anpassung des Deutschen Rechts *Gercke*, MMR 2004, 731.

[16] Vgl. dazu beispielsweise die Stellung der *Humanistischen Union*, abrufbar unter http://www.humanistische-union.de/themen/innere_sicherheit/verdeckte_ermittlungen/ (Stand Feb. 2007); Stellungnahme des *ECO Verbands*, abrufbar unter http://www.eco.de (Stand Feb. 2007); Stellungnahme des *Chaos Computer Clubs*, abrufbar unter http://www.ccc.de/press/releases/2006/20060925/ (Stand Feb. 2007) sowie die Berichterstattung bei Spiegel-Online, http://www.spiegel.de/netzwelt/politik/0,1518,438969,00.html (Stand Feb. 2007).

[17] Stellungnahme des *BITKOM e.V.* abrufbar unter www.bitkom.de/files/documents/Stellungnahme_BITKOM_StrAendG_12_07_06.pdf (Stand Feb. 2007).

bestünde nach Auffassung der Kritiker die Gefahr, dass darunter die technische Sicherheit der Informationssysteme leiden könnte.

Problemtisch erweist sich insoweit, dass § 202c Abs.1, Nr. 2 StGB-E anders als die Konvention nicht auf Computerprogramme beschränkt ist, die „in erster Linie" zur Begehung der genannten Delikte entworfen wurde. Insoweit geht der Gesetzesentwurf über die Vorgaben aus Art. 6 der Cybercrime Konvention hinaus. Doch selbst wenn die Einschränkung aufgenommen worden wäre, bliebe der Gewinn an Rechtssicherheit gering. Sowohl die Beschränkung „in erster Linie" als auch die in der Entwurfsfassung verwendete Formulierung der objektiven Zweckbestimmung[18] sind wenig präzise.

Gleichwohl weist die Bundesregierung die Kritik an der Reichweite der Norm als unberechtigt zurück.[19] Sie ist der Auffassung, der gutwillige Umgang mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen werde entgegen der geäußerten Bedenken schon deshalb nicht von § 202c StGB-E erfasst, da der objektive Tatbestand ein Computerprogramm erfordere, dessen Zweck die Begehung von Computerstraftaten ist. Da die Systemadministratoren und Sicherheitsunternehmen im Rahmen der Durchführung realitätsnaher Tests aber gerade darauf angewiesen sind, Programme für simulierte Angriffe zu nutzen, die auch bei wirklichen Angriffen eingesetzt werden und deren objektive Zweckbestimmung mithin regelmäßig (auch) die Begehung von Straftaten ist[20], wird der Tatbestand in diesen Fällen nicht aufgrund des Fehlens eines geeigneten Tatobjekts ausgeschlossen. Gleichwohl ist der Auffassung der Bundesregierung, § 202c StGB-E sei in den Fällen einer berechtigten Sicherheitsüberprüfung nicht anwendbar, zuzustimmen. § 202c StGB-E setzt voraus, dass das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonst Zugänglichmachen zum Zweck der Begehung einer Straftat nach §§ 202a oder 202b StGB-E erfolgt. Sofern ein Einverständnis des Berechtigten vorliegt, sind Sicherheitstests nicht unbefugt i.S.d. § 202a StGB. Mithin stellt auch die Vornahme der vorgelagerten Akte keine gemäß § 202c StGB-E strafbare Handlung dar.[21]

[18] Vgl. Begründung des Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität, BT-Drs. 16/3656 S. 20.

[19] Gegenäußerung der *Bundesregierung* zur Stellungnahme des Bundesrates, BT-Drs. 16/3656 Anlage 3.

[20] In der Begründung des Gesetzesentwurfs wird darauf verwiesen, des nicht darauf ankomme, dass die Software ausschließlich für die Begehung einer Computerstraftat bestimmt sein. Es reiche vielmehr aus, wenn die objektive Zweckbestimmung des Tools auch die Begehung einer solchen Straftat ist. Begründung des Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität, BT-Drs. 16/3656 S. 22.

[21] Über die Zweckbindung der Tat lassen sich auch die vom Bundesrat in die Diskussion eingebrachten Fälle der Weitergabe von Passwörtern durch Berechtigte lösen. Zu den Fällen vgl. Stellungnahme des *Bundesrates* zum Gesetzesentwurf, BR-Drs. 676/06.

3.3 Neufassung des § 303b StGB

Der Gesetzesentwurf sieht vor, die Vorgaben aus Art. 3 des EU-Rahmenbeschlusses und Art. 5 der Cybercrime Konvention zur Kriminalisierung des rechtswidrigen Systemeingriffs durch eine Neufassung des § 303b StGB-E umzusetzen. Gemäß der Entwurfsfassung soll § 303b Abs.1 StGB wie folgt neu gefasst werden:

§ 303b StGB-E

(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 Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

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

Die Neufassung setzt die Vorgaben des EU-Rahmenbeschlusses und der Cybercrime Konvention vollumfänglich um[22]. Mit der Ergänzung gehen zwei wesentliche Konsequenzen einher. Zum einen werden – anders als in der bisherigen Fassung der Norm - zukünftig nicht nur Computersysteme von fremden Betrieben, Unternehmen und Behörden, sondern auch Privatrechner in den Schutzbereich der Norm einbezogen[23]. Dabei ist jedoch zu berücksichtigen, dass mit der Beibehaltung der Formulierung „von wesentlicher Bedeutung" die bestehenden Abgrenzungsschwierigkeiten nicht beseitigt werden und – aufgrund der Ausweitung auf private Computersysteme – ggf. sogar verstärkt werden. Die zweite Änderung betrifft die Einführung zweier weiterer Tatvarianten in § 303b Abs. 1 Nr. 2 StGB. Mit der Einbeziehung des Eingebens und

[22] Vgl. dazu im Hinblick auf die Vorgaben aus Art. 3 EU-Rahmenbeschlusses und die Notwendigkeit der Anpassung des Deutschen Rechts vgl. *Gercke*, CR 2005, 470f.; zu den Vorgaben aus Art. 5 Cybercrime Konvention und die Notwendigkeit der Anpassung des Deutschen Rechts vgl. *Gercke*, MMR 2004, 731.

[23] Im § 303b Abs. 2 StGB sieht der Entwurf eine Strafschärfung vor: § 303b Abs. 2 StGB-E: 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.

Übermittelns von Daten werden nunmehr zweifelsfrei auch sog. „Denial-of-Service Angriffe“[24] von § 303b StGB-E erfasst[25]. Die Aufnahme der zusätzlichen Tathandlungen, die aufgrund der Vorgaben der Cybercrime Konvention und des EU-Rahmenbeschlusses notwenig war, beseitigt insoweit die Rechtsunsicherheit, die durch eine Entscheidung des *OLG Frankfurt*[26] zur Strafbarkeit der Blockade der Lufthansa-Seite entstanden ist.

Köln, den 16.03.2007

Dr. Marco Gercke

[24] Als Denial-of-Service Angriff werden Angriffe gegen einen Computersystem bezeichnet, bei denen durch massenhafte Anfragen eine Überlastung des Computersystems hervorgerufen wird.

[25] Es sprechen gewichtige Gründe dafür, dass entsprechende Angriffe bereits über § 303b Abs. 1 Nr. 1 i.V.m. § 303a Abs. 1 StGB über die Tatbestandsmerkmale „Unterdrücken“ und „Unbrauchbarmachen“ strafbar sind. Vgl. dazu *Gercke*, ZUM 2006, 290f.; a.A *Kitz*, ZUM 2006, 730ff.

[26] *OLG Frankfurt*, MMR 2006, 547ff. mit Anm. *Gercke*;