Deutscher Bundestag **Drucksache 16/5449**

16. Wahlperiode 23. 05. 2007

Beschlussempfehlung und Bericht

des Rechtsausschusses (6. Ausschuss)

zu dem Gesetzentwurf der Bundesregierung – Drucksache 16/3656 –

Entwurf eines . . . Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (. . . StrÄndG)

A. Problem

Zur strafrechtlichen Bekämpfung der Computerkriminalität sind auf der Ebene des Europarates und der Europäischen Union Rechtsinstrumente entstanden, die zu Umsetzungsbedarf im deutschen Strafrecht führen. So zielt das Übereinkommen des Europarates über Computerkriminalität vom 23. November 2001 neben Vorgaben für das Strafverfahrensrecht, die internationale Zusammenarbeit und zur Rechtshilfe auf einen Mindeststandard bei den Strafvorschriften über bestimmte schwere Formen der Computerkriminalität ab. Der Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme verpflichtet die Mitgliedstaaten ebenfalls, schwere Formen dieser Kriminalität unter Strafe zu stellen. Durch Angleichung der einzelstaatlichen Strafvorschriften gegen Angriffe auf Informationssysteme soll die Zusammenarbeit zwischen den Justiz- und Strafverfolgungsbehörden der Mitgliedstaaten verbessert werden.

B. Lösung

Der Umsetzung dieser Vorgaben dienen verschiedene Gesetzesänderungen im deutschen Recht (Einfügung der §§ 202b und 202c in das Strafgesetzbuch – StGB –, Änderung und Ergänzung der §§ 202a, 303a und 303b StGB, Klarstellung zu § 130 des Gesetzes über Ordnungswidrigkeiten sowie Folgeänderungen im StGB).

Annahme des Gesetzentwurfs mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion DIE LINKE.

C. Alternativen

Keine

D. Kosten

Wurden im Ausschuss nicht erörtert.

Beschlussempfehlung

Der Bundestag wolle beschließen,

den Gesetzentwurf auf Drucksache 16/3656 unverändert anzunehmen.

Berlin, den 23. Mai 2007

Der Rechtsausschuss

Andreas Schmidt (Mülheim)
Vorsitzender

Siegfried Kauder (Villingen-Schwenningen)
Berichterstatter

Sabine Leutheusser-Schnarrenberger
Berichterstatterin

Jerzy Montag
Berichterstatter

Dirk Manzewski
Berichterstatter

Wolfgang Neskovic
Berichterstatter

Bericht der Abgeordneten Siegfried Kauder (Villingen-Schwenningen), Dirk Manzewski, Sabine Leutheusser-Schnarrenberger, Wolfgang Neskovic und Jerzy Montag

I. Überweisung

Der Deutsche Bundestag hat den Gesetzentwurf auf **Drucksache 16/3656** in seiner 73. Sitzung am 14. Dezember 2006 in erster Lesung beraten und dem Rechtsausschuss zur federführenden Beratung sowie dem Innenausschuss und dem Ausschuss für Kultur und Medien zur Mitberatung überwiesen. In seiner 97. Sitzung am 10. Mai 2007 hat der Deutsche Bundestag den Gesetzentwurf nachträglich auch dem Ausschuss für Bildung, Forschung und Technikfolgenabschätzung zur Mitberatung überwiesen.

II. Stellungnahmen der mitberatenden Ausschüsse

Der **Innenausschuss** hat die Vorlage in seiner 41. Sitzung am 23. Mai 2007 beraten und mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion DIE LINKE. beschlossen, zu empfehlen, den Gesetzentwurf auf Drucksache 16/3656 anzunehmen.

Der **Ausschuss für Kultur und Medien** hat die Vorlage in seiner 35. Sitzung am 23. Mai 2007 beraten und mit den Stimmen der Fraktionen der CDU/CSU, SPD und FDP bei Abwesenheit der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN beschlossen, zu empfehlen, den Gesetzentwurf auf Drucksache 16/3656 anzunehmen.

Der **Ausschuss für Bildung, Forschung und Technikfolgenabschätzung** hat in seiner 36. Sitzung am 23. Mai 2007 auf die Abgabe eines Votums verzichtet.

III. Beratungsverlauf und -ergebnis im Rechtsausschuss

Der Rechtsausschuss hat in seiner 43. Sitzung am 17. Januar 2007 beschlossen, zu dem Gesetzentwurf eine öffentliche Anhörung durchzuführen, die am 21. März 2007 (54. Sitzung) stattfand. An der Anhörung haben folgende Sachverständige teilgenommen:

1. Prof. Dr. Borges
   Ruhr-Universität Bochum, Juristische Fakultät
2. Michael Bruns
   Generalbundesanwalt beim Bundesgerichtshof, Karlsruhe
3. Dr. Marco Gercke
   Rechtsanwalt, Köln
4. Dr. Jürgen-Peter Graf
   Richter am Bundesgerichtshof, Karlsruhe
5. Michael Hange
   Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik, Bonn
6. Prof. Dr. Erich Hilgendorf
   Julius-Maximilians-Universität Würzburg
7. Prof. Dr. Hans Kudlich
   Friedrich-Alexander-Universität, Erlangen-Nürnberg, Lehrstuhl für Strafrecht, Strafprozessrecht und Rechtsphilosophie
8. Felix Lindner
   Geschäftsführer von SABRE Labs GmbH, Berlin
9. Dr. Carl-Friedrich Stuckenberg LL.M
   Privatdozent, Universität Bonn, Institut für Strafrecht.

Hinsichtlich der Ergebnisse der Anhörung wird auf das Protokoll der 54. Sitzung des Rechtsausschusses vom 21. März 2007 mit den anliegenden Stellungnahmen der Sachverständigen verwiesen.

Der **Rechtsausschuss** hat den Gesetzentwurf in seiner 64. Sitzung am 23. Mai 2007 abschließend beraten. Er hat mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion DIE LINKE. beschlossen, zu empfehlen, den Gesetzentwurf anzunehmen.

Als Ergebnis der Beratungen hielten die **Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN** fest:

Die technische Entwicklung der vergangenen Jahre habe gezeigt, dass es im Bereich der Computerkriminalität im deutschen Strafrecht durchaus relevante Lücken gebe, deren Schließung der Rahmenbeschluss über Angriffe auf Informationssysteme (2005/222/JI) sowie das Übereinkommen des Europarates über Computerkriminalität vom 23. November 2001 forderten. Die von der Bundesregierung vorgeschlagenen Regelungen seien hierzu grundsätzlich geboten und sachgerecht. In der Anhörung des Rechtsausschusses von Vertretern der IT-Branche vorgetragene Bedenken hinsichtlich des § 202c StGB seien sehr ernsthaft geprüft worden. Der Gesetzentwurf kriminalisiere nicht den branchenüblichen Einsatz von Hacker-Tools durch Netzwerkadministratoren, insbesondere wenn diese nur die Sicherheit des eigenen Datennetzes prüfen wollten. Nach sorgfältiger Prüfung der vorgeschlagenen Regelungen sei der Rechtsausschuss der Auffassung, dass der Gesetzentwurf nicht zu einer Überkriminalisierung führe. Um Missverständnisse zu vermeiden, stelle der Rechtsausschuss klar, dass § 202c StGB hinsichtlich der Zweckbestimmung im Sinne des Artikels 6 des Europarats-Übereinkommens auszulegen sei. Danach seien nur Computerprogramme betroffen, die in erster Linie dafür ausgelegt oder hergestellt würden, um damit Straftaten nach den §§ 202a, 202b StGB zu begehen. Die bloße Geeignetheit zur Begehung solcher Straftaten begründe keine Strafbarkeit. Die geforderte Zweckbestimmung müsse eine Eigenschaft des Computerprogramms in dem Sinne darstellen, dass es sich um sog. Schadsoftware handele (vgl. hierzu den Beschluss des Bundesverfassungsgerichts vom 19. Mai 2006 – 2 BvR 1589/05 –, NJW 2006, S. 2318 f., zu so genannter Verfälschungssoftware bei Tachometermanipulation im Rahmen des § 22b StVG).

Die Strafvorschrift habe in erster Linie professionelle Anbieter im Blick, die durch die Bereitstellung von Computerprogrammen, die für die Begehung von Straftaten geschrieben würden, ein vom Gesetzgeber als unerwünscht und strafbar angesehenes Verhalten unterstützten und damit Gewinn erzielten.

Der Gesetzgeber werde die Auswirkungen der neuen Strafvorschriften genau zu beobachten haben. Sollten doch Programmentwickler und Firmen, die nicht aus krimineller Energie heraus handelten, durch diese neuen Strafvorschriften in Ermittlungsverfahren einbezogen werden, werde auf solche Entwicklungen zeitnah reagiert werden müssen.

Der Rechtsausschuss weise darauf hin, dass es sich bei den §§ 202a und 202b StGB um Antragsdelikte handele.

Der Rechtsausschuss gehe davon aus, dass sogenannte Massen-E-Mail-Proteste nicht den Tatbestand des § 303b StGB erfüllten, sondern ohne Nachteilszufügungsabsicht geschähen und von der Meinungsfreiheit nach Artikel 5 des Grundgesetzes (GG) gedeckt seien.

Die **Fraktion DIE LINKE.** stellte folgenden Änderungsantrag:

Der Bundestag wolle beschließen:

Artikel 1 wird wie folgt geändert:

a) In Nummer 3 wird § 202c wie folgt gefasst:

„§ 202c
Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er Passworte oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, 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.“

b) In Nummer 6 wird § 303b wie folgt gefasst:

„§ 303b
Computersabotage

(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 oder

2. eine Datenverarbeitungsanlage 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 und beeinträchtigt der Täter durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen erheblich, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

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

Begründung

Zu 1.

Durch die Neufassung des § 202c wird der Umgang mit Computerprogrammen, die zu Straftaten nach § 202a oder § 202b geeignet sind, von der Strafdrohung des § 202c ausgenommen. Damit macht der Entwurf von der Möglichkeit des Artikels 6 Absatz 3 des Übereinkommens des Europarates über Computerkriminalität vom 23. November 2001 Gebrauch. Der Gesetzentwurf der Bundesregierung, der demgegenüber eine weitgehende Vorfeldkriminalisierung anstrebt, lässt keine hinreichenden Kriterien erkennen, wie strafwürdige Vorbereitungen von Straftaten nach § 202a oder § 202b von dem sozialethisch nicht zu missbilligenden Umgang mit Programmen, die sich zu solchen Straftaten eignen, abgegrenzt werden können und gerät somit in einen Konflikt mit dem strafrechtlichen Bestimmtheitsgebot aus Art. 103 Abs. 2 GG. Insbesondere ist es entgegen der Begründung des Regierungsentwurfs in der Regel nicht möglich, eine hinreichend bestimmte Abgrenzung durch die objektive Zweckbestimmung des Programms zu erreichen. Die meisten dieser Programme (dual use tools) lassen sich nämlich sowohl zur Begehung der genannten Straftaten als auch zu legitimen Zwecken verwenden, so dass es letztlich der Anwender ist, der den Zweck setzt. Damit sieht sich der Programmierer, sofern er die Möglichkeit einer kriminellen Verwendung seines Programms erkennt, der Gefahr der Strafverfolgung ausgesetzt, obwohl gerade die IT-Sicherheitsbranche, Netzwerkadministratoren und Forschung auf die Herstellung und den Umgang mit solchen Programmen angewiesen sind.

Diese Unsicherheit für die gesamte IT-Sicherheitsbranche hat nicht nur existenzbedrohende Auswirkungen für die in diesem Bereich tätigen klein- und mittelständischen Unternehmen und ihre Angestellten, sie droht darüber hinaus zu einer Senkung des Sicherheitsniveaus in der gesamten deutschen IT-Branche zu führen, weil der Umgang von Programmen, die für Sicherheitstests unabdingbar sind, mit der Gefahr der Strafverfolgung verbunden ist.

Strafbarkeitslücken sind in diesem Zusammenhang schon deshalb nicht ersichtlich, weil durch die anderen Tatbestände des Computerstrafrechts bereits ein angemessener Rechtsgüterschutz verwirklicht ist. Abgesehen von den Bedenken, die schon grundsätzlich gegen exzessive Vorfeldkriminalisierungen bestehen, ist daher auch im konkreten Fall nicht ersichtlich, weshalb eine weit im Vorfeld der eigentlichen Rechtsgutsverletzung eingreifende Strafvorschrift erforderlich sein sollte.

Nach dem Änderungsantrag soll daher auf eine Inkriminierung des genannten Vorfeldbereichs gänzlich verzichtet werden.

Zu 2.

Die Änderung des § 303b Abs. 1 zielt darauf ab, die Neueinführung der Tatbestandsalternative des Eingebens oder Übermittelns von Daten in Nachteilszufügungsabsicht rückgängig zu machen. Die Schaffung dieser Alternative, die an sich neutrale Handlungen wie das Eingeben und Übermitteln von Daten unter Strafe stellt, ist weder von dem Übereinkommen des Europarates über Computerkriminalität noch durch den Rahmenbeschluss des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme gedeckt. Die europäischen Vorgaben setzen nämlich übereinstimmend voraus, dass die pönalisierte Handlung unbefugt begangen werden muss, wovon bei der Eingabe oder Übermittlung von Daten gerade nicht ausgegangen werden

kann. Anlass dafür, den Straftatbestand auch auf neutrale Verhaltensweisen auszudehnen, war vielmehr ein Beschluss des OLG Frankfurt a. M. vom 22.5.2006 (MMR 2006, 547), nach welchem sogenannte Online-Demonstrationen vom geltenden Strafrecht nicht umfasst sind. Um solche Online-Demonstrationen, die die Blockade einer bestimmten Internetseite zur Folge haben können, zu verhindern, soll es nach dem Entwurf der Bundesregierung daher genügen, mit Nachteilszufügungsabsicht die betreffende Seite anzuwählen, um nach Absatz 4 gegebenenfalls zu einer bis zu zehnjährigen Freiheitsstrafe verurteilt zu werden. Dieser Ansatz erscheint aus mehreren Gründen inakzeptabel. Zum einen ist es offensichtlich, dass sich dieses Vorgehen wertungsmäßig in eklatanten Widerspruch zu den Vorgaben des Bundesverfassungsgerichts zur Strafbarkeit sogenannter Sitzblockaden setzt. Bei diesen nämlich macht sich nicht strafbar, wer durch seine bloße Anwesenheit einem anderen die Möglichkeit nimmt, den Raum aufzusuchen oder zu passieren, an dem sich der Teilnehmer der Sitzblockade befindet. Nichts anderes geschieht aber bei einem sogenannten virtuellen Sit-in, auch hier wird derjenige, der eine Internetseite aufsuchen will, daran gehindert, weil mehrere andere Personen, diese schon vor ihm anwählten.

Problematisch ist dabei auch, dass die Inkriminierung dieser neutralen Handlungen letztlich dazu führt, dass allein die Absicht, die ihnen zu Grunde liegt, strafbarkeitsbegründend wirkt, so dass letztlich eine Gesinnung bestraft wird.

Hinzu kommt, dass die Frage, inwieweit Onlinedemonstrationen, die zur Behinderung Dritter führen, grundrechtlich geschützt sind, bisher nicht abschließend geklärt ist, obwohl das Ministerkomitee des Europarates bereits im Mai 2005 die Mitgliedsstaaten dazu aufgerufen hat, die Rahmenbedingungen für Versammlungs- und Vereinigungsfreiheit im Internet zu schaffen (Vgl.: MMR 2005, 863). So hat das Amtsgericht Frankfurt mit Urteil vom 1.7.2005 (MMR 2005, 863) entschieden, weder die Versammlungs-, noch die Meinungsäußerungsfreiheit schütze Onlinedemonstrationen. Dieses Urteil hat das OLG Frankfurt mit Beschluss vom 22.5.2006 aufgehoben, ohne zu der Anwendbarkeit der Kommunikationsrechte Stellung nehmen zu müssen.

Auch im Deutschen Bundestag scheinen sowohl bezüglich des Grundrechtsschutzes virtueller Sit-ins als auch hinsichtlich deren Strafwürdigkeit diametral entgegengesetzte Ansichten zu herrschen. So hat der ehemalige Bundesinnenminister Schily erwogen, Naziinternetauftritte auf die gleiche Art und Weise zu blockieren, wie es im Falle einer Onlinedemonstration erfolgen kann.

Der Abgeordnete Jörg Tauss, Beauftragter für Neue Medien der SPD-Bundestagsfraktion, hat wiederholt zum virtuellen Protest gegen das dem Gesetzentwurf der Bundesregierung zu Grunde liegende Cybercrime-Abkommen des Europarats aufgefordert, das seiner Meinung nach die Befugnisse der Strafverfolger auf Kosten von Bürgerrechten zu stark ausweitet (Quelle: http://www.heise.de/tp/r4/artikel/7/7907/1.html).

Sierk Hamann, Richter und Experte rund ums Online-Recht aus den Reihen der FDP, äußerte die Ansicht, dass sogar DDoS-Attacken durchaus „im Lichte der Grundrechte" gesehen werden müssten. Statt auf Artikel 8 stützt er sich dabei allerdings auf Artikel 5 des Grundgesetzes, der die allgemeine Meinungsfreiheit garantiert. Auch im Internet gelte: „Eine Demonstration ist immer ein Bündel von Grundrechten." (Quelle: http://www.heise.de/tp/r4/artikel/7/7907/1.html).

Die von der Bundesregierung geplante Einführung der neuen Tatbestandsalternative droht die Frage nach der Strafbarkeit von Onlinedemonstrationen zu entscheiden, ohne dabei auf die auch im Internet zu berücksichtigenden Grundrechte der Normunterworfenen angemessen Rücksicht zu nehmen.

Die weiteren Änderungen der Absätze 2 bis 4 zielen darauf ab, die Verhältnismäßigkeit der Strafdrohungen zu wahren und diese nicht gänzlich aus dem Rahmen der übrigen Sachbeschädigungsdelikte ausscheren zu lassen. Eine Freiheitsstrafe von bis zu zehn Jahren erscheint in diesem Bereich grundsätzlich unverhältnismäßig. Auch die Anknüpfungspunkte, die zu einer Indizwirkung für das Vorliegen eines besonders schweren Falls führen, verkennen die Realitäten des Internets. So ist der Eintritt eines Vermögensverlustes großen Ausmaßes von multiplen Faktoren aus der Sphäre des Verletzten abhängig, die für den Täter weder erkennbar noch zu beeinflussen sind. Insoweit erscheint es nicht sachgerecht in der Höhe des Vermögensverlustes ein schuldsteigerndes Merkmal zu sehen. Auch hinsichtlich der anderen Regelbeispiele ist eine Strafdrohung von drei Jahren als ausreichend anzusehen. Lediglich für den Fall, dass durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen erheblich beeinträchtigt wird, erscheint eine Erhöhung des Strafrahmens angezeigt. Die Voraussetzung der erheblichen Beeinträchtigung stellt sicher, dass eine Strafbarkeit nach Absatz 2 nur bei spürbaren Versorgungseinbußen der Bevölkerung und nicht bei bloßen Beeinträchtigungen des Angebots solcher Güter und Dienstleistungen in Betracht kommt.

Der Änderungsantrag der Fraktion DIE LINKE. wurde mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion DIE LINKE. abgelehnt.

Berlin, den 23. Mai 2007

Siegfried Kauder (Villingen-Schwenningen)
Berichterstatter

Dirk Manzewski
Berichterstatter

Sabine Leutheusser-Schnarrenberger
Berichterstatterin

Wolfgang Neskovic
Berichterstatter

Jerzy Montag
Berichterstatter

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333