Deutscher Bundestag **Drucksache 16/3656**

16. Wahlperiode 30. 11. 2006

Gesetzentwurf

der Bundesregierung

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

A. Problem und Ziel

Die rasanten Fortschritte im Bereich der Informationstechnologie bieten ein breites Spektrum neuer Möglichkeiten, aber auch des Missbrauchs, der vor den Grenzen der Staaten nicht haltmacht. Deshalb entstanden auf der Ebene des Europarates und der Europäischen Union Rechtsinstrumente, die der strafrechtlichen Bekämpfung der Computerkriminalität dienen und die zu Umsetzungsbedarf im deutschen Strafrecht führen:

1. Das Übereinkommen des Europarates über Computerkriminalität vom 23. November 2001 zielt auf einen Mindeststandard bei den Strafvorschriften über bestimmte schwere Formen der Computerkriminalität ab. Darüber hinaus enthält es Vorgaben für das Strafverfahrensrecht, die internationale Zusammenarbeit und zur Rechtshilfe.
2. Der Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme (ABl. EU Nr. L 69 S. 67) verpflichtet die Mitgliedstaaten der Europäischen Union ebenfalls, schwere Formen der Computerkriminalität unter Strafe zu stellen. Durch Angleichung der einzelstaatlichen Strafvorschriften gegen Angriffe auf Informationssysteme soll die Zusammenarbeit zwischen den Justiz- und Strafverfolgungsbehörden verbessert werden.

B. Lösung

Der Umsetzung der Vorgaben zum materiellen Strafrecht des Europarat-Übereinkommens und der Vorgaben des Rahmenbeschlusses in nationales Recht 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).

C. Alternativen

Keine

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugsaufwand

Keine

2. Vollzugsaufwand

Aufgrund der Ausdehnung des deutschen Strafrechts ist zu erwarten, dass die Anzahl der Strafverfahren in einem begrenzten Ausmaß zunimmt. Dies kann zu nicht näher quantifizierbaren Haushaltsmehrausgaben bei den für die Durchführung von Strafverfahren primär zuständigen Strafverfolgungsbehörden der Länder führen. Im Zuständigkeitsbereich des Bundes anfallende Haushaltsmehrausgaben sind allenfalls im geringen Umfang zu erwarten. Soweit Mehrkosten im Bereich der Strafverfolgung beim Bund entstehen, wird dieser Mehraufwand innerhalb des Einzelplans 07 gegenfinanziert.

E. Sonstige Kosten

Für die Wirtschaft entstehen durch dieses Gesetz bei normgemäßem Verhalten keine Kosten. Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere das Verbraucherpreisniveau, sind in der Regel nicht zu erwarten.

BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

Berlin, 29. November 2006

An den
Präsidenten des
Deutschen Bundestages
Herrn Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich den von der Bundesregierung beschlossenen

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

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium der Justiz.

Der Bundesrat hat in seiner 827. Sitzung am 3. November 2006 gemäß Artikel 76 Absatz 2 des Grundgesetzes beschlossen, zu dem Gesetzentwurf wie aus Anlage 2 ersichtlich Stellung zu nehmen.

Die Auffassung der Bundesregierung zu der Stellungnahme des Bundesrates ist in der als Anlage 3 beigefügten Gegenäußerung dargelegt.

Mit freundlichen Grüßen

Anlage 1

Entwurf eines … Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (… StrÄndG)[1]

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1
Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch … (BGBl. I S. …) wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   Nach der Angabe zu § 202a werden die Wörter „§ 202b Abfangen von Daten“ und „§ 202c Vorbereiten des Ausspähens und Abfangens von Daten“ eingefügt.

2. § 202a Abs. 1 wird wie folgt gefasst:

   „(1) 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.“

3. Nach § 202a werden die folgenden §§ 202b und 202c eingefügt:

   „§ 202b
   Abfangen von Daten

   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.

   § 202c
   Vorbereiten des Ausspähens und Abfangens von Daten

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

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

4. § 205 wird wie folgt geändert:

   a) Absatz 1 wird wie folgt geändert:

      aa) Die Angabe „bis 204“ wird durch die Angabe „, 202, 203 und 204“ ersetzt.

      bb) Folgender Satz wird angefügt:

      „Dies gilt auch in den Fällen der §§ 202a und 202b, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.“

   b) In Absatz 2 Satz 1 wird die Angabe „des § 202a“ durch die Angabe „der §§ 202a und 202b“ ersetzt.

5. Dem § 303a wird folgender Absatz 3 angefügt:

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

6. § 303b wird wie folgt geändert:

   a) Absatz 1 wird durch die folgenden Absätze 1 und 2 ersetzt:

      „(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.

      (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.“

   b) Der bisherige Absatz 2 wird Absatz 3.

   c) Die folgenden Absätze 4 und 5 werden angefügt:

      „(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,

1 Dieses Gesetz dient der Umsetzung des Übereinkommens des Europarates über Computerkriminalität und der Umsetzung des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme (ABl. EU Nr. L 69 S. 67).

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.“

7. In § 303c wird die Angabe „bis 303b“ durch die Wörter „, 303a Abs. 1 und 2 sowie § 303b Abs. 1 bis 3“ ersetzt.

Artikel 2

Änderung des Gesetzes über Ordnungswidrigkeiten

In § 130 Abs. 1 Satz 1 des Gesetzes über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), das zuletzt durch … (BGBl. I S. …) geändert worden ist, werden die Wörter „als solchen“ gestrichen.

Artikel 3

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I.

Die immer stärkere Verbreitung und Nutzung von Informations- und Kommunikationstechnologien, insbesondere die Nutzung des Internets, wirken sich unmittelbar auf alle Bereiche der Gesellschaft aus. Die Einbeziehung von Telekommunikations- und Informationssystemen, die eine entfernungsunabhängige Speicherung und Übertragung von Daten aller Art gestatten, bieten ein breites Spektrum neuer Möglichkeiten, aber auch des Missbrauchs. Insbesondere komplexe Attacken gegen moderne Informationsstrukturen durch Computerviren, digitale trojanische Pferde, logische Bomben oder Würmer und Denial-of-Service-Attacken verursachen hohe Schäden. Auch kriminelle, extremistische und terroristische Gruppen nutzen moderne Informations- und Kommunikationstechnologien verstärkt für ihre Zwecke.

Computerkriminalität weist schon seit längerem internationale Dimensionen auf. Insbesondere das weltumspannende Internet stellt eine neue Herausforderung für Strafverfolgungsbehörden im In- und Ausland dar. Gerade im Internet werden die Taten vielfach grenzüberschreitend begangen, was als Folge die Lokalisierung und Identifizierung von Straftaten erschwert. Häufig nutzen dabei Straftäter auch Unterschiede in den nationalen Rechtsordnungen aus, um der Strafverfolgung und Bestrafung zu entgehen oder diese zumindest erheblich zu behindern.

Daher wurden in den letzten Jahren sowohl im Rahmen des Europarates als auch auf Ebene der Europäischen Union strafrechtsbezogene Rechtsinstrumente beschlossen, die der Bekämpfung der Computerkriminalität dienen:

1. Das von Deutschland am 23. November 2001 gezeichnete und am 1. Juli 2004 in Kraft getretene Übereinkommen des Europarates über Computerkriminalität (Europarat-Übereinkommen; ETS-Nummer 185) hat zum Ziel, einen gemeinsamen strafrechtlichen Mindeststandard zu schaffen, um einerseits Computerdaten und -systeme gegen Angriffe auf ihre Vertraulichkeit, Integrität und Verfügbarkeit zu schützen und andererseits ihrem Missbrauch zur Begehung von Straftaten entgegenzuwirken. Darüber hinaus enthält es Vorgaben für das Strafverfahrensrecht, die internationale Zusammenarbeit und zur Rechtshilfe.
2. Der Rahmenbeschluss des Rates der Europäischen Union über Angriffe auf Informationssysteme (EU-Rahmenbeschluss) vom 24. Februar 2005 (ABl. EU Nr. L 69 S. 67), der sich auf die Bestimmungen des Titels VI des Vertrags über die Europäische Union (insbesondere die Artikel 29, 30 Abs. 1 Buchstabe a, Artikel 31 Abs. 1 Buchstabe e und Artikel 34 Abs. 2 Buchstabe b) in der Fassung vom 16. April 2003 (BGBl. 2003 II S. 1410) stützt, lehnt sich inhaltlich bei den zu harmonisierenden Straftatbeständen eng an das Europarat-Übereinkommen an, wenn auch in einigen Tatbeständen eine abweichende Terminologie verwendet wird. Durch Angleichung der einzelstaatlichen Strafvorschriften gegen Angriffe auf Informationssysteme soll die Zusammenarbeit zwischen den Justiz- und Strafverfolgungsbehörden in den Mitgliedstaaten verbessert werden. Der EU-Rahmenbeschluss verpflichtet die Mitgliedstaaten, schwere Formen der Computerkriminalität unter Strafe zu stellen, und führt hierfür strafrechtliche Mindeststandards ein.

II.

Mit diesem Gesetzesentwurf werden Änderungen im materiellen deutschen Strafrecht zur Umsetzung des EU-Rahmenbeschlusses und der Vorgaben zum materiellen Strafrecht – mit Ausnahme der Vorgaben zu inhaltsbezogenen Straftaten (Titel 3 des Europarat-Übereinkommens) – vorgeschlagen. Die Vorgaben des Europarat-Übereinkommens mit Bezug zu Kinderpornographie (Artikel 9 des Europarat-Übereinkommens) werden durch den Entwurf eines Gesetzes zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie umgesetzt. Die Umsetzung der Vorgaben hinsichtlich des Strafprozessrechts erfolgt im Rahmen eines gesonderten Gesetzesvorhabens.

Das deutsche Strafrecht entspricht den Vorgaben zum materiellen Strafrecht des Europarat-Übereinkommens und den Vorgaben des EU-Rahmenbeschlusses bereits weitgehend. Änderungen sind nur in Teilbereichen erforderlich. Ein Umsetzungsbedarf besteht lediglich – neben der erforderlichen Umsetzung von Artikel 9 – im Hinblick auf die Artikel 2, 3, 5 und 6 des Europarat-Übereinkommens und die Artikel 2 und 3 des EU-Rahmenbeschlusses; im Rahmen der Umsetzung von Artikel 12 Abs. 2 des Europarat-Übereinkommens und Artikel 8 Abs. 2 des EU-Rahmenbeschlusses soll zudem eine Klarstellung im deutschen Recht erfolgen:

1. Artikel 2 des Europarat-Übereinkommens und Artikel 2 des EU-Rahmenbeschlusses schreiben die Strafbarkeit des rechtswidrigen Zugangs zu einem Computer- und Informationssystem (so genanntes Hacking) vor. Vorgeschlagen wird daher eine Anpassung des § 202a StGB (Ausspähen von Daten). Zwar erfasst dieser Tatbestand faktisch schon heute vielfach das Hacking, also das „Knacken“ eines Informationssystems, da der Täter sich hierbei regelmäßig auch Daten verschafft. Geregelt werden soll jetzt, dass bereits der bloße Zugang zu besonders gesicherten Daten unter Überwindung von Sicherheitsmaßnahmen strafbar ist, wenn dies unbefugt geschieht.
2. Artikel 3 des Europarat-Übereinkommens enthält die Verpflichtung, das unbefugte Abfangen nichtöffentlicher Computerdatenübermittlung an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschließlich elektromagnetischer Abstrahlung aus einem Computersystem unter Strafe zu stellen. Vorgeschlagen wird ein Straftatbestand über das Abfangen von Daten (§ 202b StGB), um künftig alle nichtöffentlichen Übermittlungen auch von solchen Daten zu erfassen, die nicht durch Sicherheitsvorkehrungen besonders geschützt sind.

3. Artikel 5 des Europarat-Übereinkommens und Artikel 3 des EU-Rahmenbeschlusses enthalten die Verpflichtung, rechtswidrige Eingriffe in ein Computer- und Informationssystem unter Strafe zu stellen. Der Straftatbestand der Computersabotage (§ 303b StGB) bedarf hier der Ergänzung, da er in seiner bisherigen Fassung nur Datenverarbeitungen von fremden Unternehmen oder Behörden schützt. Künftig sollen auch private Datenverarbeitungen von wesentlicher Bedeutung erfasst werden. Außerdem ist eine Ausweitung der Tathandlungen erforderlich, da Störungshandlungen durch unbefugtes „Eingeben“ und „Übermitteln“ von Computerdaten bislang nicht strafbar sind. Über die Umsetzung dieser Rechtsinstrumente hinaus soll eine benannte Strafzumessungsregel für besonders schwere Fälle der Computersabotage vorgesehen werden.

4. Artikel 6 des Europarat-Übereinkommens schreibt die Strafbarkeit von bestimmten Vorbereitungshandlungen für Computerstraftaten nach den Artikeln 2 bis 5 des Europarat-Übereinkommens vor. Ein Tatbestand, der Vorbereitungshandlungen zur Begehung von Computerstraftaten erfasst, existiert im deutschen Strafgesetzbuch nur für den Computerbetrug (§ 263a Abs. 3 StGB). Vorgeschlagen wird daher, mit einem neuen § 202c StGB auch Vorbereitungshandlungen zum Ausspähen von Daten (§ 202a StGB) und Abfangen von Daten (§ 202b StGB – neu) unter Strafe zu stellen. Durch Verweisungen auf diesen Tatbestand sollen auch Vorbereitungshandlungen zu Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB) künftig strafbar sein (§ 303a Abs. 3 und § 303b Abs. 4 StGB).

5. Nach Artikel 8 Abs. 2 des EU-Rahmenbeschlusses muss eine juristische Person grundsätzlich auch dann verantwortlich gemacht werden können, wenn mangelnde Überwachung oder Kontrolle einer Leitungsperson dieser juristischen Person die Begehung der in den Artikeln 2 bis 5 genannten Straftaten zugunsten der juristischen Person durch eine ihr unterstellte Person ermöglicht haben. Eine entsprechende Vorgabe enthält Artikel 12 Abs. 2 des Europarat-Übereinkommens im Hinblick auf die dort umschriebenen Delikte. Durch die vorgesehene Streichung der Wörter „als solchen“ in § 130 Abs. 1 Satz 1 des Ordnungswidrigkeitengesetzes (OWiG) soll im Einklang mit der herrschenden Meinung klargestellt werden, dass § 130 OWiG nicht nur Sonderdelikte erfasst, sondern – ebenso wie § 30 OWiG – auch Allgemeindelikte, wenn sie im Zusammenhang mit der Betriebs- oder Unternehmensführung stehen und daher auch die §§ 202a, 202b, 202c, 303a und 303b StGB taugliche Anknüpfungstaten für eine Verantwortlichkeit nach den §§ 30, 130 OWiG sein können.

III.

Den übrigen Vorgaben des EU-Rahmenbeschlusses genügt das geltende Recht bereits heute:

1. Die Verpflichtung aus Artikel 4 des EU-Rahmenbeschlusses, rechtswidrige Eingriffe in Daten unter Strafe zu stellen, ist durch § 303a StGB abgedeckt.

2. Die Verpflichtung aus Artikel 5 Abs. 1 des EU-Rahmenbeschlusses (Strafbarkeit der Anstiftung und Beihilfe) wird aufgrund der im deutschen Recht nicht deliktsspezifisch ausgestalteten §§ 26, 27 StGB erfüllt.

3. Die Verpflichtung zur Einführung der Versuchsstrafbarkeit in Artikel 5 Abs. 2 des EU-Rahmenbeschlusses ist im deutschen Recht ebenfalls erfüllt, da § 303a Abs. 2 und § 303b Abs. 2 (künftig: Abs. 3) StGB diese bereits vorsehen. Von der Möglichkeit, Artikel 5 Abs. 2 des EU-Rahmenbeschlusses nicht auf die Straftaten nach Artikel 2 des EU-Rahmenbeschlusses anzuwenden, wird Gebrauch gemacht (vgl. Artikel 5 Abs. 3 des EU-Rahmenbeschlusses). Für den rechtswidrigen Zugang zu einem Informationssystem soll keine Versuchsstrafbarkeit vorgesehen werden.

4. Die Verpflichtung zur Einhaltung bestimmter Mindesthöchststrafen in Artikel 6 des EU-Rahmenbeschlusses führt nicht zu einem Umsetzungsbedarf, da die §§ 202a, 303a und 303b StGB eine Freiheitsstrafe von mindestens einem Jahr im Höchstmaß vorsehen.

5. Die Verpflichtung aus Artikel 7 des EU-Rahmenbeschlusses zur höheren Bestrafung bei bestimmten erschwerenden Umständen führt ebenfalls nicht zu einem Umsetzungsbedarf, da die im EU-Rahmenbeschluss bezeichneten Delikte ohnehin eine Freiheitsstrafe von mindestens zwei Jahren im Höchstmaß vorsehen.

6. Die Artikel 8 und 9 des EU-Rahmenbeschlusses (Verantwortlichkeit und Sanktionen bei juristischen Personen) sind – abgesehen von der zu § 130 OWiG vorgesehenen Klarstellung – durch die §§ 30, 130 OWiG abgedeckt.

7. Die Verpflichtungen aus Artikel 10 des EU-Rahmenbeschlusses (gerichtliche Zuständigkeit) werden im Wesentlichen durch § 3 ff. StGB abgedeckt. Artikel 10 Abs. 1 Buchstabe a des EU-Rahmenbeschlusses wird durch § 3 in Verbindung mit § 9 StGB erfüllt (Territorialitätsprinzip). In Artikel 10 Abs. 1 Buchstabe b des EU-Rahmenbeschlusses ist das Nationalitätsprinzip geregelt. Im deutschen Recht sind Auslandstaten Deutscher, die zur Tatzeit am Tatort mit Strafe bedroht sind oder dort keiner Strafgewalt unterliegen, strafbar (§ 7 Abs. 2 Nr. 1 StGB). Von der Möglichkeit des Artikels 10 Abs. 5 des EU-Rahmenbeschlusses, die Zuständigkeitsregeln des Artikels 10 Abs. 1 Buchstabe b und c nicht oder nur in bestimmten Fällen oder unter bestimmten Umständen anzuwenden, wird Gebrauch gemacht. Die Zuständigkeitsregel in Artikel 10 Abs. 1 Buchstabe b ist bei Taten von Deutschen, die außerhalb Deutschlands begangen wurden, nur in Fällen anzuwenden, wenn die Tat zur Tatzeit am Tatort mit Strafe bedroht ist oder dort keiner Strafgewalt unterliegt. Die Zuständigkeitsregel in Artikel 10 Abs. 1 Buchstabe c, die eine Begründung der Zuständigkeit für Fälle vorsieht, in denen die Straftat zugunsten einer juristischen Person mit Sitz im Hoheitsgebiet dieses Mitgliedstaats begangen wurde, ist nicht anzuwenden.

IV.

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 74 Abs. 1 Nr. 1 des Grundgesetzes (Strafrecht).

V.

Die Erweiterung des materiellen Strafrechts lässt zwar erwarten, dass die Anzahl der Strafverfahren zunehmen wird. Dies kann zu nicht näher quantifizierbaren Haushaltsmehrausgaben bei den für die Durchführung von Strafverfahren primär zuständigen Strafverfolgungsbehörden der Länder führen. Im Zuständigkeitsbereich des Bundes anfallende Haushaltsmehrausgaben sind allenfalls im geringen Umfang zu erwarten. Soweit Mehrkosten im Bereich der Strafverfolgung beim Bund entstehen, wird dieser Mehraufwand innerhalb des Einzelplans 07 gegenfinanziert.

Für die Wirtschaft, insbesondere für die mittelständischen Unternehmen, entstehen bei regelkonformem Verhalten keine zusätzlichen Kosten. Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten. Da Computerkriminalität zu hohen Schäden führt, kann eine stärkere Bekämpfung vielmehr dazu beitragen, Schäden und somit auch Kosten zu vermeiden. Mittelbar preisrelevante Effekte aufgrund des erforderlichen, aber geringfügigen (Gegen-)Finanzierungsaufwandes sind nicht zu erwarten, da die öffentlichen Haushalte allenfalls durch den leicht gestiegenen Vollzugsaufwand belastet werden.

VI.

Der Entwurf hat keine erkennbaren gleichstellungspolitischen Auswirkungen. Grundsätzlich sind weibliche und männliche Personen von den Vorschriften des Entwurfs in gleicher Weise betroffen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Strafgesetzbuches)

Zu Nummer 1 (Inhaltsübersicht)

Es handelt sich um redaktionelle Folgeänderungen zur Einfügung der §§ 202b und 202c StGB.

Zu Nummer 2 (§ 202a StGB)

1. Die Neufassung des Absatzes 1 dient der Umsetzung von Artikel 2 des Europarat-Übereinkommens (Rechtswidriger Zugang) und Artikel 2 des EU-Rahmenbeschlusses (Rechtswidriger Zugang zu Informationssystemen) in innerstaatliches Recht. Danach ist der unbefugte Zugang zu einem Computer- und Informationssystem als Ganzem oder zu einem Teil davon unter Strafe zu stellen (so genanntes Hacking).

   Der Gesetzentwurf schlägt vor, in Absatz 1 bereits den unbefugten Zugang zu Daten zur strafbaren Handlung zu erklären. Nach der Neufassung macht sich strafbar, wer sich oder einem anderen Zugang zu Daten verschafft, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind. Ein Sichverschaffen von Daten wird künftig nicht mehr erforderlich sein.

2. Nach dem ausdrücklichen Willen des Gesetzgebers sollte die Vorschrift des § 202a StGB, die durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986 (2. WiKG; BGBl. I S. 721) in das Strafgesetzbuch eingefügt wurde, das bloße Hacking, also den reinen Zugang zu Daten, nicht erfassen. Zur Vermeidung einer Überkriminalisierung sollte die Vorschrift nur eingreifen, wenn das Eindringen in ein Computersystem mit einem Ab-/Aufrufen von Daten verbunden ist (vgl. Beschlussempfehlung und Bericht des Rechtsausschusses, Bundestagsdrucksache 10/5058, S. 28 f.). Zur Begründung wurde angeführt, dass das bloße Eindringen ohne ein Sichverschaffen der Daten noch keine Rechtsgutsbeeinträchtigung begründe (vgl. Beschlussempfehlung und Bericht, a. a. O., S. 28).

   Die herrschende Meinung legt das „Sichverschaffen von Daten“ in § 202a StGB jedoch weit aus, so dass das Hacking faktisch bereits heute – entgegen der Absicht des Gesetzgebers – in weitem Umfang erfasst ist. So soll für die Verwirklichung des Tatbestandes jede Kenntnisnahme von Daten genügen; bei verschlüsselten Daten gelte dies jedenfalls dann, wenn sie entschlüsselbar sind (vgl. Tröndle/Fischer, StGB, 53. Aufl., § 202a Rn. 10; Schönke/Schröder-Lenckner, StGB, 27. Aufl., § 202a Rn. 10; MünchKomm-Graf, StGB, § 202a Rn. 47).

   Für die Strafwürdigkeit des Hacking wird auf die Gefahr des Eintritts von möglicherweise nur mit erheblichem Aufwand zu beseitigenden Schäden, auf Gefahren für die Integrität von Daten und Programmen sowie auf die Gefahr der Begehung von durch ein solches Eindringen möglichen weiteren Straftaten hingewiesen. Ausgehend vom geschützten Rechtsgut – dem formellen Geheimhaltungsinteresse des Verfügungsberechtigten (vgl. Bundestagsdrucksache 10/5058, S. 28 f.) – erscheine es schwierig nachzuvollziehen, dass durch das Hacking keine Rechtsgutbeeinträchtigung eintrete. In jedem Falle werde die „formale Geheimsphäre“ oder die Integrität des betreffenden Computersystems beeinträchtigt (vgl. Sieber, CR 1995, 100, 103; Dannecker, BB 1996, 1285, 1289; ähnlich Schulze-Heimig, Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls – 1995 –, S. 82 f.; Jessen, Zugangsberechtigung und besondere Sicherung im Sinne von § 202a StGB – 1994 –, S. 184). In der Praxis sei darüber hinaus ein Eindringen ohne Kenntnisnahme der Zieldateien als unwahrscheinlich anzusehen (so auch Tröndle/Fischer, a. a. O., § 202a Rn. 11; Schönke/Schröder-Lenckner, a. a. O., § 202a Rn. 10; Jessen, a. a. O., S. 180; Hauptmann, jur-pc 1989, 215, 216: eine Trennung zwischen Eindringen und Aufrufen der Daten sei technisch nicht möglich).

   Die neue Vorschrift („sich Zugang verschaffen“) mit ihrer vorverlagerten Strafbarkeit trifft das eigentliche Unrecht besser als das geltende Recht („sich Daten verschaffen“). Im Wesentlichen hat sie bezüglich der bereits herrschenden Auslegung des bisherigen § 202a StGB nur eine Klarstellungsfunktion. Die generelle Gefährlichkeit und Schädlichkeit von Hacking-Angriffen zeigen sich vor allem in jüngster Zeit auch in Deutschland (z. B. durch den Einsatz von Key-Logging-Trojanern, Sniffern oder Backdoorprogrammen), weshalb an ihrer Strafwürdigkeit und -bedürftigkeit keine Zweifel bestehen.

3. Der Tatbestand soll – im Anschluss an das geltende Recht – dadurch eingeschränkt werden, dass nur der Zugang zu Daten erfasst wird, die nicht für den Täter be-

stimmt und die gegen unberechtigten Zugang besonders gesichert sind. Zudem soll – klarstellend – vorgesehen werden, dass nur solches Verhalten strafbar ist, bei dem das Verschaffen unter Überwindung einer Zugangssicherung erfolgt. Diese Einschränkungsmöglichkeit ist durch Artikel 2 Satz 2 des Europarat-Übereinkommens und Artikel 2 Abs. 2 des EU-Rahmenbeschlusses ausdrücklich vorgesehen.

Der Einschränkung auf solche Daten, die gegen unberechtigten Zugang besonders gesichert sind, kommt eine besondere Bedeutung für die Eingrenzung des Tatbestandes zu. Daten sind gegen unberechtigten Zugang besonders gesichert, wenn Vorkehrungen getroffen sind, den Zugriff auf Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren (Schönke/Schröder-Lenckner, a. a. O., § 202a Rn. 7; Lackner/Kühl, StGB, 25. Aufl., § 202a Rn. 4; MünchKomm-Graf, a. a. O., § 202a Rn. 31). Dies braucht zwar nicht ihr einziger Zweck zu sein. Jedenfalls aber muss der Berechtigte durch die Sicherung gerade auch sein spezielles Interesse an der Geheimhaltung dokumentieren (Bundestagsdrucksache 10/5058, S. 29; Schönke/Schröder-Lenckner, a. a. O., § 202a Rn. 7 m. w. N.). Daher muss die besondere Sicherung den Zweck haben, den Zugang zu verhindern (LK-Schünemann, StGB, 11. Aufl., § 202a Rn. 15). Nicht ausreichend ist es, wenn die Sicherung, mag sie auch objektiv zugleich als Zugangssicherung wirken, ausschließlich anderen Zwecken dient oder der Zweck der Datensicherung nur von ganz untergeordneter Bedeutung oder ein bloßer Nebeneffekt ist. Ausgegrenzt werden auch die Fälle, in denen sich der Geheimhaltungswille des Berechtigten nicht auf die im System enthaltenen Daten bezieht, sondern in denen lediglich eine unbefugte Verwendung der Hardware unterbunden werden soll. Nicht erfasst werden daher die bloße Ingebrauchnahme von verschlossenen elektronischen Geräten gegen den Willen des Berechtigten und die Umgehung eines Kopierschutzes.

Dass darüber hinaus zur Tatbestandserfüllung die Überwindung der Zugangssicherung erforderlich ist, wird von der herrschenden Meinung in der Literatur bereits für den bisherigen Tatbestand angenommen, wobei dies zum Teil aus dem Sinnzusammenhang der Norm geschlossen wird (vgl. Schönke/Schröder-Lenckner, a. a. O., § 202a Rn. 10; LK-Schünemann, a. a. O., § 202a Rn. 7; MünchKomm-Graf, a. a. O., § 202a Rn. 48; Hilgendorf, JuS 1996, 702, 704). Hierdurch sollen Handlungen ausgegrenzt werden, bei denen besonders gesicherte Daten auf andere Weise erlangt werden. Dieses Erfordernis soll auch für das Zugangsdelikt übernommen werden.

Diese Einschränkung führt zudem dazu, dass Bagatellfälle aus dem Anwendungsbereich des Straftatbestandes herausgehalten werden. Das Merkmal der Zugangssicherung setzt dem Täter eine deutliche Schranke; die Überwindung der Sicherung manifestiert die strafwürdige kriminelle Energie (LK-Schünemann, a. a. O., § 202a Rn. 7 und 14 m. w. N.). Eine Schutzvorkehrung ist nur dann eine Zugangssicherung im Sinne des § 202a, wenn sie jeden Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte (Tröndle/Fischer, a. a. O., § 202a, Rn. 8). Nicht erfasst werden daher Fälle, in denen dem Angreifer die Durchbrechung des Schutzes ohne weiteres möglich ist (MünchKomm-Graf, a. a. O., § 202a Rn. 28; Tröndle/Fischer, a. a. O., § 202a Rn. 8). Erforderlich ist vielmehr, dass die Überwindung der Zugangssicherung einen nicht unerheblichen zeitlichen oder technischen Aufwand erfordert (LK-Schünemann, a. a. O., § 202a Rn. 15). Auch die Verletzung oder Umgehung von organisatorischen Maßnahmen oder Registrierungspflichten erfüllt grundsätzlich nicht den Tatbestand (LK-Schünemann, a. a. O., § 202a Rn. 14; MünchKomm-Graf, a. a. O., § 202a Rn. 21 und 31; Sieber in Hoeren/Sieber, Handbuch Multimediarecht, 2004, 19 Rn. 420). Der Fall, dass sich ein Täter ohne ordnungsgemäßen Anschluss Zugang zu entgeltlichen Datenbanken verschafft, wird allerdings von § 202a erfasst (Bundestagsdrucksache 10/5058, S. 29).

Auch nach der Neufassung des Tatbestandes ist die Verschaffung des Zugangs zu Daten unter Verletzung von Sicherheitsmaßnahmen nur strafbewehrt, wenn der Täter unbefugt handelt. Nicht strafbar ist daher z. B. das Aufspüren von Sicherheitslücken im EDV-System eines Unternehmens, soweit der „Hacker“ vom Inhaber des Unternehmens mit dieser Aufgabe betraut wurde.

Wie beim bisherigen Tatbestand soll es nicht erforderlich sein, dass es sich bei den geschützten Daten um Computerdaten handelt, also solche, die in einer EDV-Anlage gespeichert oder in eine solche oder aus einer solchen übermittelt werden (zum bisherigen § 202a: Möhrenschlager, wistra 1986, 128, 140). Insoweit geht die vorgeschlagene Vorschrift über die Vorgaben des Europarat-Übereinkommens und des EU-Rahmenbeschlusses hinaus, die auf den Zugang zu einem Computer- und Informationssystem abstellen.

4. Trotz der Herabsetzung der Schwelle zur Tatbestandsverwirklichung soll die Strafhöhe nicht herabgesetzt werden, da auch der Fall des Sichverschaffens von Daten von der Neufassung des § 202a StGB erfasst wird. Die Anforderungen der Artikel 6 und 7 des EU-Rahmenbeschlusses an die Mindesthöchststrafe werden eingehalten.

5. Eine Versuchsstrafbarkeit wird angesichts der ohnehin geringen Schwelle zur Verwirklichung des Tatbestandes nicht vorgeschlagen. Hierbei wird von der Möglichkeit in Artikel 5 Abs. 3 des EU-Rahmenbeschlusses Gebrauch gemacht, Artikel 5 Abs. 2 mit seiner Verpflichtung zur Einführung der Strafbarkeit des Versuchs nicht anzuwenden.

Zu Nummer 3 (§§ 202b und 202c StGB)

Zu § 202b StGB (Abfangen von Daten)

Der neue § 202b StGB setzt Artikel 3 des Europarat-Übereinkommens (Rechtswidriges Abfangen) um. Artikel 3 gibt den Vertragsstaaten vor, das mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen an, aus oder innerhalb eines Computersystems einschließlich elektromagnetischer Abstrahlungen aus einem Computersystem, das Träger solcher Computerdaten ist, unter Strafe zu stellen.

1. Der Gesetzentwurf schlägt daher vor, in § 202b StGB das Sichverschaffen von Daten aus einer nichtöffentlichen Datenübermittlung und aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Anwen-

dung technischer Mittel unter Strafe zu stellen. Diese Vorschrift stellt das elektronische Pendant zu dem Abhören und Aufzeichnen von Telefongesprächen dar. Erfasst werden alle Formen der elektronischen Datenübermittlung. Hierzu gehören u. a. E-Mail, Fax und Telefon. Tatobjekt sind nur Daten, die sich zur Zeit der Tat in einem Übertragungsvorgang befinden. Gespeicherte Daten, die zu einem früheren Zeitpunkt übermittelt wurden, fallen nicht hierunter. Da Daten nicht nur bei einem Übermittlungsvorgang abgefangen, sondern auch aus elektromagnetischen Abstrahlungen aus Computersystemen wiederhergestellt werden können, werden solche Tathandlungen ausdrücklich erfasst.

§ 202b StGB trägt dem technischen Fortschritt Rechnung, da die gängigen Kommunikationsformen heutzutage nicht mehr auf das herkömmliche Telefon beschränkt sind. Das bisher geltende Recht erfasst diese Fälle nur fragmentarisch. Nach § 201 StGB ist das illegale Abhören von Telefongesprächen, nach § 148 in Verbindung mit § 89 des Telekommunikationsgesetzes das Abhören von Nachrichten mit einer Funkanlage strafbar. § 202a StGB erfasst zwar auch Daten, die übermittelt werden, allerdings nur dann, wenn sie besonders gesichert sind, womit die Regelung nur einen Schutz gegenüber verschlüsselten Daten gewährt. Aufgrund der Lückenhaftigkeit des geltenden Rechts besteht ein Regelungsbedarf, da es keinen Unterschied macht, welche Mittel für einen Kommunikationsvorgang eingesetzt werden können. Schutzwürdig sind alle nichtöffentlichen Kommunikationen. Die Tathandlung, das eigennützige oder fremdnützige Verschaffen von Daten, kann auf verschiedenste Weise realisiert werden. Es ist nicht erforderlich, dass die maßgeblichen Daten abgespeichert oder aufgezeichnet werden. Vielmehr genügen zum Beispiel bei Telefongesprächen das Mithören und bei E-Mails die bloße Kenntnisnahme. Ausreichend ist der Erwerb der Herrschaft über die Daten.

2. Der Tatbestand soll dadurch eingeschränkt werden, dass nur die nichtöffentliche Übermittlung von Daten, die nicht für den Täter bestimmt sind, erfasst wird. Entscheidend für die „Nichtöffentlichkeit“ einer Datenübermittlung sind nicht Art oder Inhalt der übertragenen Daten, sondern die Art des Übertragungsvorgangs. So kann auch eine Übermittlung über das Internet nichtöffentlich sein, selbst wenn es sich bei den übermittelten Daten um Informationen öffentlich zugänglicher Art handelt. Zur Auslegung des Begriffs „nichtöffentlich“ kann auf die Regelung in § 201 Abs. 2 Nr. 2 StGB zurückgegriffen werden.

3. Eine weitere Einschränkung des Tatbestandes soll durch die Voraussetzung der Anwendung „technischer Mittel“ erreicht werden, um eine Überkriminalisierung zu verhindern. Technische Mittel können neben Vorrichtungen zur Erfassung und Aufzeichnung drahtloser Kommunikationen auch Software, Codes oder Passwörter sein.

4. Der neue § 202b StGB enthält eine ausdrückliche Subsidiaritätsklausel. Damit wird klargestellt, dass die neue Vorschrift im Wesentlichen nur eine Ergänzungsfunktion hat, wenn beispielsweise nicht bereits die §§ 201 und 202a StGB eingreifen.

5. Eine Versuchsstrafbarkeit wird wegen der geringen Schwelle zur Verwirklichung des Tatbestandes und der Subsidiarität des Tatbestandes zu § 202a StGB, der ebenfalls keine Versuchsstrafbarkeit vorsieht, nicht vorgeschlagen. Es soll von der Möglichkeit, einen Vorbehalt gegen die Verpflichtung aus Artikel 11 Abs. 2 des Europarat-Übereinkommens hinsichtlich der Versuchsstrafbarkeit in Bezug auf das rechtswidrige Abfangen (Artikel 3 des Europarat-Übereinkommens) einzulegen, Gebrauch gemacht werden (vgl. Artikel 11 Abs. 3 des Europarat-Übereinkommens). Bei Hinterlegung der Ratifikationsurkunde wird daher eine Erklärung nach den Artikeln 40, 42 des Europarat-Übereinkommens abgegeben werden, nach der Artikel 11 Abs. 2 des Europarat-Übereinkommens nur teilweise angewendet wird.

6. Die Einfügung des Tatbestandes in den 15. Abschnitt soll die Struktur der vorhandenen Regelungen unangetastet lassen, die dem Schutz des persönlichen Lebens- und Geheimbereichs zwar als eigenständiges, in den einzelnen Tatbeständen aber sehr differenziertes Rechtsgut dienen. Die Differenzierung soll beibehalten werden. Schutzgut des neuen § 202b StGB ist zwar wie bei § 202a StGB auch das formelle Geheimhaltungsinteresse des Verfügungsberechtigten, aber nicht aufgrund einer besonderen Manifestation des Geheimhaltungswillens, sondern aufgrund des allgemeinen Rechts auf Nichtöffentlichkeit der Kommunikation.

Zu § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten)

Mit dem neuen § 202c StGB sollen bestimmte besonders gefährliche Vorbereitungshandlungen selbständig mit Strafe bedroht werden. Die Regelung dient der Umsetzung von Artikel 6 Abs. 1 Buchstabe a des Europarat-Übereinkommens (Missbrauch von Vorrichtungen).

1. Nach Artikel 6 Abs. 1 Buchstabe a Nr. ii des Europarat-Übereinkommens hat jede Vertragspartei zumindest das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen, mit dem Vorsatz, sie zur Begehung bestimmter Computerstraftaten zu verwenden, unter Strafe zu stellen.

   Daher schlägt der Gesetzesentwurf vor, in § 202c Abs. 1 Nr. 1 StGB die Vorbereitung einer Straftat nach den §§ 202a und 202b StGB durch Herstellen, sich oder einem anderen Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonst Zugänglichmachen von Passwörtern oder sonstigen Sicherungscodes zur strafbaren Handlung zu erklären.

2. Zudem enthält das Europarat-Übereinkommen in Artikel 6 Abs. 1 Buchstabe a Nr. i die Vorgabe, das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen einer Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, bestimmte Computerstraftaten zu begehen, als Straftat auszugestalten. Zwar sieht das Europarat-Übereinkommen in Artikel 6 Abs. 3 die Möglichkeit vor, einen Vorbehalt gegen diese Vorgabe einzulegen. Von der

Vorbehaltsmöglichkeit soll aber nur hinsichtlich des Merkmals „Vorrichtung“ Gebrauch gemacht werden. Die Erstreckung der Strafbarkeit auf die übrigen Vorbereitungshandlungen ist dagegen sachgerecht. Diese Verhaltensweisen werden strafrechtlich zwar bereits als Beihilfehandlung (§ 27 StGB) im Fall der tatsächlichen Begehung einer Straftat nach § 202a Abs. 1 StGB erfasst. Das strafwürdige Unrecht wird damit aber nicht ausreichend berücksichtigt. Kommt es nicht zur Begehung der Haupttat des § 202a Abs. 1 StGB, läge nur eine nicht strafbare versuchte Beihilfe vor. Für ein Strafbedürfnis spricht die hohe Gefährlichkeit solcher Tathandlungen. Erfasst werden insbesondere die so genannten Hacker-Tools, die bereits nach der Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen, und die aus dem Internet weitgehend anonym geladen werden können. Insbesondere die durch das Internet mögliche weite Verbreitung und leichte Verfügbarkeit der Hacker-Tools sowie ihre einfache Anwendung stellen eine erhebliche Gefahr dar, die nur dadurch effektiv bekämpft werden kann, dass bereits die Verbreitung solcher an sich gefährlichen Mittel unter Strafe gestellt wird.

Daher wird in Absatz 1 Nr. 2 vorgeschlagen, die Vorbereitung einer Straftat nach den §§ 202a und 202b StGB durch Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonst Zugänglichmachen von Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist, unter Strafe zu stellen.

3. Eine Einschränkung des Absatzes 1 Nr. 2 soll – in Anlehnung an § 263a Abs. 3 StGB – dadurch erreicht werden, dass bereits im objektiven Tatbestand auf die Bestimmung des Computerprogramms als Mittel zur Begehung einer Straftat nach den §§ 202a und 202b StGB abgestellt wird, um eine Überkriminalisierung zu verhindern. Es kommt insoweit auf die (objektivierte) Zweckbestimmung des Programms an. Somit ist sichergestellt, dass nur Hacker-Tools erfasst werden und die allgemeinen Programmier-Tools, -sprachen oder sonstigen Anwendungsprogramme bereits nicht unter den objektiven Tatbestand der Strafvorschrift fallen. Das Programm muss aber nicht ausschließlich für die Begehung einer Computerstraftat bestimmt sein. Es reicht, wenn die objektive Zweckbestimmung des Tools auch die Begehung einer solchen Straftat ist.

4. Der Tatbestand ist bereits dann erfüllt, wenn sich die Tathandlung auf nur ein Passwort oder einen sonstigen Sicherungscode oder auf nur ein Computerprogramm bezieht. Die Verwendung des Plurals hat lediglich sprachliche Gründe und erfolgt in Angleichung an andere Tatbestände, mit denen Vorbereitungshandlungen unter Strafe gestellt werden (z. B. § 149 Abs. 1, § 263a Abs. 3 und § 275 Abs. 1 StGB). Auch dort wird der Plural für die Tatobjekte verwendet, obwohl nicht ausschließlich die Mehrzahl gemeint ist. Aus der Verwendung des Plurals sind keine begrifflichen Folgerungen zu ziehen (vgl. RGSt 55, 101, 102; BGHSt 23, 46, 53; BGHSt 46, 147, 153).

5. Von der Möglichkeit, einen Vorbehalt gegen die Vorgabe in Artikel 6 Abs. 1 des Europarat-Übereinkommens hinsichtlich der weiteren Tathandlung des Besitzes einzulegen, soll Gebrauch gemacht werden. Bei der Hinterlegung der Ratifikationsurkunde wird daher eine Erklärung nach den Artikeln 40, 42 des Übereinkommens abgegeben werden, nach der Artikel 6 Abs. 1 des Übereinkommens nur teilweise angewendet wird.

6. Absatz 2 enthält durch den Verweis auf § 149 Abs. 2 und 3 StGB den Strafaufhebungsgrund der tätigen Reue. Dieser soll wie bei den §§ 152a, 152b, 263a, 275 und 276a i. V. m. 275 StGB auch auf die Fälle des § 202c Abs. 1 StGB Anwendung finden.

Zu Nummer 4 (§ 205 StGB)

An dem Antragserfordernis bei Taten des Ausspähens von Daten (§ 202a StGB) soll weiterhin festgehalten werden. Auch für das Abfangen von Daten (§ 202b StGB) soll ein Antragserfordernis vorgesehen werden. Soweit die Strafverfolgungsbehörde wegen eines besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält, soll jedoch in den Fällen der §§ 202a und 202b StGB auf den Antrag verzichtet werden können. Diese Einschränkung des Antragserfordernisses ist für eine effektive Verfolgung von Taten erforderlich, bei denen Daten von Dritten betroffen sind. Solche Dritte sind nicht Verletzte und damit nicht Antragsberechtigte, da nach herrschender Meinung im Falle des 202a StGB nur derjenige, der formell über die Daten verfügen darf, Verletzter sein kann (MünchKomm-Graf, a. a. O., § 205 Rn. 8; Schönke/Schröder-Lenckner, a. a. O., § 205 Rn. 7; LK-Schünemann, a. a. O., § 205 Rn. 5; a. A. Lackner/Kühl, a. a. O., § 205 Rn. 2).

§ 202c StGB soll dagegen kein Antragsdelikt sein. Anders als die §§ 202a und 202b StGB knüpft § 202c StGB nicht an eine Verletzung der Rechtsgüter Einzelner an, sondern stellt ein abstraktes Gefährdungsdelikt dar, so dass es (noch) keinen Geschädigten gibt, der einen Strafantrag stellen könnte. Auch im Hinblick auf § 202c StGB sind die §§ 153, 153a der Strafprozessordnung, §§ 45, 47 des Jugendgerichtsgesetzes anwendbar und stellen einen wichtigen Filter zur Verhinderung von unnötigen Strafverfahren dar, wenn die Schuld gering ist und eine materielle Rechtsgutsbeeinträchtigung nicht vorliegt.

Zu Nummer 5 (§ 303a StGB)

Die Erweiterung des § 303a StGB dient der Umsetzung von Artikel 6 des Europarat-Übereinkommens. Nach Artikel 6 Abs. 1 Buchstabe a sind bestimmte besonders gefährliche Vorbereitungshandlungen auch im Hinblick auf den Eingriff in Daten unter Strafe zu stellen. Daher soll der vorgeschlagene § 202c StGB auch auf die Vorbereitung einer Straftat nach § 303a Abs. 1 StGB Anwendung finden (§ 303a Abs. 3 StGB).

Zu Nummer 6 (§ 303b StGB)

1. Die Erweiterung des § 303b Abs. 1 StGB und die Einfügung eines neuen Absatzes 2 dienen der Umsetzung von Artikel 5 des Europarat-Übereinkommens (Eingriff in ein System) und Artikel 3 des EU-Rahmenbeschlusses (Rechtswidriger Systemeingriff). Diese sehen vor, die unbefugte schwere Behinderung oder Störung des Betriebs eines Computer- und Informationssystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beein-

trächtigen, Verstümmeln, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten im innerstaatlichen Recht als Straftat zu umschreiben.

Es wird daher vorgeschlagen, Absatz 1 auf Datenverarbeitungen auszudehnen, die „für einen anderen“ von wesentlicher Bedeutung sind. Außerdem soll Absatz 1 in einer neuen Nummer 2 um die Tathandlungen des Eingebens und Übermittelns erweitert werden. Die bisherige Nummer 2 wird Nummer 3. Zudem soll der bisherige Tatbestand der Computersabotage in einem neuen Absatz 2 als Qualifikationstatbestand aufrechterhalten bleiben. Der bisherige Absatz 2 wird Absatz 3.

a) Der Tatbestand der Computersabotage schützt bislang nur Datenverarbeitungen von fremden Betrieben, fremden Unternehmen und Behörden. Da das Europarat-Übereinkommen und der EU-Rahmenbeschluss jedoch auch Computer- und Informationssysteme von Privatpersonen erfassen, wird Absatz 1 erweitert, indem nunmehr generell auf Datenverarbeitungen abgestellt wird. Dies zieht auch eine Änderung der Schutzrichtung des Straftatbestandes nach sich. Wurde als geschütztes Rechtsgut bislang das Interesse von Wirtschaft und Verwaltung an der Funktionstüchtigkeit ihrer Datenverarbeitung angesehen, so ist dies nun das Interesse der Betreiber und Nutzer von Datenverarbeitungen allgemein an deren ordnungsgemäßer Funktionsweise.

   Das Merkmal „von wesentlicher Bedeutung“ soll in der vorgeschlagenen Form aufrechterhalten bleiben. Es dient als Filter für Bagatellfälle, die durch den Tatbestand nicht erfasst werden sollen. Eine solche Einschränkung ist nach Artikel 5 des Europarat-Übereinkommens („schwere Behinderung“) und nach Artikel 3 des EU-Rahmenbeschlusses („wenn kein leichter Fall vorliegt“) zulässig. Um die Strafbarkeit nicht zu weit auszudehnen, ist diese Einschränkung auch erforderlich. Bei Privatpersonen als Geschädigte wird darauf abzustellen sein, ob die Datenverarbeitungsanlage für die Lebensgestaltung der Privatperson eine zentrale Funktion einnimmt. So wird eine Datenverarbeitung im Rahmen einer Erwerbstätigkeit, einer schriftstellerischen, wissenschaftlichen oder künstlerischen Tätigkeit regelmäßig als wesentlich einzustufen sein, nicht aber jeglicher Kommunikationsvorgang im privaten Bereich oder etwa Computerspiele.

   Da durch die Erweiterung des Tatbestandes auch weniger schwerwiegende Fälle als bisher erfasst werden, soll der Strafrahmen auf Freiheitsstrafe bis zu drei Jahren abgesenkt werden. Die Anforderungen der Artikel 6 und 7 des EU-Rahmenbeschlusses an die Mindesthöchststrafe bleiben dabei erfüllt. Wird eine Datenverarbeitung gestört, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, soll es jedoch bei der bisherigen Strafdrohung verbleiben (vgl. neuer Absatz 2).

b) Durch die vorgeschlagene Erweiterung des Absatzes 1 durch eine neue Nummer 2 sollen künftig auch solche zur Störung einer Datenverarbeitung führenden Fälle zur strafbaren Handlung werden, in denen – über die bereits von Nummer 1 im geltenden Recht erfassten Tathandlungen hinausgehend – Daten in Nachteilszufügungsabsicht eingegeben oder übermittelt werden.

   Die Bedeutung dieser Erweiterung beruht vor allem darauf, dass auch an sich neutrale Handlungen wie das „Eingeben“ und „Übermitteln“ von Daten in ein Computersystem bei unbefugter oder missbräuchlicher Begehungsweise geeignet sein können, erhebliche Störungen zu verursachen. Beispiele hierfür sind die „Denial-of-Service-Attacken“, bei denen die Dienste eines Servers durch eine Vielzahl von Anfragen derart belastet werden, dass dessen Aufnahme- und Verarbeitungskapazität nicht ausreicht und somit der Zugang für berechtigte Kontaktaufnahmen mit dem Server blockiert oder zumindest erschwert wird.

   Das subjektive Korrektiv „in der Absicht, einem anderen Nachteil zuzufügen“ stellt dabei sicher, dass beispielsweise in der Netzwerkgestaltung begründete gängige Aktivitäten oder andere zulässige Maßnahmen der Betreiber oder Unternehmen nur dann unter Strafe gestellt werden, wenn diese missbräuchlich, das heißt in Schädigungsabsicht erfolgen. Zur Auslegung der Nachteilszufügungsabsicht kann auf die Auslegung des § 274 Abs. 1 Nr. 1 StGB zurückgegriffen werden. Erforderlich ist das Bewusstsein, dass der Nachteil die notwendige Folge der Tat ist. Ein Nachteil ist jede Beeinträchtigung, nicht nur der Vermögensschaden.

c) Die Einfügung des Merkmals „erheblich“ dient der Klarstellung. Eine Störung im Sinne des § 303b StGB wird allgemein erst dann angenommen, wenn eine nicht unerhebliche Beeinträchtigung des reibungslosen Ablaufs der genannten Datenverarbeitung vorliegt (vgl. Bundestagsdrucksache 10/5058, S. 35; Schönke/Schröder-Stree, a. a. O., § 303b Rn. 10). Im Hinblick auf die Erweiterung des Tatbestandes auf Computer- und Informationssysteme von Privatpersonen soll aber bereits im Tatbestand selbst hervorgehoben werden, dass nur Handlungen, die eine Erheblichkeitsschwelle überschreiten, strafbar sind.

d) Die Versuchsstrafbarkeit soll auch für den erweiterten Grundtatbestand in § 303b Abs. 1 StGB bestehen bleiben. Eine solche wird durch Artikel 5 Abs. 2 des EU-Rahmenbeschlusses zwingend vorgeschrieben.

e) Der bisherige Tatbestand der Computersabotage mit seiner erhöhten Strafdrohung soll als Qualifikationstatbestand aufrechterhalten bleiben. In den Fällen, in denen eine Datenverarbeitung für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe daher neben Geldstrafe weiterhin Freiheitsstrafe bis zu fünf Jahren.

f) Eine Computersabotage ist bereits nach geltendem Recht Antragsdelikt nach § 303c StGB. Dies soll auch für den erweiterten Tatbestand gelten.

2. Der Entwurf sieht in Absatz 4 eine Strafzumessungsregel für besonders schwere Fälle der Computersabotage vor, die sich vom Strafrahmen des Absatzes 2 nicht immer angemessen erfassen lassen. Die in den Nummern 1 und 2

vorgeschlagenen Regelbeispiele enthalten unter anderem auch die Strafzumessungsregeln der Tatbestände des Computerbetrugs (§ 263a Abs. 2 in Verbindung mit § 263 Abs. 3 Satz 2 Nr. 1 und 2 StGB) und der Fälschung beweiserheblicher Daten (§ 269 Abs. 3 in Verbindung mit § 267 Abs. 3 Satz 2 Nr. 1 und 2 StGB). Die Nummer 3 entspricht überwiegend § 316b Abs. 3 StGB.

Computersabotagehandlungen können beträchtliche wirtschaftliche Schäden nach sich ziehen. Wenn solche Handlungen zu hohen Vermögensverlusten bei den betroffenen Behörden oder Unternehmen führen, ist es sachgerecht, die Sabotagehandlungen in der Regel mit einer höheren Strafe zu ahnden. Dies gilt auch für die gewerbs- oder bandenmäßige Begehung von Computersabotage. Die Auslegung der Merkmale in den Nummern 1 und 2 kann sich an der Auslegung dieser Merkmale in anderen Strafzumessungsregelungen orientieren.

Da eine Störung der Datenverarbeitung nach § 303b StGB nicht den in § 316b StGB vorausgesetzten Grad der Störung öffentlicher Betriebe erreichen muss (vgl. Bundestagsdrucksache 10/5058, S. 35), im Hinblick auf die technischen Entwicklungen dennoch schwere Folgen für die Allgemeinheit nach sich ziehen kann, soll das Regelbeispiel in § 316b Abs. 3 StGB künftig auch für besonders schwere Fälle der Computersabotage vorgesehen werden (Nummer 3). Dies trägt auch der Tatsache Rechnung, dass die Verfahrensabläufe in besonders schützenswerten Infrastrukturen, z. B. öffentlichen Versorgungswerken und Krankenhäusern, heute überwiegend elektronisch erfolgen und damit für Sabotageakte besonders anfällig sind. In gleicher Weise anfällig sind solche Infrastrukturen, die der Versorgung der Bevölkerung mit lebenswichtigen Dienstleistungen, z. B. Energie- und Bankwirtschaft, und der Sicherheit der Bundesrepublik Deutschland dienen, so dass von Nummer 3 auch die besonders schweren Folgen von Angriffen auf solche Infrastrukturen erfasst werden sollen.

Die Auslegung des Begriffs der Sicherheit der Bundesrepublik Deutschland kann sich an der Begriffsbestimmung und Auslegung des § 92 Abs. 3 Nr. 2 StGB orientieren. Der Begriff Sicherheit umfasst die innere und äußere Sicherheit. Durch die Gleichstellung der Beeinträchtigung der Sicherheit der Bundesrepublik Deutschland mit der Beeinträchtigung der Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen soll klargestellt werden, dass die erhöhte Strafdrohung nur für Angriffe mit vergleichbar schweren Folgen gilt.

3. Der vorgeschlagene neue Absatz 5 dient der Umsetzung von Artikel 6 des Europarat-Übereinkommens. Nach Artikel 6 Abs. 1 Buchstabe a sollen bestimmte besonders gefährliche Vorbereitungshandlungen auch im Hinblick auf den Eingriff in ein System selbstständig mit Strafe bedroht werden. Daher soll der vorgeschlagene § 202c StGB auch auf die Vorbereitung einer Straftat nach § 303b Abs. 1 StGB Anwendung finden (§ 303b Abs. 4 StGB).

Zu Nummer 7 (§ 303c StGB)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 2 (Änderung des Gesetzes über Ordnungswidrigkeiten)

Artikel 8 Abs. 2 des EU-Rahmenbeschlusses erfordert die Verantwortlichkeit einer juristischen Person grundsätzlich bereits dann, wenn mangelnde Überwachung oder Kontrolle einer ihrer Leitungspersonen die Begehung der in den Artikeln 2, 3, 4 und 5 genannten Straftaten ermöglicht hat. Eine entsprechende Vorgabe enthält Artikel 12 Abs. 2 des Europarat-Übereinkommens im Hinblick auf die dort umschriebenen Delikte. Die Tatbestände der §§ 202a, 202b, 202c, 303a und 303b StGB, auch in Verbindung mit den §§ 26, 27 StGB, mit denen die Vorgaben der Artikel 2 bis 5 des EU-Rahmenbeschlusses und der Artikel 2 bis 8 und 11 Abs. 1 des Europarat-Übereinkommens umgesetzt werden, sind Allgemeindelikte, die von jedermann verwirklicht werden können. Die in § 130 Abs. 1 Satz 1 OWiG vorgesehene Streichung der Wörter „als solchen“ soll daher klarstellen, dass § 130 OWiG nicht nur Sonderdelikte erfasst, sondern – ebenso wie § 30 OWiG – grundsätzlich auch Allgemeindelikte erfassen kann (so schon die h. M. zum bisherigen Recht, vgl. u. a. Göhler/König, OWiG, 14. Aufl., § 130 Rn. 18 m. N.; a. A. Rogall in Karlsruher Kommentar, OWiG, 3. Aufl., § 130 Rn. 87 ff., ebenfalls m. N.). Daher können auch die vorstehend genannten Straftatbestände des Ausspähens von Daten, des Abfangens von Daten, des Vorbereitens des Ausspähens und Abfangens von Daten, der Datenveränderung und der Computersabotage taugliche Bezugstaten nach § 130 OWiG sein und damit über diese Vorschrift eine Verantwortlichkeit der juristischen Person nach § 30 OWiG begründen.

Trotz dieser Streichung bleibt es aber bei dem – auch bei § 30 OWiG geltenden – Erfordernis, dass die Pflichtverletzung im Zusammenhang mit der Betriebs- oder Unternehmensführung erfolgt sein muss (vgl. Göhler/König, a. a. O., § 30 Rn. 20, § 130 Rn. 18), womit insbesondere Pflichtverletzungen mit per se höchstpersönlichem Einschlag, aber auch solche, die keinen Bezug zur wirtschaftlichen Betätigung des Betriebs oder Unternehmens haben, weiterhin ausgeschlossen bleiben. Für die hier in Rede stehenden Delikte der Computerkriminalität bedeutet dies zum Beispiel Folgendes: Handelt es sich um ein Unternehmen, das für einen Kunden eine neue Software entwickelt, und verschaffen sich die Mitarbeiter im Rahmen dieser Entwicklungstätigkeit unbefugt Zugang zu besonders gesicherten Daten des Kunden, löschen oder verändern sie rechtswidrig dessen Daten oder beschädigen sie dessen Datenverarbeitungsanlage, so wird dieser Zusammenhang zur Unternehmens- und Betriebstätigkeit in der Regel zu bejahen sein. Wird die Tat hingegen zum Beispiel von dem allein für den internen EDV-Einsatz zuständigen Mitarbeiter eines Architekturbüros gelegentlich seiner Tätigkeit im Hinblick auf die Daten einer Privatperson verübt, wird es daran fehlen. Im Übrigen kann bei der konkreten Rechtsanwendung auf die – auch zu § 30 OWiG – entwickelte Rechtsprechung zurückgegriffen werden (vgl. zuletzt OLG Celle vom 26. November 2004, NStZ-RR 2005, S. 82 f., zu § 30 OWiG).

Das Erfordernis des betrieblichen Zusammenhanges widerspricht auch nicht den Vorgaben des EU-Rahmenbeschlusses und des Europarat-Übereinkommens, da diese nur solche Taten erfassen, die „zugunsten der juristischen Person“ begangen werden. Dieses Merkmal verdeutlicht, dass sich die

Tat auf die Tätigkeit der juristischen Person beziehen muss und es daher gerechtfertigt ist, weiterhin einen Zusammenhang zur Unternehmens- und Betriebsführung einzufordern, um den Haftungsrahmen für den Inhaber eines Betriebs oder Unternehmens nicht zu überspannen.

Zu Artikel 3 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes. Der EU-Rahmenbeschluss verpflichtet die Mitgliedstaaten, die erforderlichen Umsetzungsmaßnahmen bis spätestens 16. März 2007 zu treffen (Artikel 12 des EU-Rahmenbeschlusses). Einer Frist, um sich auf die neue Rechtslage einzustellen, bedarf es nicht. Das Gesetz soll deshalb bereits am Tag nach der Verkündung im Bundesgesetzblatt in Kraft treten.

Anlage 2

Stellungnahme des Bundesrates

Der Bundesrat hat in seiner 827. Sitzung am 3. November 2006 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Abs. 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. **Zum Gesetzentwurf insgesamt**

   a) Der Bundesrat stimmt der Bundesregierung in ihrer Auffassung zu, dass das geltende Computerstrafrecht verbessert werden muss. Die Defizite des geltenden Rechts, die unter anderem durch die rasche Fortentwicklung der modernen Kommunikationsmöglichkeiten bedingt sind, sind in der Begründung des Regierungsentwurfs zutreffend dargestellt.

   b) Der Bundesrat weist jedoch zugleich darauf hin, dass die Gefahr besteht, durch eine weite Tatbestandsfassung ein Spektrum von Handlungsweisen in die Strafbarkeit einzubeziehen, die das Verdikt der Strafbarkeit nicht verdienen. Diese Problematik, die bereits das geltende Recht betrifft und die der Regierungsentwurf im Grundsatz nicht verkennt, ist noch nicht überzeugend gelöst. In diesem Zusammenhang weist der Bundesrat beispielhaft auf Folgendes hin:

      aa) Mit der Neufassung des § 202a StGB soll das Phänomen des „Hacking“ besser erfasst werden. Soweit das „Hacking“ im eigentlichen Sinne, also das unbefugte Eindringen in fremde Computersysteme durch Missbrauch der modernen Kommunikationsmöglichkeiten, in Frage steht, bestehen auch keine Bedenken in Bezug auf die Strafwürdigkeit und Strafbedürftigkeit. Jedoch reicht die Strafbarkeit weit über solche Konstellationen hinaus. Dies ist vor allem darauf zurückzuführen, dass der Entwurf auf den Zugang zu Daten abstellt, kaum aber noch elektronische Geräte existieren, die ohne Datenspeicherung und -verarbeitung auskommen. Beispielsweise würde sich nach dem Entwurf wohl strafbar machen, wer sich Zugang zu dem von seinem Kind verschlossenen MP3-Player verschafft, um die darauf gespeicherten Musikstücke anzuhören. Dies würde jedenfalls dann gelten, wenn das Kind durch den Verschluss auch verhindern will, dass ein Dritter hört, welche Musik er konsumiert. Ebenfalls strafbar machen würde sich der Jugendliche, der sich das von seinen Eltern an einem (vermeintlich) sicheren Ort verwahrte Passwort für nicht jugendfreie Sendungen im Pay-TV verschafft und sich verbotener Weise eine solche Sendung ansieht. Es handelt sich dabei lediglich um Beispiele aus einer nicht überschaubaren Palette von Handlungen, die unter den neuen Tatbestand fallen würden. Der Umstand hat Auswirkungen auch auf die Reichweite des vorgeschlagenen § 202c StGB-E, der an § 202a StGB anknüpft.

      Es erscheint nicht überzeugend, in diesem Zusammenhang auf die Möglichkeit der Verfahrenseinstellung nach Opportunitätsgrundsätzen zu verweisen.

      bb) In § 202c StGB-E sollen Vorbereitungshandlungen unter Strafe gestellt werden. Auch insoweit verfolgt der Regierungsentwurf in Übereinstimmung mit dem umzusetzenden Rahmenbeschluss wichtige Anliegen, namentlich, um der Verbreitung von „Hacker-Tools“ entgegenzuwirken. Jedoch ist der Tatbestand abermals sehr weit geraten. Auch im Hinblick darauf, dass bezüglich der vorbereiteten Tat bedingter Vorsatz ausreicht, würden künftig wohl unter anderem die folgenden Verhaltensweisen in die Strafbarkeit einbezogen:

      Der gerade auf Dienstreise befindliche „Täter“ (Angehöriger einer Behörde oder eines Unternehmens) übermittelt einer Schreibkraft sein Passwort, weil er dringend eine E-Mail aus seinem E-Mail-Postfach benötigt. Er rechnet dabei damit und nimmt billigend in Kauf, dass sich die Schreibkraft bei weiteren Gelegenheiten mit seinem Passwort „einloggt“ und sich so den Zugang zu nicht für sie bestimmten Daten verschafft (was sie dann nicht tut).

      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).

      Dem lässt sich nicht überzeugend entgegenhalten, dass es in solchen Fällen an der Überwindung der Zugangssicherung durch den „Haupttäter“ fehlen würde, weil der Zugang zu den Daten demjenigen, der über das Passwort verfügt, keinen erheblichen zeitlichen oder technischen Aufwand mehr bereitet (vgl. Einzelbegründung zu § 202a StGB-E, Bundesratsdrucksache 676/06, S. 14). Eine solche Interpretation kann schon deswegen nicht richtig sein, weil § 202c StGB-E in Bezug auf das Passwort sonst immer leerlaufen würde. Die diesbezügliche Passage in der Entwurfsbegründung ist wohl in dem Sinne zu verstehen, dass die Überwindung der Zugangssicherung ohne Kenntnis des Passworts erheblichen Aufwand bereiten muss.

      cc) § 303a StGB ist überaus heftiger Kritik aus nahezu dem gesamten Schrifttum ausgesetzt (vgl. etwa Tröndle/Fischer, § 303a Rn. 4 mit zahlreichen Nachweisen). So wirft die Frage der Ver-

fügungsberechtigung über die jeweiligen Daten vor allem in vernetzten Systemen kaum überwindliche Auslegungsprobleme auf (vgl. hierzu LK-Tolksdorf, § 303a Rn. 7, 8 ff.). Es ist zu befürchten, dass die Vorschrift in der gegenwärtigen Fassung einer verfassungsrechtlichen Prüfung nicht standhalten würde.

dd) § 303b StGB soll auf den privaten Bereich erweitert werden. Damit ist auch eine erhebliche Ausdehnung der Strafbarkeit verbunden. Dieser Umstand erhält dadurch besonderes Gewicht, dass der Begriff der Datenverarbeitung aufgrund der bei elektronischen Geräten fortschreitenden Digitalisierung eine Vielzahl von Geräten erfasst (dazu schon oben Buchstabe a). Lediglich Beispiele sind Videorekorder, Hifi-Anlagen, Fernsehgeräte oder Navigationssysteme bis hin zu Wasch- und Spülmaschinen oder etwa programmierbaren Elektroherden. Die Störung des Betriebs auch solcher Geräte kann nach der neuen Vorschrift strafbar sein, wenn die Datenverarbeitung für den Berechtigten von wesentlicher Bedeutung ist. Im Extremfall kann damit selbst die Beeinträchtigung des Betriebs einer Wasch- oder Spülmaschine unter den Tatbestand der Computersabotage subsumiert werden.

c) Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens nach Lösungen zu suchen, mit denen die vorgenannten Probleme ausgeräumt oder zumindest vermindert werden. Er hält dies auch vor dem Hintergrund der derzeitigen tatsächlichen Entwicklung für zwingend geboten: Beispielsweise rechnet eine deutsche Staatsanwaltschaft aufgrund entsprechender Ankündigung eines Rechteinhabers damit, dass wegen der illegalen Verbreitung von lediglich vier Computerspielen über das Internet noch in diesem Jahr über 200 000 Urheberrechtsverstöße bei ihr angezeigt werden. Bei anderen Staatsanwaltschaften wurden in der jüngsten Vergangenheit bereits mehrere 10 000 Fälle angezeigt. Den in dem Entwurf beschriebenen Verhaltensweisen kann unter Umständen eine ähnliche Breitenwirkung zukommen. Auch angesichts dessen muss zumindest eine auf die der Strafe würdigen und bedürftigen Handlungen begrenzte Tatbestandsfassung angestrebt werden.

2. **Zu Artikel 1 Nr. 3** (§ 202c StGB)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen,

a) ob die aktuelle Ausgestaltung des § 202c StGB-E beim gutwilligen Umgang mit allgemeinen Programmier-Tools, -sprachen oder sonstigen Softwareprogrammen sowie „Hacker-Tools“ zur Sicherheitsüberprüfung von IT-Systemen ausreichend vor einer ungewollten Kriminalisierung schützt und

b) ob der § 202c StGB-E um eine konkrete Aufnahme des Tatbestandes des „Phishing“ (Versuch, per E-Mail den Empfänger durch irreführende und manipulierte Angaben und Inhalte zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen) erweitert werden kann.

Anlage 3

Gegenäußerung der Bundesregierung

Zu Nummer 1 (Zum Gesetzentwurf insgesamt)

Soweit der Bundesrat unter Buchstabe c bittet, nach Lösungen zu suchen, mit denen die unter Buchstabe b genannten Probleme zu weiter Tatbestandsfassungen ausgeräumt oder vermindert werden, hält die Bundesregierung Änderungen bei den vorgeschlagenen Tatbestandsfassungen nicht für veranlasst. Die vorgeschlagenen Straftatbestände sind bereits eng gefasst, um der Gefahr, nicht strafwürdige Handlungsweisen zu erfassen, wirksam zu begegnen. Zu den vom Bundesrat unter Buchstabe b gebildeten Beispielsfällen weist die Bundesregierung auf Folgendes hin:

Zu Doppelbuchstabe aa

Die vom Bundesrat angesprochenen Fälle der bloßen Ingebrauchnahme von gesicherten elektronischen Geräten gegen den Willen des Berechtigten werden durch das Tatbestandsmerkmal der besonderen Zugangssicherung („die gegen unberechtigten Zugang besonders gesichert sind“) aus dem Anwendungsbereich des § 202a StGB herausgefiltert. Dieses Tatbestandsmerkmal soll gegenüber der bisher geltenden Fassung des § 202a StGB unverändert beibehalten werden. Geändert werden soll lediglich das Merkmal der Datenverschaffung. Ausreichend soll künftig die Verschaffung des Zugangs zu Daten sein. Diese Änderung hat keine Auswirkungen auf die vom Bundesrat gebildeten Fälle. Zur Nichterfassung nicht strafwürdiger Fälle wird im Übrigen auf die Gesetzesbegründung (Teil B., zu Artikel 1, zu den Nummern 2 und 3) verwiesen.

Zu Doppelbuchstabe bb

Die Herausgabe des Passworts durch den Berechtigten führt nicht dazu, dass dieser sich wegen des Vorbereitens des Ausspähens und Abfangens von Daten strafbar machen kann, wenn er damit rechnet oder es in Kauf nimmt, dass der Empfänger des Passworts dieses missbräuchlich nutzt, um auf Daten des Berechtigten zuzugreifen. Der Verschaffung des Zugangs zu Daten mit Hilfe des freiwillig durch den Berechtigten herausgegebenen Passworts stellt bereits keine Computerstraftat im Sinne des § 202a StGB dar. Es fehlt an dem objektiven Tatbestandsmerkmal der Überwindung der besonderen Zugangssicherung.

Zu Doppelbuchstabe cc

§ 303a Abs. 1 StGB soll im Rahmen des vorgeschlagenen Gesetzentwurfs nicht geändert werden. Soweit der Bundesrat die Befürchtung äußert, dass § 303a Abs. 1 StGB in der derzeit gültigen Fassung einer verfassungsrechtlichen Prüfung nicht standhalten würde, hält die Bundesregierung diese Befürchtung nicht für begründet. In der Literatur besteht zwar Einigkeit darüber, dass ohne die Einbeziehung des Merkmals „rechtswidrig“ der Tatbestand keinen Unrechtstyp beschreibt. Dieser kann erst dadurch konstruiert werden, dass aus dem Rechtswidrigkeitserfordernis ein einschränkendes Tatbestandselement abgeleitet wird. Ein Grund zu einer weiteren Änderung des Tatbestandes besteht aber nicht. Die Einschränkung entspricht dem Willen des Gesetzgebers. In der Gesetzesbegründung wird darauf hingewiesen, dass sich die Rechtswidrigkeit sowohl aus der Verletzung des Verfügungsrechts des Speichernden als auch aus der Verletzung von Interessen des vom Inhalt der Daten Betroffenen (§ 43 des Bundesdatenschutzgesetzes) ergeben kann (Bundestagsdrucksache 10/5058, S. 34). Zwar wird in der Literatur teilweise die Verfassungsmäßigkeit der Vorschrift wegen der (angeblichen) Unbestimmtheit des Tatbestandes in Frage gestellt. Allerdings hat bereits das Bayerische Oberste Landesgericht in seinem Urteil vom 24. Juni 1993 (Az.: 5 St RR 5/93) eine Verurteilung wegen Datenveränderung nach § 303a StGB bestätigt, ohne die Verfassungsmäßigkeit des Tatbestandes zu problematisieren.

Zu Doppelbuchstabe dd

Die Erweiterung des § 303b StGB auf den privaten Bereich dient der Umsetzung des Europarat-Übereinkommens und des EU-Rahmenbeschlusses. Um die Strafbarkeit nicht zu weit auszudehnen und Bagatellfälle nicht zu erfassen, wurde die engste noch mögliche Fassung für die Umsetzung der internationalen Rechtsinstrumente gewählt. Dabei dienen sowohl das Merkmal der Datenverarbeitung „von wesentlicher Bedeutung“ als auch das Merkmal „erheblich stört“ als Filter für Bagatellfälle. Zu beiden Merkmalen gibt es bereits durch Literatur und Rechtsprechung eine gefestigte Auslegung. Zudem wird nicht jede Störungshandlung unter Strafe gestellt; strafbar sind nur die in Absatz 1 Nr. 1 bis 3 aufgeführten Handlungen. Damit ist in dreifacher Weise sichergestellt, dass Bagatellfälle im privaten Bereich nicht von § 303b StGB erfasst werden. Dies wird ausdrücklich in der Gesetzesbegründung klargestellt.

Zu Nummer 2 (Zu Artikel 1 Nr. 3, § 202c StGB)

Die Bundesregierung hat die vom Bundesrat angesprochenen Fragen bereits bei der Erstellung und Abstimmung des Regierungsentwurfs einer eingehenden Überprüfung unterzogen.

Zu Buchstabe a

Die Befürchtung, dass auch der gutwillige Umgang mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen von § 202c StGB-E erfasst werden könnte, ist nicht begründet. Die Nichterfassung des gutwilligen Umgangs mit Softwareprogrammen zur Sicherheitsüberprüfung von IT-Systemen wird bereits auf Tatbestandsebene durch zwei gesetzliche Tatbestandsmerkmale abgesichert. Einerseits muss es sich objektiv um ein Computerprogramm handeln, dessen Zweck die Begehung einer Computerstraftat ist, und andererseits muss die Tathandlung – also das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonst Zugänglichmachen – zur Vorbereitung einer Computerstraftat erfolgen.

Durch die objektive Beschränkung auf Computerprogramme, deren Zweck die Begehung einer Computerstraftat ist, wird bereits auf Tatbestandsebene sichergestellt, dass keine Computerprogramme erfasst werden, die beispielsweise der Überprüfung der Sicherheit oder Forschung in diesem Bereich dienen. Unter Strafe gestellt werden lediglich das Herstellen, Verschaffen, Verbreiten usw. solcher Programme, denen die illegale Verwendung immanent ist, die also nach Art und Weise des Aufbaus oder ihrer Beschaffenheit auf die Begehung von Computerstraftaten angelegt sind. Bei Programmen, deren funktionaler Zweck nicht eindeutig ein krimineller ist und die erst durch ihre Anwendung zu einem Tatwerkzeug eines Kriminellen oder zu einem legitimen Werkzeug (z. B. bei Sicherheitsüberprüfungen oder im Forschungsbereich) werden (sog. dual use tools), ist der objektive Tatbestand des § 202c StGB-E nicht erfüllt. Die bloße Eignung von Software zur Begehung von Computerstraftaten ist daher nicht ausreichend, so dass auch solche Programme aus dem Tatbestand herausfallen, die lediglich zur Begehung von Computerstraftaten missbraucht werden können.

Zudem muss die Tathandlung zur Vorbereitung einer Computerstraftat (§§ 202a, 202b, 303a, 303b StGB) erfolgen. Entscheidend für die Tatbestandserfüllung des § 202c StGB-E ist, dass der Täter eine eigene oder fremde Computerstraftat in Aussicht genommen hat. Das ist nicht der Fall, wenn das Computerprogramm beispielsweise zum Zwecke der Sicherheitsüberprüfung, zur Entwicklung von Sicherheitssoftware oder zu Ausbildungszwecken in der IT-Sicherheitsbranche hergestellt, erworben oder einem anderen überlassen wurde, da die Sicherheitsüberprüfung, die Entwicklung von Sicherheitssoftware oder die Ausbildung im Bereich der IT-Sicherheit keine Computerstraftat darstellen. Das gilt auch für den Fall, in dem ein Computerprogramm, das ursprünglich nur zu kriminellen Zwecken hergestellt worden ist, verschafft, verkauft, überlassen, verbreitet oder sonst zugänglich gemacht wird, wenn dies ausschließlich zu nicht kriminellen Zwecken erfolgt und keine Anhaltspunkte für eine eigene oder fremde Computerstraftat nach den §§ 202a, 202b, 303a, 303b StGB bestehen. Auch in diesem Fall wird keine Computerstraftat in Aussicht genommen. Wenn also beispielsweise in den Fällen des Entwickelns von Sicherheitssoftware auch Schadprogramme verschafft werden, dann erfolgt dies nicht zur Vorbereitung einer Computerstraftat nach den §§ 202a, 202b, 303a, 303b StGB und ist daher nicht nach den § 202c StGB-E strafbar. § 202c StGB-E ist demzufolge nicht so zu verstehen, dass allein das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonst Zugänglichmachen der in Rede stehenden Computerprogramme ein Vorbereiten der Computerstraftaten nach den §§ 202a, 202b, 303a, 303b StGB darstellt.

Zu Buchstabe b

Die Bundesregierung hat bereits bei der Erarbeitung des Gesetzentwurfs geprüft, ob die Aufnahme eines ausdrücklichen Phishing-Straftatbestandes in das Strafgesetzbuch erforderlich ist. Im Rahmen der Länderbeteiligung zu diesem Gesetzentwurf erfolgte eine Befragung der Strafverfolgungspraxis. Auf der Grundlage dieser Befragung haben fast alle Landesjustizverwaltungen mitgeteilt, dass sie einen ausreichenden strafrechtlichen Schutz gegen Phishing-Angriffe nach geltendem Recht für gewährleistet halten und zumindest derzeit keine Notwendigkeit für ergänzende strafrechtliche Regelungen sehen. Die Bundesregierung teilt diese Auffassung.

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