Bundesrat **Drucksache** **248/19**

28.05.19

Gesetzesantrag
des Landes Nordrhein-Westfalen

Entwurf eines Strafrechtsänderungsgesetzes - Gesetz zur effektiveren Verfolgung der Computerkriminalität

A. Problem und Ziel

Die Digitalisierung und die zunehmende Vernetzung über das Internet haben in vielen Bereichen zu einem Innovationsschub und zur Verbesserung der Lebensqualität beigetragen. In offenen Gesellschaften darf aber nicht außer Acht gelassen werden, dass durch so umfassende Veränderungsprozesse naturgemäß auch neue Verletzbarkeiten entstehen und dadurch Schutzbedürfnisse neu gewichtet werden müssen.

Die Kehrseite der Vorzüge der Digitalisierung ist die Cyberkriminalität, die zunehmende Gefahren für die Sicherheit der Bürgerinnen und Bürger, der Unternehmen und des Staates mit sich bringt. Daten haben deutlich an Wertigkeit zugenommen. Sie werden deshalb mehr und mehr begehrtes Ziel von Straftätern.

Die bekannt gewordenen „Datenleaks“ der letzten Jahre verdeutlichen dabei die enorme Dimension, die unberechtigte Datenabgriffe inzwischen erlangt haben. So wurden bei MySpace 360 Mio. Datensätze, bei Sony 102 Mio. Datensätze, bei Dropbox 69 Mio. Datensätze, bei LinkedIn 177 Mio. Datensätze, bei Yahoo 500 Mio. Datensätze und bei Ashley Madison 36 Mio. Datensätze unbefugt abgegriffen. Eine im Januar 2019 bekanntgewordene Sammlung von Passwort-Leaks enthielt bei einem Volumen von 935 Gigabyte über 2,2 Milliarden Accounts. Bundesweites Aufsehen erregte Ende des Jahres 2018/Anfang 2019 die Meldung, dass ein Hacker mit offenbar einfachen Mitteln massenhaft persönliche Daten von mehreren hundert Politikern, Prominenten und Journalisten ausgespäht und auf der Internetplattform Twitter verbreitet hatte. Neben diesen „Datenleaks“ kam es zuletzt auch vermehrt zu Cyberattacken, bei denen Verschlüsselungstrojaner (sog. Ransomware) in die IT-Infrastruktur von Unternehmen oder Krankenhäusern eingeschleust wurden und

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

dort zu massiven Betriebsstörungen und Schäden führten.

Diese aktuellen Vorfälle zeigen, dass Cyberkriminalität inzwischen ein Ausmaß erreicht hat, das das Sicherheitsgefühl der Menschen massiv bedroht und das Potential hat, die Grundlagen von Demokratie, Staat und Wirtschaft zu gefährden. Die wirtschaftlichen Schäden, die etwa durch Produktionsausfälle, den Verlust von Geschäftsgeheimnissen oder die Kosten für eine Wiederherstellung von Daten entstehen, sind groß. Gleiches gilt für die negativen Folgen, die mit der Veröffentlichung sensibler Informationen oder dem Eindringen in Datenverarbeitungen verbunden sein können. Im Extremfall können Cyberangriffe etwa auf Krankenhäuser, Flughäfen oder Verteidigungseinrichtungen sogar den Verlust von Menschenleben fordern. Daten und Datenverarbeitungssysteme werden aufgrund ihrer wachsenden Bedeutung für die Bürgerinnen und Bürger, den Staat und die Wirtschaft zum Tatobjekt für organisierte kriminelle Strukturen.

Es ist Aufgabe des Strafrechts, die für solche Angriffe verantwortlichen Personen zügig zu ermitteln und schuldangemessen zu bestrafen - nicht zuletzt um andere potentielle Täter abzuschrecken, die Gesellschaft zu schützen, die mittels der Digitalisierung erreichte Wirtschaftskraft nicht durch Straftaten zu gefährden und das Vertrauen in die staatliche Handlungsfähigkeit zu erhalten. Diese Aufgabe kann das Strafrecht derzeit jedoch nur bedingt erfüllen.

Wie in der analogen Welt ist auch in der digitalen eine vernünftige Balance zwischen Freiheit und Sicherheit zu wahren und angesichts der Bedrohungslage neu auszubalancieren. Dabei sind einerseits die Besonderheiten der Cyberwelt, in der Straftäter in Distanz zu den Opfern und den Folgen ihrer Taten agieren, in den Blick zu nehmen. Andererseits ist sicherzustellen, dass der Rechtsgüterschutz digitaler Daten nicht hinter dem Schutz der körperlichen Gegenstände zurückbleibt, wenn Tatbegehung und Tatfolgen vergleichbar sind. Der materiell-strafrechtliche Schutz vor Delikten aus dem Phänomenbereich der Cyberkriminalität, der gegenwärtig im Wesentlichen durch die §§ 202a ff., §§ 303a f. StGB gewährt wird, ist dafür de lege lata nicht zureichend. Es fehlt - anders als bei den klassischen Deliktsbereichen - weitgehend an spezifischen Qualifikationstatbeständen und Regelbeispielen mit erhöhten Strafdrohungen, um auf schwerwiegende Taten mit einem gesteigerten Unrechtsgehalt tat- und schuldangemessen reagieren zu können. Dies hat zur Folge, dass beispielsweise Hacker, die sich mit großer krimineller Energie als Bande zusammengeschlossen oder gewerbsmäßig unbefugt Zugang zu einer Datenbank ver-

schaffen und dabei mehrere Millionen Datensätze abgreifen, derzeit lediglich eine Freiheitsstrafe von maximal drei Jahren oder eine Geldstrafe zu befürchten haben, obwohl wertvolle Daten gezielt ausgespäht werden, um aus der Straftat Gewinne zu erzielen. Auch können kritische Infrastrukturen oder die Sicherheit des Staates durch Cyberangriffe gefährdet werden. Tatvarianten, die geeignet sind, erhebliche Bedrohungslagen auszulösen, bleiben im Bereich des Kerncomputerstrafrechts anders als in der analogen Welt weitgehend ohne Auswirkung auf den in den Blick zu nehmenden Strafrahmen.

Beim Verdacht einer Straftat aus dem Bereich des Cybercrime können derzeit häufig die Täter nicht ermittelt und überführt werden, weil den Strafverfolgungsbehörden auch unter Berücksichtigung der Beschuldigtenrechte angemessene strafprozessualen Befugnisse für erfolgversprechende Ermittlungen in der digitalen Welt nicht oder nur eingeschränkt zur Verfügung stehen. Eine Überwachung der Telekommunikation in Form der „Serverüberwachung“ zur Identifizierung der Täter, zur Aufhellung der verwendeten Infrastruktur und zum Führen des Tatnachweises ist mangels Vorliegens einer Katalogtat nach § 100a Absatz 2 StPO derzeit rechtlich nicht zulässig. Diese technische Ermittlungsmaßnahme stellt aber oftmals den einzig erfolgversprechenden und zugleich verhältnismäßigen Ermittlungsansatz dar, da die Delikte der Cyberkriminalität in den allermeisten Fällen auch oder ausschließlich unter Zuhilfenahme von Telekommunikationsdiensten begangen werden.

Die geschilderten Defizite im materiellen Strafrecht und Strafprozessrecht werden weder der gesellschaftlichen und wirtschaftlichen Bedeutung digitaler Daten noch der Bedeutung des Grundrechts auf informationelle Selbstbestimmung in der heutigen digitalen Welt gerecht.

Vor diesem Hintergrund hat der Strafrechtsausschuss der Justizministerkonferenz und der Arbeitskreis II der Innenministerkonferenz die Gemeinsame Arbeitsgruppe Justiz/Polizei (GAG) bereits im Jahr 2011 beauftragt, sich unter anderem mit dem Thema Cybercrime zu befassen. Die Unterarbeitsgruppe „Cybercrime“ unter Federführung des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz hat aktuelle Rechtsfragen bei der Bekämpfung von Cybercrime erörtert und in ihrem 2013 vorgelegten Abschlussbericht u. a. die Schaffung qualifizierter Begehungsweisen für den Bereich der Computerdelikte empfohlen.

Zuletzt hat sich im Jahr 2018 die durch die Justizministerkonferenz eingesetzte und unter dem Vorsitz Hessens arbeitende Länder-Arbeitsgruppe „Digitale Agenda für das Straf- und Strafprozessrecht“ in ihrem Abschlussbericht mit der Thematik der

Bagatellisierung der Cyberkriminalität befasst und gesetzgeberischen Handlungsbedarf gesehen. Die Justizministerinnen und Justizminister der Länder haben auf ihrer Herbstkonferenz am 15. November 2018 den Abschlussbericht der Arbeitsgruppe des Strafrechtsausschusses „Digitale Agenda für das Straf- und Strafprozessrecht“ als Bestandsaufnahme der sich aus der technischen Entwicklung für die Strafverfolgungspraxis ergebenden Anforderungen und als Beitrag zur rechtspolitischen Diskussion zur Kenntnis genommen. Außerdem haben sie die Bundesministerin der Justiz und für Verbraucherschutz darum gebeten, die in dem Bericht enthaltenen Empfehlungen der Arbeitsgruppe zu würdigen und die ggf. erforderlichen gesetzgeberischen Schritte zu unternehmen.

B. Lösung

Der Entwurf beseitigt die unangemessene Bagatellisierung der Computer- und Datendelikte, indem er spezifische Qualifikationstatbestände und Regelbeispiele mit erhöhten Strafdrohungen schafft, um den differenzierten Unrechtsgehalt der in Betracht kommenden Fallgestaltungen sachgerecht erfassen zu können. Ferner verbessert der Entwurf die Möglichkeiten der Täterermittlung und Sachverhaltsaufklärung, indem er unter Wahrung des Verhältnismäßigkeitsgrundsatzes den Straftatenkatalog des § 100a Absatz 2 StPO um bestimmte, schwerwiegende Begehungsweisen der Cybercrime-Delikte ergänzt und damit den Anwendungsbereich der Telekommunikationsüberwachung in verfassungsmäßiger Weise an die Bedürfnisse einer effektiven Strafverfolgung anpasst. Der Entwurf trägt unter Berücksichtigung der betroffenen Grundrechtspositionen damit dem Umstand Rechnung, dass die Strafverfolgungsbehörden bei Delikten in der digitalen Welt darauf angewiesen sind, auch digital ermitteln zu können.

C. Alternativen

Beibehaltung des bisherigen, unbefriedigenden Zustands.

D. Haushaltsaufgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Keiner.

Davon Bürokratiekosten aus Informationspflichten.

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Keiner.

F. Weitere Kosten

Die vorgeschlagenen Neuregelungen im materiellen Strafrecht und die Erweiterung des Anwendungsbereichs der technischen Ermittlungsmaßnahmen können zu einem Mehraufwand für Polizei und Justiz führen, dessen Umfang derzeit noch nicht quantifizierbar ist. Der Mehraufwand ist angesichts des verbesserten Rechtsgüterschutzes gerechtfertigt.

Bundesrat **Drucksache** **248/19**

28.05.19

Gesetzesantrag
des Landes Nordrhein-Westfalen

Entwurf eines Strafrechtsänderungsgesetzes - Gesetz zur effektiveren Verfolgung der Computerkriminalität

Der Ministerpräsident
des Landes Nordrhein-Westfalen

Düsseldorf, 28. Mai 2019

An den
Präsidenten des Bundesrates
Herrn Ministerpräsidenten
Daniel Günther

Sehr geehrter Herr Bundesratspräsident,

die Landesregierung von Nordrhein-Westfalen hat beschlossen, dem Bundesrat den als Anlage beigefügten

> Entwurf eines Strafrechtsänderungsgesetzes – Gesetz zur effektiveren Verfolgung der Computerkriminalität

zuzuleiten.

Ich bitte, die Vorlage gemäß § 36 Absatz 2 der Geschäftsordnung des Bundesrates in die Tagesordnung der Sitzung des Bundesrates am 7. Juni 2019 aufzunehmen und anschließend den zuständigen Ausschüssen zur Beratung zuzuweisen.

Mit freundlichen Grüßen

Armin Laschet

Entwurf eines Strafrechtsänderungsgesetzes - Gesetz zur effektiveren Verfolgung der Computerkriminalität

Vom ….

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Strafgesetzbuchs

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

1. § 202a wird wie folgt geändert:

Nach Absatz 2 werden folgende Absätze 3 und 4 neu eingefügt:

„(3) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat,

2. in der Absicht handelt, durch die fortgesetzte Begehung von Taten nach Absatz 1 Daten einer unübersehbaren Anzahl von Personen auszuspähen,

3. durch die Tat die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet.

(4) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, wird bestraft, wer in den Fällen des Absatzes 3 Satz 2 Nummer 1 erste Alternative oder Nummern 2 oder 3 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat.“

2. § 202b wird wie folgt geändert:

a) Der bisherige § 202b wird § 202b Absatz 1.

b) Nach Absatz 1 werden folgende Absätze 2 und 3 neu eingefügt:

„(2) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat,

2. in der Absicht handelt, durch die fortgesetzte Begehung von Taten nach Absatz 1 Daten einer unübersehbaren Anzahl von Personen abzufangen,

3. durch die Tat die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur gefährdet oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet.

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren, wird bestraft, wer in den Fällen des Absatzes 2 Satz 2 Nummer 1 erste Alternative oder Nummern 2 oder 3 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat."

3. § 202c wird wie folgt geändert:

a) In Absatz 1 wird das Wort „, verbreitet“ gestrichen.

b) Nach Absatz 2 werden folgende Absätze 3 und 4 neu eingefügt:

„(3) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat, oder

2. die in Absatz 1 genannten Sicherungscodes und Computerprogramme einer großen Anzahl von Personen zugänglich macht.

(4) Mit Freiheitsstrafe von drei Monaten bis zu zehn Jahren wird bestraft, wer in den Fällen des Absatzes 3 Satz 2 Nummer 1 erste Alternative oder Nummer 2 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat.“

4. § 202d StGB wird wie folgt gefasst:

a) In Absatz 1 wird das Wort „, verbreitet“ gestrichen.

b) Nach Absatz 1 werden folgende Absätze 2 und 3 neu eingefügt:

„(2) In besonders schweren Fällen des Absatzes 1 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu fünf Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat,

2. die Datenhehlerei in der Absicht begeht, durch die fortgesetzte Tatbegehung sich oder einem anderen die Daten einer unübersehbaren Anzahl von Personen zu verschaffen oder die Daten einer großen Anzahl von Personen zugänglich zu machen,

3. durch die Tat die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit kritischer Infrastrukturen oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet.

(3) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, wird bestraft, wer in den Fällen des Absatzes 2 Satz 2 Nummer 1 erste Alternative oder Nummern 2 oder 3 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat.“

c) Der bisherige Absatz 2 wird Absatz 4; der bisherige Absatz 3 wird Absatz 5.

5. § 205 wird wie folgt geändert:

a) In § 205 Absatz 1 Satz 2 wird hinter den Angaben „202a“, „202b“ und „202d“ jeweils die Angabe „Abs. 1“ eingefügt.

b) In § 205 Absatz 2 Satz 1 werden die Wörter „; dies gilt nicht in den Fällen der §§ 202a, 202b und 202d“ gestrichen.

6. § 303b wird wie folgt geändert:

a) Absatz 4 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter „des Absatzes 2“ durch die Wörter „der Absätze 1 und 2“ ersetzt.

bb) In Satz 2 Nummer 1 werden nach dem Wort „herbeiführt“ die Wörter „oder in der Absicht handelt, durch die fortgesetzte Begehung von Computersabotage eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen“ eingefügt.

cc) In Satz 2 Nummer 2 wird das Wort „Computersabotage“ durch die Wörter „Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b“ ersetzt.

dd) Satz 2 Nummer 3 wird wie folgt neu gefasst: „durch die Tat die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit kritischer Infrastrukturen oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet.“

b) Nach Absatz 4 werden die folgenden Absätze 5 und 6 neu eingefügt:

„(5) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, wird bestraft, wer in den Fällen des Absatzes 4 Satz 2 Nummer 1, Nummer 2 erste Alternative oder Nummer 3 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat.

(6) Verursacht der Täter durch die Computersabotage wenigstens leichtfertig den Tod eines anderen Menschen, so ist die Strafe Freiheitsstrafe nicht unter drei Jahren, in minder schweren Fällen von einem Jahr bis zu zehn Jahren. Verursacht der Täter durch die Computersabotage wenigstens leichtfertig eine schwere Gesundheitsschä-

digung eines anderen Menschen, so ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen von sechs Monaten bis zu fünf Jahren."

c) Der bisherige Absatz 5 wird Absatz 7.

Artikel 2

Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch ... geändert worden ist, wird wie folgt geändert:

§ 100a Absatz 2 Nummer 1 wird wie folgt geändert:

a) Nach Buchstabe g) wird folgender Buchstabe h) neu eingefügt:

> „h) Computer- und Datendelikte nach §§ 202a Absatz 3 und 4, 202b Absatz 2 und 3, 202c Absatz 3 und 4, 202d Absatz 2 und 3, 303b Absatz 4 bis 6,“

b) Die bisherigen Buchstaben h) bis u) werden zu Buchstaben i) bis v).

Artikel 3

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung des Entwurfs und Notwendigkeit der Regelungen

Die Digitalisierung und die zunehmende Vernetzung über das Internet haben in vielen Bereichen zu einem Innovationsschub und zur Verbesserung der Lebensqualität beigetragen. In offenen Gesellschaften darf aber nicht außer Acht gelassen werden, dass durch so umfassende Veränderungsprozesse naturgemäß auch neue Verletzbarkeiten entstehen und dadurch Schutzbedürfnisse neu gewichtet werden müssen.

Die Kehrseite der Vorzüge der Digitalisierung ist die Cyberkriminalität, die zunehmende Gefahren für die Sicherheit der Bürgerinnen und Bürger, der Unternehmen und des Staates mit sich bringt. Daten haben deutlich an Wertigkeit zugenommen. Sie werden deshalb mehr und mehr begehrtes Ziel von Straftätern.

Die bekannt gewordenen „Datenleaks“ der letzten Jahre verdeutlichen dabei die enorme Dimension, die unberechtigte Datenabgriffe inzwischen erlangt haben. So wurden bei MySpace 360 Mio. Datensätze, bei Sony 102 Mio. Datensätze, bei Dropbox 69 Mio. Datensätze, bei LinkedIn 177 Mio. Datensätze, bei Yahoo 500 Mio. Datensätze und bei Ashley Madison 36 Mio. Datensätze unbefugt abgegriffen. Eine im Januar 2019 bekanntgewordene Sammlung von Passwort-Leaks enthielt bei einem Volumen von 935 Gigabyte über 2,2 Milliarden Accounts. Bundesweites Aufsehen erregte Ende des Jahres 2018/Anfang 2019 die Meldung, dass ein Hacker mit offenbar einfachen Mitteln massenhaft persönliche Daten von mehreren hundert Politikern, Prominenten und Journalisten ausgespäht und auf der Internetplattform Twitter verbreitet hatte. Neben diesen „Datenleaks“ kam es zuletzt auch vermehrt zu Cyberattacken, bei denen Verschlüsselungstrojaner (sog. Ransomware) in die IT-Infrastruktur von Unternehmen oder Krankenhäusern eingeschleust wurden, die dort zu massiven Betriebsstörungen und Schäden führten.

Diese aktuellen Vorfälle zeigen, dass Cyberkriminalität inzwischen ein Ausmaß erreicht hat, das das Sicherheitsgefühl der Menschen massiv bedroht und das Potential hat, die Grundlagen von Demokratie, Staat und Wirtschaft zu gefährden. Die wirtschaftlichen Schäden, die etwa durch Produktionsausfälle, den Verlust von Geschäftsgeheimnissen oder die Kosten für eine Wiederherstellung von Daten entstehen, sind groß. Gleiches gilt für die negativen Folgen, die mit der Veröffentlichung sensibler Informationen oder dem Eindringen in Datenverarbeitungen verbunden sein können. Im Extremfall können Cyberangriffe etwa auf Krankenhäuser, Flughäfen oder Verteidigungseinrichtungen sogar den Verlust von Menschenleben fordern. Daten und Datenverarbeitungssysteme rücken mit ihrer

wachsenden Bedeutung für die Bürgerinnen und Bürger, den Staat und die Wirtschaft in den Fokus organisierter kriminelle Strukturen.

Es ist Aufgabe des Strafrechts, die für solche Angriffe verantwortlichen Personen zügig zu ermitteln und schuldangemessen zu bestrafen - nicht zuletzt um andere potentielle Täter abzuschrecken, die Gesellschaft vor Cyberangriffen zu schützen, die mittels der Digitalisierung erzielte Wirtschaftskraft nicht durch Straftaten zu gefährden und das Vertrauen in die staatliche Handlungsfähigkeit zu erhalten. Diese Aufgabe kann das Strafrecht derzeit jedoch nur bedingt erfüllen.

Wie in der analogen Welt ist auch in der digitalen eine vernünftige Balance zwischen Freiheit und Sicherheit zu wahren und angesichts der Bedrohungslage neu auszubalancieren. Dabei sind einerseits die Besonderheiten der Cyberwelt, in der Straftäter in Distanz zu den Opfern und den Folgen ihrer Taten agieren, in den Blick zu nehmen. Andererseits ist sicherzustellen, dass der Rechtsgüterschutz digitaler Daten nicht hinter dem Schutz der körperlichen Gegenstände zurückbleibt, wenn Tatbegehung und Tatfolgen vergleichbar sind. Der materiell-strafrechtliche Schutz vor Delikten aus dem Phänomenbereich der Cyberkriminalität, der gegenwärtig im Wesentlichen durch die §§ 202a ff., §§ 303a f. StGB gewährt wird, ist dafür de lege lata nicht zureichend. Anders als bei den klassischen Eigentums- und Vermögensdelikten fehlt es weitgehend an spezifischen Qualifikationstatbeständen und Regelbespielen mit erhöhten Strafdrohungen, um Fallgestaltungen mit einem gesteigerten Unrechtsgehalt in einer angemessenen Weise erfassen zu können und der Bedeutung der Daten in der digitalen Welt von heute gerecht zu werden. Lediglich bei der Computersabotage finden sich Regelungen für qualifizierende und besonders schwere Fälle (§§ 303b Absätze 2 und 4 StGB), wobei die Computersabotage im Fall des § 303b Absatz 1 Nummer 1 StGB ihrerseits eine Qualifikation der Datenveränderung nach § 303a StGB darstellt. Im Übrigen kann im Bereich der Cybercrime-Delikte auf schwerwiegende Taten mit einem gesteigerten Unrechtsgehalt nicht tat- und schuldangemessen reagiert werden.

Dies hat zur Folge, dass beispielsweise Hacker, die sich mit großer krimineller Energie als Bande zusammengeschlossen oder gewerbsmäßig unbefugt Zugang zu einer Datenbank verschaffen und dabei mehrere Millionen Datensätze abgreifen, derzeit lediglich eine Freiheitsstrafe von maximal drei Jahren oder eine Geldstrafe zu befürchten haben, obwohl wertvolle Daten ausgespäht werden, um aus der Straftat Gewinne zu erzielen. Auch können kritische Infrastrukturen oder die Sicherheit des Staates durch Cyberangriffe gefährdet werden. Der Bundesgesetzgeber hat bereits 2007 mit dem 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität auf neuen Herausforderungen reagiert, die sich aus dem rasanten Fortschritt im Bereich der Informationstechnologie und damit eröffnete Missbrauchsmöglichkeiten ergeben. In den vergangenen zwölf Jahren ist die informationstechnologische Entwicklung weiter vorangeschritten. Die Digitalisierung nimmt heute eine herausragende Bedeutung im gesellschaftlichen, wirtschaftlichen

und politischen Leben ein. Vernetzte Systeme erleichtern einen Informationsaustausch, zugleich werden die Systeme verwundbarer und offen für kriminelle Zugriffe von außen. Daraus folgen neue Tatmodalitäten mit gravierenden gesellschaftlichen und wirtschaftlichen Folgen. Der technische Fortschritt und damit einhergehend auch die wachsende Bedrohung durch die Cyberkriminalität haben dazu geführt, dass das Kerncomputerstrafrecht in schwerwiegenden Fällen dem verwirklichen Unrecht und general- wie spezialpräventiven Strafbedürfnissen nicht mehr gerecht wird. Deshalb ist auch die strafrechtliche Bekämpfung der Computerkriminalität fortzuentwickeln.

Beim Verdacht einer Straftat aus dem Bereich des Cybercrime können derzeit häufig die Täter nicht ermittelt und überführt werden, weil den Strafverfolgungsbehörden auch unter Berücksichtigung der Beschuldigtenrechte angemessene strafprozessuale Befugnisse für erfolgversprechende Ermittlungen in der digitalen Welt nicht oder nur eingeschränkt zur Verfügung stehen. Eine Überwachung der Telekommunikation in Form der „Serverüberwachung“ zur Identifizierung der Täter, zur Aufhellung der verwendeten Infrastruktur und zum Führen des Tatnachweises ist mangels Vorliegens einer Katalogtat nach § 100a Absatz 2 StPO derzeit rechtlich nicht zulässig. Diese technische Ermittlungsmaßnahme stellt aber oftmals den einzig erfolgversprechenden und zugleich verhältnismäßigen Ermittlungsansatz dar, da die Delikte der Cyberkriminalität in den allermeisten Fällen auch oder ausschließlich unter Zuhilfenahme von Telekommunikationsdiensten begangen werden.

Das gilt zum Beispiel insbesondere für die Straftaten im Zusammenhang mit der sog. Botnetzkriminalität, bei der zahlreiche Computersysteme über das Internet mittels einer Schadsoftware infiltriert und zu einem mitunter mehrere Millionen Geräte umfassenden Verbund, einem sog. Botnetz, zusammengeschlossen werden. Dieser Verbund lässt sich durch den Angreifer über das Internet fernsteuern und beispielsweise für sog. „Distributed-denial-of-service (DDos)-Attacken“ benutzen, die darauf abzielen, ein bestimmtes Zielsystem durch eine Vielzahl von gleichzeitigen Anfragen der zum Botnetz gehörenden Rechner derart zu belasten, dass dieses unter der Last des Datenaufkommens zusammenbricht. So führte im Oktober 2016 der Angriff des „Mirai-Botnetzes“, bestehend aus ca. 300.000 Geräten internetfähiger Steuerungs- und Überwachungshardware (IoT), zum Ausfall eines großen DNS-Dienstes, wodurch mehrere große Plattformen nicht mehr erreichbar waren. Derartige Straftaten können nur mit Mitteln der modernen Informationstechnik, insbesondere des Internets, begangen werden, so dass technische Ermittlungsmaßnahmen oftmals den einzigen Ermittlungsansatz darstellen, um die Täter zu identifizieren und die dahinter stehenden Netzwerke aufzudecken.

Die geschilderten Defizite im materiellen Strafrecht und Strafprozessrecht werden weder der gesellschaftlichen und wirtschaftlichen Bedeutung digitaler Daten und informationstechnischer Systeme noch der Bedeutung des Grundrechts auf informationelle Selbstbestimmung in der heutigen digitalen Welt gerecht.

Diese Defizite sollen durch den Entwurf behoben werden. Der Entwurf zielt darauf ab, den strafrechtlichen Schutz digitaler Daten und informationstechnischer Systeme an deren gestiegene gesellschaftliche und wirtschaftliche Bedeutung unter gleichzeitiger Berücksichtigung der Besonderheiten der digitalen Welt anzupassen und den Strafverfolgungsbehörden die rechtlichen und zugleich verhältnismäßigen Ermittlungsbefugnisse an die Hand zu geben, die zur effektiven Verfolgung der Cyberkriminalität unabdingbar sind. Der Entwurf dient damit letztlich dem Schutz der modernen Informationsgesellschaft vor einer wachsenden Bedrohung durch die Cyberkriminalität.

Zu diesem Zweck sieht der Entwurf vor, Strafzumessungsregeln für besonders schwere Fälle, Qualifikationstatbestände und erfolgsqualifizierte Tatbestände mit erhöhten Strafdrohungen für die §§ 202a ff., § 303b StGB zu schaffen. Der Entwurf beschränkt sich dabei mit Blick auf den Schuld- und Verhältnismäßigkeitsgrundsatz auf solche Fallgestaltungen, die typischerweise einen deutlich gesteigerten Unrechtsgehalt aufweisen. So sieht der Entwurf aufgrund der hohen kriminellen Energie bzw. des hohen Schadens- und Gefahrenpotentials - für die einzelnen Straftatbestände differenziert - erhöhte Strafdrohungen für solche Taten vor, die gewerbs- und/oder bandenmäßig begangen werden, die Daten einer unübersehbaren Anzahl von Personen bzw. die Weitergabe von illegal erlangten Daten oder digitalen Tatwerkzeugen an eine große Anzahl von Personen betreffen, Daten kritischer Infrastrukturen angehen, die Sicherheit der Bundesrepublik Deutschland oder der Länder gefährden oder leichtfertig den Tod eines Menschen oder eine schwere Gesundheitsschädigung verursachen.

Soweit sich der Entwurf dabei für die Strafrahmen der Delikte aus der digitalen Welt an die Straftatbestände aus der analogen Welt anlehnt, wird nicht verkannt, dass die in beiden Deliktsbereichen betroffenen Tatobjekte ihrem Wesen nach durchaus Unterschiede aufweisen. So sind digitale Daten im Gegensatz zu körperlichen Gegenständen nicht exklusiv und nicht abnutzbar, das heißt, prinzipiell beliebig kopierbar und von mehreren Personen zur gleichen Zeit ohne Verschleiß nutzbar. Daher ist es zum Beispiel im Falle eines „Datendiebstahls“ möglich, dass dem Opfer die Nutzung der vom Täter kopierten Daten erhalten bleibt, während das Opfer eines Sachdiebstahls den entwendeten körperlichen Gegenstand nicht mehr nutzen kann. Auch hat der Täter in der Regel eine geringere Hemmschwelle für die Begehung der Tat zu überwinden. Wegen der abstrakt-technischen Begehungsweise agiert der Straftäter oft weit entfernt von dem Ort, an dem der Erfolg der Tat spürbar wird. Die Straftat wird nicht im unmittelbaren persönlichen Kontakt zum Opfer verwirklicht. Oftmals tritt zu der örtlichen und persönlichen Distanz auch noch eine zeitliche hinzu, weil sich die wahrnehmbaren Folgen der Tat erst nach Tagen oder sogar Wochen bzw. Monaten manifestieren, wenn ganze Informationssysteme zusammenbrechen. Jedoch hindern diese Wesensunterschiede den Gesetzgeber nicht, für digitale Daten angesichts ihres Bedeutungszuwachses ein vergleichbares Schutzniveau wie für körperliche Gegenstände vorzusehen, wenn die Tatbegehung auch von einer

vergleichbaren kriminellen Energie getragen ist, zumal die Bevölkerung inzwischen die Cyberkriminalität ebenso als massive Bedrohung ihrer Sicherheit im privatesten Lebensbereich wahrnimmt wie die klassische Eigentums- und Vermögenskriminalität. Zudem können die Folgen der Taten in der digitalen Welt mindestens ebenso schwer sein wie bei Taten in der analogen Welt.

In Ergänzung zu den materiell-rechtlichen Strafschärfungen sieht der Entwurf vor, die strafprozessualen Ermittlungsbefugnisse der Strafverfolgungsbehörden auszubauen, indem er - bei Wahrung der verfassungsrechtlichen Vorgaben und unter Berücksichtigung der Bedürfnisse einer effektiven Strafverfolgung - den Straftatenkatalog des § 100a Absatz 2 StPO und damit den Anwendungsbereich der Telekommunikationsüberwachung erweitert. Der Entwurf ermöglicht es somit den Strafverfolgungsbehörden, bei digitalen Delikten auch digital ermitteln zu können. Er beschränkt diese Möglichkeit zur Wahrung des Verhältnismäßigkeitsgrundsatzes aber von vornherein auf solche Delikte, die als schwer einzustufen sind. Damit trägt er den Vorgaben des Bundesverfassungsgerichts Rechnung, wonach die genannte Ermittlungsmaßnahme zur Rechtfertigung des mit ihnen verbundenen, nicht unerheblichen Grundrechtseingriffs auf die Verfolgung von Straftaten mit einem entsprechenden Schweregrad zu beschränken sind (vgl. etwa BVerfG NJW 2016, 1781 [1784]; NJW 2012, 833 [836]; NJW 2010, 833 [841]). Soweit die Delikte aber den notwendigen Schweregrad erreichen, ist ihre Aufnahme in den Anlasstatenkatalog der Telekommunikationsüberwachung nach § 100a StPO nicht zur zulässig, sondern auch geboten, da die wirksame Aufklärung gerade schwerer Straftaten - wie das Bundesverfassungsgericht wiederholt betont hat (BVerfG NJW 2004, 999 [1008]) - ein wesentlicher Auftrag des rechtsstaatlichen Gemeinwesens ist. In Erfüllung dieses Auftrags bestimmt der Entwurf zur effektiven Verfolgung der Computerkriminalität in den neuen § 100a Absatz 2 Nummer 1 Buchstabe h StPO-E, dass auch schwere bzw. besonders schwere Computer- und Datendelikte als Anlasstaten für die dort geregelte Ermittlungsmaßnahme in Betracht kommen. Insgesamt betrachtet, schafft der Entwurf durch das Zusammenspiel der materiellen Strafschärfungen mit den verbesserten strafprozessualen Ermittlungsbefugnissen die Möglichkeit, auf neue Verletzbarkeiten aufgrund der Cyberkriminalität zu reagieren, Schutz- und Strafbedürfnissen neu und zugleich nachhaltig sowie angemessen gerecht zu werden, das Vertrauen der Bevölkerung in die Handlungsfähigkeit staatlicher Organe und in den Rechtsstaat zu erhalten sowie die Qualität der Bürgerfreiheiten zu sichern.

II. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Art. 74 Absatz 1 Nummer 1 des Grundgesetzes (Strafrecht, gerichtliches Verfahren).

III. Auswirkungen

Durch die vorgeschlagenen Änderungen im materiellen Strafrecht und Strafprozessrecht, insbesondere durch die Erweiterung des Anwendungsbereichs der technischen Ermittlungsmaßnahme nach § 100a StPO kann ein Mehraufwand für die Strafverfolgungsbehörden entstehen, dessen Umfang derzeit noch nicht quantifizierbar ist. Der Mehraufwand ist jedoch angesichts des verbesserten Rechtsgüterschutzes gerechtfertigt. Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Strafgesetzbuchs)

Zu Nummer 1 (§ 202a Absätze 3 und 4 StGB-E)

Der Entwurf schafft mit den Absätzen 3 und 4 des § 202a StGB-E einen Qualifikationstatbestand und eine Strafzumessungsregel für besonders schwere Fälle der Datenausspähung, die sich vom Strafrahmen des Grundtatbestandes nicht immer angemessen erfassen lassen. § 202a StGB sieht de lege lata keine Möglichkeit vor, Taten mit einem besonderen Unrechtsgehalt schärfer und damit schuldangemessen zu bestrafen. Insbesondere haben bisher bestimmte Tatvarianten, die sich in vielen Bereichen des Kernstrafrechts strafschärfend auswirken, wie etwa eine gewerbs- oder bandenmäßige Tatbegehung, bei der Datenausspähung keine Auswirkung auf den in Betracht kommenden Strafrahmen. Dies ist insbesondere bei einem Vergleich mit den klassischen Diebstahlsdelikten, die in den §§ 243 ff. StGB Strafschärfungen für qualifizierte Begehungsweisen erhalten, nicht sachgerecht. Im Einzelnen:

1. Der vorgeschlagene Absatz 3 des § 202a StGB-E sieht eine Strafzumessungsregel für besonders schwere Fälle der Datenausspähung mit einem erhöhten Strafrahmen von drei Monaten bis zu fünf Jahren vor. Dabei werden in Nummer 1 bis 3 des § 202a Absatz 4 Satz 2 StGB-E zur Konkretisierung mehrere Regelbeispiele benannt:

   - Nach Nummer 1 des § 202a Absatz 4 Satz 2 StGB-E liegt ein besonders schwerer Fall in der Regel dann vor, wenn das Ausspähen von Daten gewerbs- oder bandenmäßig begangen wird. Die Auslegung dieser Merkmale kann sich an der Auslegung der entsprechenden Merkmale in anderen Regelungen im StGB orientieren (vgl. etwa §§ 243 Absatz 1 Satz 2 Nummer 3, 244 Absatz 1 Nummer 2, 263 Absatz 3 Satz 2 Nummer 1 StGB). Im Falle der bandenmäßigen Begehung muss sich die Bandenabrede auf eine Tat nach §§ 202a bis 202d, 263a, 269 oder 303b beziehen. Erfasst sind also nicht nur die Computer- und Datendelikte im engeren Sinn nach §§ 202a bis 202d, 303b StGB, sondern auch die oftmals mitverwirklichten Delikte des Computerbetrugs nach § 263a StGB und der Fälschung beweiserheblicher Daten nach § 269 StGB. Dadurch wird sichergestellt, dass auch solche Banden unter das Regelbeispiel fallen, deren überwiegendes Ziel die Begehung von Verwertungstaten ist und für die die Begehung etwa einer Datenausspähung lediglich einen den eigentlichen Bandenzweck vorbereitenden Charakter aufweist.

Der im Vergleich zum Grundtatbestand erhöhte Strafrahmen rechtfertigt sich aus der erhöhten kriminellen Energie, die mit der gewerbs- oder bandenmäßigen Tatbegehung im Regelfall verbunden ist. Hinzu kommt bei Bandendelikten die erhöhte Gefährlichkeit, die aus dem auf eine gewisse Dauer angelegten Zusammenschluss von mehr als zwei Tätern zu einer Bande und dem damit einhergehenden Anreiz zur Begehung weiterer Straftaten resultiert. Anders als bei den Diebstahlsdelikten (vgl. § 244 Absatz 1 Nummer 2 StGB), aber entsprechend den Betrugsdelikten (§ 263 Absatz 3 Satz 2 Nummer 1 StGB), gestaltet der Entwurf die bandenmäßige Tatbegehung lediglich als Regelbeispiel und nicht als Qualifikation aus, um unverhältnismäßige Sanktionen im Einzelfall zu verhindern. Dies gilt umso mehr, als der Entwurf - anders als § 244 Absatz 1 Nummer 2 StGB, aber wie § 263 Absatz 3 Satz 2 Nummer 1 StGB - auf das Erfordernis der Mitwirkung eines anderen Bandenmitglieds an der Tat verzichtet, so dass aufgrund der fehlenden Mitwirkung eines zweiten Bandenmitglieds bei der Tatausführung die Gefahr für das geschützte Rechtsgut im Einzelfall auch geringer sein kann als beim Bandendiebstahl nach § 244 Absatz 1 Nummer 2 StGB.

- Nummer 2 des § 202a Absatz 4 Satz 2 StGB-E sieht ein Regelbeispiel für den Fall vor, dass der Täter in der Absicht handelt, durch die fortgesetzte Tatbegehung Daten einer unübersehbaren Anzahl von Personen auszuspähen. Mit dem Wort „ausspähen“ wird auf die Tathandlung des Grundtatbestandes nach § 202a Absatz 1 StGB Bezug genommen, so dass - wie beim Grundtatbestand - auch für die Verwirklichung des Regelbeispiels die bloße Zugangsverschaffung ausreicht. Das Regelbeispiel ist erfüllt, wenn der Täter in der Absicht handelt, sich oder einem anderen durch die fortgesetzte Tatbegehung den Zugang zu Daten von einer unübersehbaren Anzahl von Personen zu verschaffen.

  Für die Zugangsverschaffung genügt es dabei, wenn der Täter oder ein anderer so weit in ein informationstechnisches System eindringt, dass er ohne weiteres Hindernis im nächsten Schritt auf die nicht für ihn bestimmten Daten zugreifen kann. Er muss sich also nicht diese Daten, sondern lediglich den Zugang zu den Daten verschaffen (indem er sich etwa das Passwort oder einen anderen Zugangsschlüssel besorgt). Dies betrifft die in der Praxis auftretenden Fälle, in denen der Täter den erlangten Zugang nicht unmittelbar für den Download der Daten nutzt, sondern sich, um unentdeckt zu bleiben, lediglich den konkreten Zugriff auf wertvoll erscheinende Daten sichert.

  Bei der „unübersehbaren Anzahl von Personen“ handelt es sich um einen unbestimmten Rechtsbegriff, der nach objektiven Gesichtspunkten unter Berücksichtigung des technischen Fortschritts zu bestimmen ist. Eine unübersehbare Anzahl von Personen liegt entsprechend den zu § 309 Absatz 2 StGB entwickelten Grundsätzen dann vor, wenn die Daten von einer

so großen Zahl von Personen ausgespäht werden, dass sie für einen objektiven Beobachter nicht ohne weiteres übersehbar ist. Mit diesem Regelbeispiel sollen insbesondere auch solche Fälle erfasst werden, in denen ein Täter bei einer nicht überschaubaren Zahl von unterschiedlichen Personen jeweils nur eine kleine Menge an Daten ausspäht. Das Regelbeispiel ist dabei - ebenso wie das ähnliche Regelbeispiel in § 263 Absatz 3 Satz 2 Nummer 2 Alternative 2 StGB - nicht erst dann erfüllt, wenn der Täter eine unübersehbare Anzahl von Personen ausgespäht hat, sondern bereits dann, wenn er in der Absicht handelt, die Daten einer unübersehbaren Zahl von Personen auszuspähen. Liegt eine solche Absicht vor, reicht schon die erste Tatbegehung für die Erfüllung des Regelbeispiels aus, auch wenn es dann entgegen der Intention des Täters nicht zu weiteren Ausspähhandlungen bei anderen Personen kommt. Mit dem Erfordernis einer nicht nur großen, sondern unübersehbaren Anzahl von Personen werden alle Fälle erfasst, in denen sich die typische, enorme Dimension der Cyberkriminalität verwirklicht und die Zahl der Betroffenen Ausmaße erreicht, dass eine zielgerichtete Warnung an die Opfer der Straftaten über einen erfolgten Zugriff nicht möglich ist. Gerade diese Unbestimmtheit führt zu einer großen Verunsicherung der Bevölkerung durch Cyberkriminalität, da jeder Nutzer eines Internetdienstes von einem bekannt werdenden Angriff betroffen sein könnte. Aufgrund der fehlenden Kenntnis der persönlichen Betroffenheit ist es kaum möglich, selbst Abwehrmaßnahmen zu ergreifen. Die Zugehörigkeit der Daten zu Personen bestimmt sich nach datenschutzrechtlichen Grundsätzen über den Personenbezug von Daten, so dass Daten von Plattformnutzern nicht dem Betreiber der Plattform, sondern den Nutzern zuzuordnen sind.

- Nach Nummer 3 des § 202a Absatz 4 Satz 2 StGB-E liegt ein besonders schwerer Fall in der Regel vor, wenn der Täter durch die Tat die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit kritischer Infrastrukturen oder die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet. Der Begriff der kritischen Infrastrukturen ist in Anlehnung an die Legaldefinition in § 2 Absatz 10 des Gesetzes für Sicherheit in der Informationstechnik (BSIG) zu verstehen. Kritische Infrastrukturen sind danach Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Zu den kritischen Infrastrukturen im Sinne des hier vorgeschlagenen Regelbeispiels zählen also zum Beispiel Krankenhäuser, Kernkraftwerke, Flughäfen oder Banken. Die Aufnahme dieser kritischen Infrastrukturen in den Katalog der Regelbeispiele trägt dem Umstand Rechnung, dass diese Infrastrukturen besonders schutzwürdig sind,

da sie aufgrund der fortschreitenden Digitalisierung in hohem Maße auf informationstechnische Systeme angewiesen sind und unberechtigte Zugriffe auf diese Systeme schwerwiegende Folgen auch für die Allgemeinheit haben können. Der Schutzbereich der kritischen Infrastrukturen umfasst in Anlehnung an § 8a Absatz 1 Satz 1 BSIG deren Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität und Vertraulichkeit. Hiervon hängt die zu schützende Funktionsfähigkeit der kritischen Infrastrukturen ab. Die Voraussetzungen sind in einer für künftige Entwicklungen offenen und zugleich einer rechtssicheren Anwendung zugänglichen Weise gefasst worden.

Die Sicherheit der Bundesrepublik Deutschland umfasst die innere und äußere Sicherheit. Die Begriffsbestimmung kann sich - wie bei § 303b Absatz 4 Satz 2 Nummer 3 StGB - an § 92 Absatz 3 Nummer 2 StGB orientieren. Gemeint ist also die Fähigkeit der Bundesrepublik, sich nach außen und innen gegen Störungen zur Wehr zu setzen. Entsprechendes gilt für die Sicherheit eines der Länder der Bundesrepublik Deutschland.

Nach dem Entwurf ist nicht erforderlich, dass die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit einer kritischen Infrastruktur oder die Sicherheit der Bundesrepublik Deutschland bzw. eines ihrer Länder durch die Tat beeinträchtigt wird. Vielmehr soll aus generalpräventiven Gründen bereits die konkrete Gefährdung genügen, um die erhöhte Strafdrohung der Strafzumessungsregel auszulösen.

2. Der vorgeschlagene Absatz 4 des § 202a StGB-E sieht schließlich einen Qualifikationstatbestand vor. Danach wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, bestraft, wer in den Fällen des Absatzes 4 Satz 2 Nummer 1 erste Alternative und Nummern 2 oder 3 als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Delikten nach §§ 202a bis 202d, 263a, 269 oder 303b verbunden hat. Der Entwurf erhebt damit - in Anlehnung an die Regelungen in §§ 244a, 260a und 263 Absatz 5 StGB - die bandenmäßige Begehung von Datenausspähungen unter erschwerenden Umständen (nämlich unter den Umständen des Absatz 3 Satz 2 Nummer 1 erste Alternative oder Nummern 2 oder 3) zu einem Verbrechenstatbestand. Hierdurch wird erreicht, dass zur schweren Kriminalität zählende Cyberattacken insbesondere aus dem Bereich des Organisierten Cybercrime von den Gerichten in einer schuldangemessenen Weise bestraft werden können. Zum Organisierten Cybercrime zählt die vom Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Computer- und Datendelikten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind und an denen mehr als zwei Beteiligte auf längere oder unbestimmte Dauer

arbeitsteilig unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen, unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken (vgl. Ziff. 2. 1 der Gemeinsamen Richtlinien der Justizminister/-senatoren und der Innenminister/-senatoren der Länder über die Zusammenarbeit bei der Verfolgung der Organisierten Kriminalität; Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Auflage 2018, Kapitel 1 Rn. 37). Der Bekämpfung dieser besonders schwerwiegenden Kriminalitätsform dient Absatz 4, der insbesondere durch die kumulative Verbindung der gewerbsmäßigen mit der bandenmäßigen Begehungsweise wesentliche Bereiche der Organisierten Cyber-Kriminalität erfasst.

Zu Nummer 2 (§ 202b StGB-E)

Zu Buchstabe a (Absatz 1 StGB-E)

Der Entwurf sieht vor, dass der bisherige Normtext des § 202b als neuer Absatz 1 des § 202b StGB-E den Grundtatbestand für das Abfangen von Daten bildet.

Zu Buchstabe b (Absätze 2 und 3 StGB-E)

Der Entwurf fügt in § 202b StGB zudem einen neuen Absatz 2 mit einer Strafzumessungsregel für besonders schwere Fälle des Abfangens von Daten und einen neuen Absatz 3 mit einem Qualifikationstatbestand ein, um auch Taten mit einem gesteigerten Unrechtsgehalt in einer schuldangemessenen, den Bedürfnissen der General- und Spezialprävention genügenden Weise bestrafen zu können. Im Einzelnen:

1. In diesem Sinne sieht Absatz 2 des § 202b StGB-E vor, besonders schwere Fälle des Abfangens von Daten mit einer Freiheitsstrafe von drei Monaten bis zu fünf Jahren zu bestrafen. Zur Konkretisierung werden in den Nummern 1 bis 3 des § 202b Absatz 3 Satz 2 StGB-E - in Anlehnung an § 202a Absatz 3 Satz 2 StGB-E - Regelbeispiele für besonders schwere Fälle benannt. Ein besonders schwerer Fall liegt danach in der Regel vor, wenn das Abfangen von Daten gewerbs- oder bandenmäßig begangen wird (Nummer 1), eine unübersehbare Anzahl von Personen betrifft (Nummer 2) oder kritische Infrastrukturen oder die Sicherheit der Bundesrepublik Deutschland bzw. eines ihrer Länder gefährdet (Nummer 3). Für diese Regelbeispiele gelten die obigen Ausführungen zu § 202a Absatz 3 StGB-E

entsprechend mit der Maßgabe, dass in den Fällen des § 202b Absatz 2 StGB-E im Gegensatz zu § 202a Absatz 3 StGB-E ein Verschaffen der Daten und nicht des bloßen Zugangs zu Daten erforderlich ist. Dies ergibt sich daraus, dass bereits der Grundtatbestand des Abfangens von Daten nach § 202b Absatz 1 StGB-E - im Unterschied zum Ausspähen von Daten nach § 202a Absatz 1 StGB-E - eine bloße Zugangsverschaffung nicht ausreichen lässt.

2. Der in Absatz 3 des § 202b StGB-E vorgesehene Qualifikationstatbestand dient in Anlehnung an § 202a Absatz 4 StGB-E insbesondere der Bekämpfung der schweren Kriminalitätsform des Organisierten Cybercrime, indem er die bandenmäßige Tatbegehung unter erschwerten Umständen (nämlich unter den Umständen des Absatz 2 Satz 2 Nummer 1 erste Alternative oder Nummern 2 oder 3) mit einer erhöhten Strafdrohung von sechs Monaten bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren, belegt. Anders als § 202a Absatz 4 StGB-E wurde dabei davon abgesehen, den § 202b Absatz 3 StGB-E als Verbrechenstatbestand auszugestalten, um dem auch bereits im jeweiligen Grundtatbestand zum Ausdruck kommenden abgestuften Unrechtsgehalt beider Straftatbestände Rechnung zu tragen.

Zu Nummer 3 (§ 202c StGB-E)

Zu Buchstabe a (Absatz 1 StGB-E)

Absatz 1 des § 202c StGB, der das Vorbereiten des Ausspähens und Abfangens von Daten als abstraktes Gefährdungsdelikt unter Strafe stellt, wird durch den Entwurf in der Form geändert, dass im Vergleich zur bisherigen Fassung auf die explizite Erwähnung der Tathandlung des Verbreitens im Grundtatbestand verzichtet wird. Die Verbreitung ist nur eine Form des ebenfalls in Absatz 1 erwähnten Zugänglichmachens, bei der die Tatobjekte an einen größeren, nach Zahl und Individualität unbestimmten oder für den Täter nicht mehr kontrollierbaren Personenkreis weitergegeben werden (vgl. zur Definition der Tathandlung des Verbreitens etwa Eisele in: Schönke/Schröder, 30. Auflage 2018, § 202d Rn. 12). Diese Form der Zugänglichmachung an eine große Anzahl von Personen soll künftig aufgrund des gesteigerten Unrechtsgehalts in § 202c Absatz 3 Satz 2 Nummer 2 StGB-E als Regelbeispiel für einen besonders schweren Fall einer Vorbereitungshandlung erfasst werden. Die Verbreitung an einen Personenkreis, der das Kriterium der großen Anzahl nicht erfüllt, bleibt als sonstige Form der Zugänglichmachung strafbar.

Zu Buchstabe b (Absätze 3 und 4 StGB-E)

Der Entwurf sieht ferner vor, zwei neue Absätze 3 und 4 in § 202c StGB einzufügen, um auch dem erhöhten Unrechtsgehalt besonders schwerer oder qualifizierter, abstrakt gefährlicher Vorbereitungshandlungen in einer schuldangemessenen Weise Rechnung tragen zu können.

1. Zu diesem Zweck schafft der Entwurf mit dem neuen Absatz 3 des § 202c StGB-E eine Strafzumessungsregel für besonders schwere Fälle von selbständig strafbaren Vorbereitungshandlungen. Ein besonders schwerer Fall liegt nach Satz 2 des § 202c Absatz 3 StGB-E in der Regel vor, wenn die Vorbereitungshandlung gewerbs- oder bandenmäßig begangen wird (Nummer 1) oder die in Absatz 1 genannten Tatobjekte in Form von Sicherungscodes oder Computerprogrammen einer großen Anzahl von Personen zugänglich gemacht werden (Nummer 2). Eine große Anzahl von Personen liegt dabei entsprechend der zu § 263 Absatz 3 Nr. 2 StGB entwickelten Maßstäbe jedenfalls dann vor, wenn der Personenkreis mehr als fünfzig Personen umfasst. Die vorgeschlagenen Regelbeispiele weisen einen über den Normalfall hinausgehenden, gesteigerten Unrechts- und Gefährdungsgehalt auf, der sich mit dem Strafrahmen des Grundtatbestandes des § 202c Absatz 1 StGB nicht immer angemessen erfassen lässt.

2. Der vorgeschlagene neue Absatz 4 des § 202c StGB enthält einen Qualifikationstatbestand für den Fall, dass die Vorbereitungshandlung bandenmäßig begangen wird und dabei zugleich eines der Regelbeispiele aus § 202c Absatzes 3 Satz 2 Nummer 1 erste Alternative oder Nummer 2 StGB-E verwirklicht. Wer also bei der Vorbereitung eines Ausspähens oder Abfangens von Daten banden- und zugleich gewerbsmäßig handelt oder wer bei der Vorbereitung als Mitglied einer Bande die Sicherungscodes bzw. Computerprogramme einer großen Anzahl von Personen zugänglich macht, hat nach dem Entwurf eine Freiheitsstrafe von drei Monaten bis zu zehn Jahren zu befürchten. Diese Strafdrohung ist aus general- und spezialpräventiven Gründen geboten und mit Blick auf das verwirklichte Unrecht und die geschaffene abstrakte Gefährdung auch gerechtfertigt.

Zu Nummer 4 (§ 202d StGB-E)

Zu Buchstabe a (Absatz 1 StGB-E)

Der Entwurf streicht in § 202d Absatz 1 StGB - wie bei § 202c Absatz 1 StGB - das Wort „verbreitet“, da die Verbreitung nur eine Form des ebenfalls in Absatz 1 erwähnten Zugänglichmachens ist, bei der die Daten an einen größeren, nicht mehr überschaubaren Personenkreis weitergegeben werden (vgl. zur Definition der Tathandlung des Verbreitens etwa Eisele in: Schönke/Schröder, 30. Auflage 2018, § 202d Rn. 12). Diese Form der Zugänglichmachung an eine große Anzahl von Personen soll künftig aufgrund des gesteigerten Unrechtsgehalts in § 202d Absatz 2 Satz 2 Nummer 2 StGB-E als Regelbeispiel für einen besonders schweren Fall erfasst werden. Die Verbreitung an einen Personenkreis, der das Kriterium der großen Anzahl nicht erfüllt, bleibt als sonstige Form der Zugänglichmachung strafbar.

Zu Buchstabe b (Absätze 2 und 3 StGB-E)

Der Entwurf schafft mit den Absätzen 2 und 3 eine Strafzumessungsregel für besonders schwere Fälle und einen Qualifikationstatbestand, um auch Taten mit einem erhöhten Unrechtsgehalt in einer schuldangemessenen Weise bestrafen zu können. Ein praktisches Bedürfnis für erhöhte Strafdrohungen bei der Datenhehlerei besteht insbesondere mit Blick auf den lebhaften Handel mit „gestohlenen Daten“ im Darknet. So stellt der Handel mit Kreditkartendaten oder Accounts bei Zahlungsdienstleistern und Verkaufsplattformen auf den universellen Marktplätzen im Darknet, gleich nach dem Angebot von Betäubungsmitteln, derzeit eine der größten Kategorien dar (z.B. Kategorie „Fraud“ auf den Plattformen „Dream Market“ oder „Wallstreet Market“). Im Einzelnen:

1. Der Entwurf schafft mit dem neuen Absatz 2 des § 202d StGB-E die Möglichkeit, besonders schwere Fälle der Datenhehlerei mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen. Die besonders schweren Fälle werden dabei in den Nummern 1 bis 3 des § 202d Absatz 2 Satz 2 StGB-E mit drei Regelbeispielen konkretisiert, die weitgehend den Regelbeispielen aus § 202a Absatz 3 Satz 2 Nummern 1 bis 3 und § 202b Absatz 2 Satz 2 Nummern 1 bis 3 StGB-E entsprechen bzw. zumindest an diese angelehnt sind.

   So werden als erschwerende Umstände in Nummer 1 die Gewerbs- oder Bandenmäßigkeit genannt. Nummer 2 stuft die Datenhehlerei in der Regel als besonders schweren Fall ein, wenn sie in der Absicht begangen wird, durch die

fortgesetzte Tatbegehung sich oder einem anderen die Daten einer unübersehbaren Anzahl von Personen zu verschaffen oder die Daten einer großen Anzahl von Personen zugänglich zu machen. Über dieses Regelbeispiel sollen insbesondere auch solche Fälle erfasst werden, in denen der Täter an eine große Anzahl von Personen jeweils nur eine kleine Datenmenge verbreitet. Gerade auf den Marketplaces im Darknet ist es durchaus üblich, dass große Mengen von aktuellen und daher werthaltigen Zahlungsdaten in kleinere Tranchen geteilt und veräußert werden, da hierdurch ein weitaus höherer Gewinn zu erzielen ist. Nummer 3 stellt auf die Gefährdung kritischer Infrastrukturen oder der Sicherheit der Bundesrepublik Deutschland bzw. eines ihrer Länder ab.

2. Der vorgeschlagene Absatz 3 des § 202d StGB-E erhebt in Anlehnung an § 202a Absatz 4 StGB-E und § 260a Absatz 1 StGB die bandenmäßig begangene Datenhehlerei zum Verbrechen, sofern der Täter zugleich einen der erschwerenden Umstände aus § 202d Absatz 2 Satz 2 Nummer 1 erste Alternative oder Nummern 2 oder 3 StGB-E verwirklicht. Hierdurch soll vor allem dem organisierten Schwarzmarkthandel mit „gestohlenen“ Daten im Darknet Rechnung getragen werden.

Zu Buchstabe c (Absätze 4 und 5 StGB-E)

Es handelt sich lediglich um eine Folgeänderung aus der Einfügung der neuen Absätze 2 und 3, die dazu führt, dass die bisherigen Absätze 2 und 3 zu den Absätzen 4 und 5 werden.

Zu Nummer 5 (§ 205 StGB-E)

Zu Buchstabe a (Absatz 1 Satz 2 StGB-E)

Nach dem Entwurf soll im Ergebnis in dem Umfang an dem Strafantragserfordernis für das Ausspähen von Daten (§ 202a StGB), das Abfangen von Daten (§ 202b StGB) und die Datenhehlerei (§ 202d StGB) festgehalten werden, in dem es bislang nach § 205 Absatz 1 Satz 2 StGB gilt. Die Strafantragsregelung in § 205 Absatz 1 Satz 2 StGB ist daher dahingehend abzuändern, dass sie nur die Grundtatbestände der vorgenannten Delikte (§§ 202a Absatz 1, 202b Absatz 1, 202d Absatz 1 StGB-E) erfasst, nicht aber auch die Strafzumessungsregeln und die Qualifikationstatbestände (§§ 202a Absätze 3 und 4, 202b Absätze 2 und 3, 202d Absätze 2 und 3 StGB-E), die der Entwurf für die vorgenannten Delikte vorschlägt.

Eine Einbeziehung der Regelungen zu den besonders schweren und qualifizierten Fällen in das Strafantragserfordernis des § 205 Absatz 1 Satz 2 StGB erscheint mit Blick auf den erhöhten Unrechtsgehalt dieser Taten nicht sachgerecht, zumal die Strafverfolgungsbehörden in diesen Fällen aufgrund der Schwere der Taten ohnehin in aller Regel das besondere öffentliche Interesse an der Strafverfolgung zu bejahen hätten. Dementsprechend hat der Gesetzgeber im Übrigen auch bei den Diebstahlsdelikten in § 248a StGB davon abgesehen, die besonders schweren und qualifizierten Fallgestaltungen der §§ 243 ff. StGB dem Strafantragserfordernis zu unterstellen.

Zu Buchstabe b (Absatz 2 Satz 1 StGB-E)

In § 205 Absatz 2 Satz 1 StGB, der den Übergang des Antragsrechts im Falle des Todes des Verletzten auf die Angehörigen nach § 77 Absatz 2 StGB regelt, wird durch den Entwurf der einschränkende zweite Halbsatz, der diesen Übergang bei Taten nach §§ 202a, 202b und 202d StGB bislang ausschließt, gestrichen. Diese Rechtsverkürzung ist gerade angesichts der zunehmenden Werthaltigkeit vieler elektronischer Daten heute nicht mehr angemessen und zeitgemäß (so Graf in MüKo-StGB, 3. Auflage 2017, § 205 Rn. 13). Die Streichung erscheint ferner sachgerecht, weil beim Ausspähen und anschließenden Veröffentlichen von höchstpersönlichen Daten ein Bedürfnis besteht, es auch den Angehörigen zu ermöglichen, gemäß § 77 Absatz 2 StGB eine Strafverfolgung in die Wege leiten zu können.

Zu Nummer 6 (§ 303b StGB-E)

Zu Buchstabe a (Absatz 4 StGB-E)

Zu Buchstabe aa (Absatz 4 Satz 1 StGB-E)

Der Entwurf erweitert den Anwendungsbereich der Strafzumessungsregel für besonders schwere Fälle in § 303b Absatz 4 StGB, der bislang nach Satz 1 auf die Fälle des Absatzes 2 beschränkt ist, auf die Fälle des Absatzes 1. Dies hat zur Folge, dass eine Strafschärfung nicht mehr nur dann möglich ist, wenn die Computersabotage nach Absatz 2 einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde betrifft, sondern auch dann, wenn die Computersabotage nach Absatz 1 zum Nachteil einer Privatperson begangen wird.

Diese Erweiterung des Anwendungsbereichs der Strafzumessungsregel erscheint aus general- und spezialpräventiven Gründen zum Schutz von Privatpersonen geboten, da auch deren informationstechnische Systeme zunehmend von Sabotageakten

betroffen sind. Breites Aufsehen in der Öffentlichkeit erregten in den letzten Jahren insbesondere die Schadprogramme "Locky", "WannaCry" und „GrandCrab“, sowie andere Verschlüsselungs- bzw. Erpressungstrojaner, die massenhaft Computersysteme auch von Privatpersonen infizierten, den Zugriff auf die Systeme sperrten bzw. die darauf gespeicherten Daten verschlüsselten und die Freigabe von der Zahlung eines „Lösegeldes“ abhängig machten. Anders als im gewerblichen Umfeld sind im privaten Bereich ausreichende Backups häufig nicht vorhanden. Der Verlust der gesamten privaten „digitalen Vergangenheit“, bestehend aus unersetzbaren Dokumenten, Lichtbildern und sonstigen wichtigen Daten, führt dann zu einer Rechtsgutbeeinträchtigung für die Opfer.

Die Erweiterung des Anwendungsbereichs der Strafzumessungsregel ist aber nicht nur aus Gründen der General- und Spezialprävention geboten, sondern mit Blick auf das von § 303b StGB geschützte Rechtsgut auch sachgerecht und konsequent, da der Straftatbestand der Computersabotage ganz allgemein das Interesse der Betreiber und Nutzer von Datenverarbeitungen an deren ordnungsgemäßer Funktionsweise schützt. Mag die Computersabotage im betrieblichen, unternehmerischen oder behördlichen Bereich auch zu höheren Schäden führen können, so kann es doch nicht überzeugen, dass beispielsweise der Eintritt eines Vermögensverlusts großen Ausmaßes (§ 303b Absatz 4 Satz 2 Nummer 1 StGB) nur deshalb keine Auswirkung auf den in Betracht kommenden Strafrahmen haben soll, weil es eine Privatperson ist, die den Verlust erleidet. Der Verlust von 50.000 EUR oder mehr dürfte eine Privatperson typischerweise sogar noch empfindlicher treffen als ein großes Unternehmen.

Zu Buchstabe bb (Absatz 4 Satz 2 Nummer 1 StGB-E)

Der Entwurf ergänzt den in Nummer 1 des § 303b Absatz 4 Satz 2 StGB genannten erschwerenden Umstand der Herbeiführung eines Vermögensverlusts großen Ausmaßes um ein weiteres Regelbeispiel. Danach soll künftig in Anlehnung an § 263 Absatz 3 Satz 2 Nummer 2 StGB ein besonders schwerer Fall nicht mehr nur dann vorliegen, wenn der Täter einen Vermögensverlust großen Ausmaßes herbeiführt (erste Alternative), sondern auch dann, wenn der Täter in der Absicht handelt, durch die fortgesetzte Begehung von Computersabotage eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen (Alternative 2). Diese Ergänzung trägt dem Umstand Rechnung, dass das Handeln eines Täters, der durch mehrere rechtlich selbständige Sabotagehandlungen zwar eine große Zahl von Menschen schädigt oder schädigen will, wobei die Schäden jeweils aber kein großes Ausmaß erreichen, nicht unter die bisherige Regelung in § 303b Absatz 4 Satz 2 Nummer 1 StGB subsumiert werden kann. Denn eine Addition der Einzelschäden kommt weder bei mehreren Tatopfern noch bei mehreren rechtlich selbständigen Handlungen in Betracht. Bei der Auslegung der vom Entwurf vorgeschlagenen Neu-

regelung der Regelbeispiele in Nummer 1 kann auf die Auslegung der gleichlautenden Regelung in § 263 Absatz 3 Satz 2 Nummer 2 StGB zurückgegriffen werden.

Zu Buchstabe cc (Absatz 4 Satz 2 Nummer 2 StGB-E)

Der Entwurf trägt mit der Ersetzung des Wortes „Computersabotage“ in Nummer 2 des § 303b Absatz 4 Satz 2 StGB durch die allgemeine Formulierung „Taten nach §§ 202a bis 202d, 263a, 269 oder 303b“ dem Umstand Rechnung, dass sich Banden im Bereich der Cyberkriminalität in aller Regel nicht ausschließlich zur Begehung von Delikten der Computersabotage, sondern allgemein zur Begehung von Delikten nach §§ 202a bis 202d, 263a, 269 oder 303b StGB zusammenschließen.

Zu Buchstabe dd (Absatz 4 Satz 2 Nummer 3 StGB-E)

Die Nummer 3 des § 303b Absatz 4 Satz 2 StGB wird durch die Neufassung im Entwurf in zweierlei Hinsicht geändert:

Zum einen ersetzt der Entwurf die bisherige Fassung der ersten Alternative der Nummer 3, die eine Beeinträchtigung der Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen verlangt, durch die etwas allgemeiner gefasste Formulierung, dass durch die Tat die Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität oder Vertraulichkeit kritischer Infrastrukturen gefährdet sein muss. Damit soll einem zu engen Verständnis, das sich etwa aus dem Begriff „lebenswichtig“ ergeben könnte, vorgebeugt und gewährleistet werden, dass alle kritischen Infrastrukturen den gleichen strafrechtlichen Schutz erhalten. Zugleich wird damit eine begriffliche Anpassung an die entsprechenden Regelbeispiele bei den anderen Straftatbeständen aus §§ 202a, 202b und 202d StGB-E erreicht (vgl. § 202a Absatz 4 Satz 2 Nummer 3, § 202b Absatz 3 Satz 2 Nummer 3, § 202d Absatz 3 Satz 2 Nummer 3 StGB-E).

Zum anderen passt der Entwurf auch die Alternative 2 der Nummer 3 an die entsprechenden Regelungen bei den vorgenannten Straftatbeständen an. Hierfür wird die bereits jetzt im Gesetz erwähnte Sicherheit der Bundesrepublik Deutschland um die Sicherheit eines der Länder ergänzt.

Ferner erweitert der Entwurf den Anwendungsbereich der Alternative 2 auch insofern, als er keine Beeinträchtigung der Sicherheit mehr verlangt, sondern - ebenso wie für Alternative 1 - eine konkrete Gefährdung ausreichen lässt. Diese Erweiterung ist mit Blick auf das Ausmaß der potentiell drohenden Schäden sachge-

recht, zumal es oftmals nur vom Zufall abhängen wird, ob sich die geschaffene Gefahr auch in konkreten Beeinträchtigungen realisiert. Vor diesem Hintergrund stellt es auch keine unverhältnismäßige Sanktion dar, wenn derjenige, der eine Computersabotage begeht und dabei billigend in Kauf nimmt, beispielsweise die Funktionsfähigkeit der Flugsicherheit oder die Verteidigungsfähigkeit und damit die äußere Sicherheit der Bundesrepublik Deutschland zu gefährden, eine Freiheitsstrafe von mindestens sechs Monaten bis maximal zehn Jahren zu befürchten hat. Eine solche Strafdrohung scheint vielmehr aufgrund des hohen Gefahrenpotentials aus generalpräventiven Gründen geboten, um potentielle Täter von vornherein von der Begehung entsprechender Taten abzuschrecken.

Zu Buchstabe b (Absätze 5 und 6 StGB-E)

Der Entwurf schlägt des Weiteren vor, in § 303b StGB zwei neue Absätze 5 und 6 mit einem qualifizierten und einem erfolgsqualifizierten Tatbestand für Fallgestaltungen einzufügen, die sich aufgrund ihres erhöhten Unrechtsgehalts mit den bestehenden Strafrahmen der Absätze 1, 2 oder 4 nicht in einer schuldangemessenen Weise erfassen und bestrafen lassen.

1. Der in Absatz 5 des § 303b StGB-E vorgeschlagene Qualifikationstatbestand erhebt in Anlehnung an § 202a Absatz 4 StGB-E die bandenmäßig begangene Computersabotage unter erschwerten Umständen zum Verbrechenstatbestand. Wer also als Mitglied einer Bande handelt und dabei zugleich kumulativ einen der in § 303b Absatz 4 Satz 2 Nummer 1, Nummer 2 erste Alternative oder Nummer 3 genannten, erschwerenden Umstände verwirklicht, hat nach dem Entwurf eine Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen eine Freiheitstrafe von sechs Monaten bis zu fünf Jahren zu erwarten. Der Qualifikationstatbestand erfasst insbesondere durch die kumulative Verbindung der gewerbs- und bandenmäßigen Begehungsweise wesentliche Bereiche der Organisierten und damit schweren Cyberkriminalität, so dass die Ausgestaltung als Verbrechenstatbestand sachgerecht ist. Dies gilt umso mehr, als alle Bereiche des modernen Lebens aufgrund der fortschreitenden Digitalisierung in einem zunehmenden Maße von einem störungsfreien Funktionieren ihrer Datenverarbeitungsanlagen abhängig sind und mit Akten der Computersabotage gerade im Bereich der Wirtschaft immense wirtschaftliche Schäden verbunden sein können, die etwa im Falle von Produktionsausfällen bis zum wirtschaftlichen Ruin eines Unternehmens und dem Verlust von Arbeitsplätzen reichen können.

2. Der Entwurf schlägt zudem vor, in einem neuen Absatz 6 eine als Verbrechenstatbestand ausgestaltete Erfolgsqualifikation für den Fall zu schaffen, dass der Täter durch die Computersabotage wenigstens leichtfertig den Tod (Satz 1) oder eine schwere Gesundheitsschädigung (Satz 2) eines anderen Menschen verursacht. Hierdurch sollen insbesondere Fallgestaltungen angemessen erfasst werden, in denen der Täter durch die Computersabotage vorsätzlich eine erhebliche Störung der informationstechnischen Systeme von Krankenhäusern, Flughäfen oder anderen kritischen Infrastrukturen herbeiführt und dadurch wenigstens leichtfertig den Tod oder eine schwere Gesundheitsschädigung eines Menschen verursacht (etwa weil lebenserhaltende Geräte in einem Krankenhaus oder die Steuerungselektronik von Ampelanlagen oder Herzschrittmachern ausfallen oder weil die Flugsicherungssysteme eines Fluglotsen derart gestört werden, dass es zu einem Absturz oder Zusammenstoß zweier Flugzeuge kommt). Angesichts der schweren Tatfolgen ist - in Anlehnung an die Strafrahmen der §§ 226 Absatz 1, 227 Absatz 1 StGB - beim Verlust eines Menschenlebens eine im Mindestmaß erhöhte Strafdrohung von nicht unter drei Jahren und bei einer schweren Gesundheitsschädigung eine Strafdrohung von einem bis zu zehn Jahren sachgerecht, um eine schuldangemessene Bestrafung zu gewährleisten und general- wie spezialpräventiven Strafbedürfnissen gerecht zu werden. Sofern im konkreten Einzelfall strafmildernde Umstände beträchtlich überwiegen sollten, ist durch die gleichzeitige Regelung von minder schweren Fällen mit niedrigeren Strafrahmen von einem bis zehn Jahren (im Fall der Verursachung des Todes eines Menschen) und von sechs Monaten bis zu fünf Jahren (im Fall der Verursachung einer schweren Gesundheitsschädigung) sichergestellt, dass die Gerichte auch in solchen Fällen schuldangemessen reagieren können.

Zu Buchstabe c (Absatz 7 StGB-E)

Der bisherige Absatz 5, der für die Vorbereitung einer Computersabotage die entsprechende Anwendung des § 202c StGB anordnet, wird Absatz 7. Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 2 (Änderung der Strafprozessordnung)

§ 100a Absatz 2 Nummer 1 StPO-E

Zu Buchstabe a (Buchstabe h StPO-E)

Der Entwurf erweitert den Anwendungsbereich der Telekommunikationsüberwachung, indem er den Straftatenkatalog des § 100a Absatz 2 StPO um die schweren Computer- und Datendelikte nach §§ 202a Absatz 3 und 4, 202b Absatz 2 und 3, 202c Absatz 3 und 4, 202d Absatz 2 und 3 und § 303b Absatz 4 bis 6 StGB-E ergänzt. Diese Delikte werden entsprechend der bisherigen Gesetzessystematik, welche die Katalogtaten nach ihrer Paragraphenzahl in aufsteigender Reihenfolge anordnet, in den Katalog als neuer Buchstabe h aufgenommen.

Die Aufnahme dieser Delikte in den Anlasstatenkatalog des § 100a Absatz 2 StPO ist zur effektiven Verfolgung der schweren Cyberkriminalität kriminalpolitisch notwendig und unter Berücksichtigung der bundesverfassungsgerichtlichen Vorgaben auch zulässig.

Notwendig ist die Aufnahme, da ohne die Eröffnung der Telekommunikationsüberwachung Straftaten aus dem Bereich der Cyberkriminalität kaum erfolgreich aufgeklärt werden können. Diese Taten werden der Natur der Sache nach in den allermeisten Fällen auch oder ausschließlich unter Zuhilfenahme von Telekommunikationsdiensten begangen, so dass die Überwachung der Telekommunikation zum Beispiel in Form der Server- oder DSL-Überwachung oftmals den einzigen Ermittlungsansatz zur Identifizierung der Täter und zur Aufklärung des Sachverhalts darstellen. Der Entwurf trägt damit den Bedürfnissen der Strafverfolgungspraxis Rechnung, die seit längerem eine entsprechende Erweiterung des Anwendungsbereichs der Telekommunikationsüberwachung fordert.

Die Aufnahme der genannten Computer- und Datendelikte in den Katalog des § 100a Absatz 2 StPO ist verfassungsrechtlich auch zulässig. Das Bundesverfassungsgericht gewährt dem Gesetzgeber ausdrücklich einen Beurteilungsspielraum bei der Bestimmung des Unrechtsgehalts eines Delikts und bei der Entscheidung darüber, welche Straftaten er zum Anlass für bestimmte strafprozessuale Ermittlungsmaßnahmen machen will (BVerfG NJW 2012, 833 [836]). Erforderlich für die Aufnahme in den Katalog von Anlasstaten ist aufgrund des Eingriffs in das Fernmeldegeheimnis aus Artikel 10 GG zur Wahrung der Verhältnismäßigkeit allerdings, dass es sich um eine schwere Straftat handelt. Für die Qualifizierung einer Straftat als schwer können insbesondere der Strafrahmen, aber auch das geschützte Rechtsgut und dessen Bedeutung für die Rechtsgemeinschaft von Bedeutung sein (BVerfG NJW 2012, 833 [836]).

Gemessen daran ist die Aufnahme der Computer- und Datendelikte nach §§ 202a Absatz 3 und 4, 202b Absatz 2 und 3, 202c Absatz 3 und 4, 202d Absatz 2 und 3, 303b Absatz 4 bis 6 StGB-E in den Katalog der schweren Straftaten aus § 100a Absatz 2 StPO nicht zu beanstanden.

Die besonders schweren bzw. qualifizierten Fälle des Ausspähens von Daten nach § 202a Absatz 4 StGB-E, des Abfangens von Daten nach § 202b Absatz 3 StGB-E, des Vorbereitens von bestimmten Delikten nach § 202c Absatz 4 StGB-E, der Datenhehlerei nach § 202d Absatz 3 StGB-E und der Computersabotage nach § 303b Absatz 4 bis 6 StGB-E sind bereits nach ihrem Strafrahmen - alle sehen eine höhere Höchststrafe als fünf Jahre vor - unzweifelhaft als schwere Straftaten anzusehen.

Die besonders schweren Fälle des Ausspähens von Daten nach § 202a Absatz 3 StGB-E, des Abfangens von Daten nach § 202b Absatz 2 StGB-E, des Vorbereitens bestimmter Datendelikte nach § 202c Absatz 3 StGB-E und der Datenhehlerei nach § 202d Absatz 2 StGB-E sind zwar nur mit einer Höchststrafe von fünf Jahren Freiheitsstrafe bedroht. Die Delikte sind indes bei einer Gesamtschau, welche die geschützten Rechtsgüter und deren Bedeutung für die Rechtsgemeinschaft in den Blick nimmt, ebenfalls als „schwer“ einzustufen. Die §§ 202a bis 202d StGB schützen das formelle Datengeheimnis (vgl. Graf in: MüKo-StGB, 3. Aufl. 2017, § 202a Rn. 2, § 202b Rn. 2, § 202c Rn. 2, § 202d Rn. 3). Diesem Rechtsgut kommt in der modernen Informationsgesellschaft, in der informationstechnische Systeme allgegenwärtig und die Menschen auf die Nutzung dieser Systeme zunehmend angewiesen sind, eine hohe Bedeutung zu. Das Bundesverfassungsgericht hat daraus sogar ein grundrechtlich erhebliches Schutzbedürfnis gefolgert und aus dem allgemeinen Persönlichkeitsrecht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme abgeleitet (BVerfG NJW 2008, 822 [825]). Vor diesem Hintergrund besteht ein hohes öffentliches Aufklärungsinteresse in Bezug auf solche Delikte, die sich gegen die vorgenannten Rechtsgüter richten. Dies gilt umso mehr, als die Cyberkriminalität inzwischen ein Ausmaß erreicht hat, das die Privatsphäre und das Sicherheitsgefühl der Bevölkerung massiv bedroht, die Grundlagen von Staat, Wirtschaft und Gesellschaft gefährdet und zudem geeignet ist, das Vertrauen in den Rechtsstaat und die Handlungsfähigkeit staatlicher Organe nachhaltig zu erschüttern. Die Zuordnung der vorgenannten Delikte zu den schweren Straftaten ist daher vom Beurteilungsspielraum des Gesetzgebers umfasst.

Zu Buchstabe b (Buchstabe i bis v StPO-E)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 3 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.