Bundesrat **Drucksache** **33/19**

18.01.19

Gesetzesantrag
des Landes Nordrhein-Westfalen

Entwurf eines Strafrechtsänderungsgesetzes - Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen

A. Problem und Ziel

Vermehrt nutzen Straftäter die Möglichkeiten der Anonymisierung, die ihnen das Internet bietet. Eine häufig genutzte Form der Anonymisierung erfolgt über das »The Onion Router« (Tor)-Netzwerk, das aus einer Vielzahl von weltweit verteilten Servern besteht, über die Datenpakete in ständig wechselnder Form geleitet werden. Beim Verbindungsaufbau wird durch das Programm eine zufällige Route über einen Teil der Server festgelegt, ohne dass Herkunft oder Ziel der Daten protokolliert werden. Durch die Verschlüsselung der Nutzerdaten und die dynamische Routenwahl wird die Feststellung von Anfangs- und Endpunkten eines Datentransfers erheblich erschwert. Insbesondere über das Tor-Netzwerk erfolgt der Zugang zum sogenannten Darknet. Zugang und Erreichbarkeit der Darknet-Angebote sind durch das Erfordernis besonderer Programme, wie des Tor-Browsers, beschränkt.

Die Angebote im Darknet umfassen, wie auch auf andere Weise zugangsbeschränkte Dienste, neben Foren für Whistleblower oder Chatrooms für politisch Verfolgte in autoritär geführten Staaten auch Inhalte bekannter Servicebetreiber, etwa Facebook. Ebenso finden sich jedoch Angebote mit strafrechtlicher Relevanz, darunter Handel mit Betäubungsmitteln, Kinderpornographie oder Waffen, mit Schadsoftware und Ausweispapieren. Vergleichbare Angebote finden sich auch in weiteren Teilen des Internets. In technischer Hinsicht entsprechen die angebotenen Dienste denen bekannter Online-Handelsplattformen mit Vorschaubildern der angebotenen Waren, Werbung, Bewertungen für Verkäufer und Hinweisen auf weitere möglicherweise für einen Nutzer interessanten Angeboten (vgl. *Tzanetakis*, Drogenhandel im Darknet, in Aus Politik und Zeitgeschichte 2017, 46-47/2017, S. 41 ff.).

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

Das Kriminalitätsphänomen gewinnt in der Praxis der Strafverfolgung zunehmend an Gewicht und beschränkt sich dabei nicht auf wenige Einzelfälle. Aufgrund des ständigen Auftretens neuer Angebote und der auf Verschleierung angelegten Vorgehensweise liegen keine genauen Daten über die Anzahl einschlägiger Foren vor. Die Zentralstellen der Staatsanwaltschaften für die Verfolgung von Cybercrime der Länder haben in den vergangenen Jahren jedoch bereits zahlreiche Ermittlungsverfahren gegen die Verantwortlichen einschlägiger Foren oder Plattformen und deren Nutzer geführt, z. B. „Deutschland im Deep Web“ oder „crimenetwork.biz“. Im internationalen Bereich wurden Verfahren gegen die Verantwortlichen von „Silkroad“, „AlphaBay“ und „Hansa Market“ geführt. Nach Einschätzung des Bundeskriminalamtes wurden im Jahr 2016 circa 50 einschlägige Plattformen unterhalten (BT-Drucks. 18/9487, S. 2). Das dort betriebene Geschäftsmodell des „*Cybercrime-as-a-Service*“ wird in der kriminellen Szene weiter ausgebaut (Lagebild Cybercrime des Bundeskriminalamtes 2016, abrufbar unter www.bka.de, dort S. 16 ff.). Illegale Onlinehandelsplattformen stellen aus Sicht von EUROPOL eine der zentralen Schnittstellen von Cybercrime und weiteren Formen - auch organisierter - Kriminalität dar (Internet Organised Crime Threat Assessment 2017, abrufbar unter www.europol.eu).

Die Erfahrungen aus den geführten Ermittlungsverfahren lassen ein arbeitsteiliges Zusammenwirken von Plattformbetreibern und Nutzern der Plattform, also sowohl Händlern als auch Käufern, erkennen. Es zeigt sich zudem, dass die klassischen Organisationsdelikte und die historischen gesetzgeberischen Vorstellungen von Täterschaft und Teilnahme auf moderne, internetbasierte Täterstrukturen kaum übertragbar sind. Die Betreiber selbst stellen lediglich eine - in einigen Fällen vollautomatisierte - technische Infrastruktur zur Verfügung. Aufgrund dieser Umstände ist eine Beihilfehandlung zu einer konkreten Haupttat in der Praxis nur schwer erweislich. Auch die Zurechnung von Einzeltaten unter dem Gesichtspunkt einer bandenmäßigen Tatbegehung ist häufig nicht möglich, da in der Regel kriminelle Foren und Marktplätze der Underground Economy in amorphen Organisationsstrukturen jenseits des überkommenen Bandenbegriffs geführt werden.

Weil der Zugang zu den einschlägigen Angeboten in der Regel keinen besonderen technischen Anforderungen unterliegt und die Erreichbarkeit zwar beschränkt, aber ohne erheblichen technischen Aufwand möglich ist, bieten die Handelsplattformen somit einen niedrigschwelligen Zugriff auf logistische Infrastrukturen für die Begehung von Straftaten auch für Personen, die herkömmliche Beschaffungswege für Waffen, Betäubungsmittel oder kriminelle Dienstleistungen nicht beschreiten. Diese

Angebote stellen eine erhebliche Gefahr für die öffentliche Sicherheit dar, ohne dass die geltende Rechtslage ausreichende Möglichkeiten für eine angemessene strafrechtliche Verfolgung bietet.

Vor diesem Hintergrund haben sich die Justizministerinnen und Justizminister der Länder bereits anlässlich ihrer Herbstkonferenz am 17. November 2016 in Berlin mit der Effektivität strafrechtlicher Ermittlungen im Darknet befasst. Die Justizministerinnen und Justizminister halten für erforderlich, das öffentliche Feilbieten von Gegenständen und Dienstleistungen zur Vorbereitung von Straftaten im Internet zu unterbinden. Sie haben daher die Bundesregierung um Prüfung gebeten, inwieweit dies durch Anpassungen des materiellen Strafrechts, namentlich des Waffengesetzes, besser als bisher erreicht werden kann.

B. Lösung

Der Entwurf führt einen neuen Straftatbestand des Anbietens von Leistungen zur Ermöglichung von Straftaten ein. Der Tatbestand erfasst ausschließlich internetbasierte Angebote in hinsichtlich Zugang und Erreichbarkeit beschränkten Netzwerken und setzt die Ausrichtung der Leistung auf die Ermöglichung von Delikten, deren Begehung besondere Gefahren für die öffentliche Sicherheit begründen, voraus. Ergänzt wird der Grundtatbestand durch eine Qualifikation im Falle gewerbsmäßiger Begehung. Lediglich diese Qualifikation soll Anknüpfungstat für die cyberspezifische, eingriffsintensive Ermittlungsmaßnahme der Überwachung der Telekommunikationsüberwachung sein.

C. Alternativen

Beibehaltung des bisherigen, unbefriedigenden Zustands, der nicht sämtliche strafwürdigen Verhaltensweisen in angemessener Weise erfasst.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht oder entfällt kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht oder entfällt kein Erfüllungsaufwand.

Davon Bürokratiekosten aus Informationspflichten:

Für Unternehmen werden keine Informationspflichten eingeführt, vereinfacht oder abgeschafft.

E.3 Erfüllungsaufwand der Verwaltung

Aufgrund der Ausweitung der Strafbarkeit ist zu erwarten, dass die Anzahl der Ermittlungs- und Strafverfahren in einem begrenzten Ausmaß zunimmt. Dies kann zu nicht näher quantifizierbaren Haushaltsmehrausgaben bei den für die Durchführung von Ermittlungs- und Strafverfahren primär zuständigen Strafverfolgungsbehörden der Länder führen.

F. Weitere Kosten

Den Bürgerinnen und Bürgern sowie der Wirtschaft entstehen keine sonstigen Kosten. Auswirkungen auf das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

Bundesrat **Drucksache** **33/19**

18.01.19

Gesetzesantrag
des Landes Nordrhein-Westfalen

Entwurf eines Strafrechtsänderungsgesetzes - Einführung einer eigenständigen Strafbarkeit für das Betreiben von internet-basierten Handelsplattformen für illegale Waren und Dienstleistungen

Der Ministerpräsident
des Landes Nordrhein-Westfalen

Düsseldorf, 16. Januar 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 – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen**

zuzuleiten.

Ich bitte, die Vorlage gemäß § 36 Absatz 2 der Geschäftsordnung des Bundesrates in die Tagesordnung der Sitzung des Bundesrates am 15. Februar 2019 aufzunehmen und anschließend den zuständigen Ausschüssen zur Beratung zuzuweisen.

Mit freundlichen Grüßen
Armin Laschet

Entwurf eines Strafrechtsänderungsgesetzes – Einführung einer eigenständigen Strafbarkeit für das Betreiben von internetbasierten Handelsplattformen für illegale Waren und Dienstleistungen

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), das zuletzt durch Artikel … des Gesetzes vom (BGBl. I S. …) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 126 folgende Angabe eingefügt:

   „§ 126a Anbieten von Leistungen zur Ermöglichung von Straftaten“.

2. Nach § 126 wird folgender § 126a eingefügt:

„§ 126a
Anbieten von Leistungen zur Ermöglichung von Straftaten

(1) Wer eine internetbasierte Leistung anbietet, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt und deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten im Sinne von Satz 2 zu ermöglichen oder zu fördern, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Rechtswidrige Taten im Sinne des Satzes 1 sind

1. § 95 Absatz 1 des Gesetzes über den Verkehr mit Arzneimitteln,
2. §§ 29 Absatz 1 Nr. 1, 29a, 30, 30a des Betäubungsmittelgesetzes,
3. § 19 Absatz 1 des Grundstoffüberwachungsgesetzes,
4. § 52 Absatz 1 Nr. 1 und Abs. 3 Nr. 1 des Waffengesetzes,
5. § 40 Absatz 1 und 2 des Sprengstoffgesetzes,
6. §§ 19 Absatz 1, 20 Abs. 1, 20a Absatz 1, 22a Absatz 1 Nr. 1, 2 und 4 des Gesetzes über die Kontrolle von Kriegswaffen sowie
7. §§ 146, 147, 149, 152a, 152b, 184b Abs.1, 202a, 202b, 202c, 263a, 275, 276, 303a und 303b des Strafgesetzbuches.

(2) Die Strafe darf nicht schwerer sein, als die für die Tat im Sinne von Absatz 1 Satz 2 angedrohte Strafe.

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat gewerbsmäßig begeht.“

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 Buchstabe d wird wie folgt gefasst:

„d) Straftaten gegen die öffentliche Ordnung nach den §§ 126a Absatz 3, 129 bis 130,“.

Artikel 3
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeines

I. Zielsetzung und wesentlicher Inhalt des Gesetzentwurfs

Vermehrt nutzen Straftäter die Möglichkeiten der Anonymisierung, die ihnen das Internet bietet. Eine häufig genutzte Form der Anonymisierung erfolgt über das »The Onion Router« (Tor)-Netzwerk, das aus einer Vielzahl von weltweit verteilten Servern besteht, über die Datenpakete in ständig wechselnder Form geleitet werden. Beim Verbindungsaufbau wird durch das Programm eine zufällige Route über einen Teil der Server festgelegt, ohne dass Herkunft oder Ziel der Daten protokolliert werden. Durch die Verschlüsselung der Nutzerdaten und die dynamische Routenwahl wird die Feststellung von Anfangs- und Endpunkten eines Datentransfers erheblich erschwert. Über das Tor-Netzwerk erfolgt der Zugang zum sogenannten Darknet. Zugang und Erreichbarkeit der Darknet-Angebote sind durch das Erfordernis besonderer Programme, wie des Tor-Browsers, beschränkt.

Die Angebote im Darknet umfassen, wie auch auf andere Weise zugangsbeschränkte Dienste, neben Foren für Whistleblower oder Chatrooms für politisch Verfolgte in autoritär geführten Staaten auch Inhalte bekannter Servicebetreiber. Ebenso finden sich jedoch Angebote mit strafrechtlicher Relevanz, darunter Handel mit Betäubungsmitteln, Kinderpornographie oder Waffen, mit Schadsoftware und Ausweispapieren. Vergleichbare Angebote finden sich auch in weiteren Bereichen des Internets.

Die Zentralstellen für die Verfolgung von Cybercrime der Länder haben in den vergangenen Jahren zahlreiche Ermittlungsverfahren mit überwiegend internationalen Bezügen geführt und einschlägige Foren sowie Handelsplattformen schließen können. In der Praxis zeigt sich jedoch, dass Anbieter und Kunden ihre Aktivitäten mit allenfalls geringem zeitlichem Verzug über alternative Plattformen fortführen. Die Verfahren lassen im Übrigen durchweg ein arbeitsteiliges Zusammenwirken von Plattformbetreibern und Nutzern der Plattform, also sowohl Händlern als auch Käufern, erkennen. Die Erfahrungen zeigen zudem, dass die klassischen Organisationsdelikte und die historischen gesetzgeberischen Vorstellungen von Täterschaft und Teilnahme auf moderne, internetbasierte Täterstrukturen kaum übertragbar sind. Die Betreiber selbst stellen lediglich eine technische Infrastruktur zur Verfügung. Ihr Verdienst entsteht durch Werbung oder einen Treuhand-Service im Rahmen der Zahlungsabwicklung.

Das Kriminalitätsphänomen beschränkt sich auch nicht auf wenige Einzelfälle. Bereits im Jahr 2016 waren dem Bundeskriminalamt circa 50 einschlägige Plattformen bekannt (BT-Drucks. 18/9487, S. 2). Das dort betriebene Geschäftsmodell des „*Cybercrime-as-a-Service*“ wird in der kriminellen Szene weiter ausgebaut (Lagebild Cybercrime des Bundeskriminalamtes 2016, abrufbar unter www.bka.de, dort S. 16 ff.).

Illegale Onlinehandelsplattformen stellen aus Sicht von EUROPOL eine der zentralen Schnittstellen von Cybercrime und weiteren Formen - auch organisierter - Kriminalität dar (Internet Organised Crime Threat Assessment 2017, abrufbar unter www.europol.eu). Gegenüber den bereits etablierten Handelsgütern, wie z. B. Betäubungsmitteln, sei eine deutliche Zunahme bei Angeboten von Hackertools und -dienstleistungen zu verzeichnen. Diese Aspekte hat auch die Europäische Kommission in der gemeinsamen Mitteilung mit der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik an das Europäische Parlament und den Rat „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“ vom 13.09.2017 betont und auf das derzeit nur geringe Risiko der Tatentdeckung hingewiesen [JOIN(2017) 450, dort S. 18].

In der strafrechtlichen Praxis stellt sich das Problem, dass eine Beihilfe gemäß § 27 StGB zu den über die Plattform begangenen Straftaten oft nicht nachweisbar ist, da die Haupttaten bilateral zwischen den Beteiligten über verschlüsselte Kommunikationskanäle abgewickelt werden, jedenfalls aber nicht offen im Forum sichtbar sind. Zudem sind bei vielen Foren die Arten von Straftaten, die über sie abgewickelt werden sollen, zu Beginn nicht klar definiert. Die Täter stellen eine informationstechnische Struktur zur Verfügung und wissen um die strafrechtliche Relevanz der über den Dienst abgewickelten Geschäfte. Welche Art von Gütern konkret gehandelt wird, spielt für die Täter dabei keine Rolle. Moderne Foren verfügen zudem häufig über vollautomatisierte Verkaufssysteme, bei denen eine Beihilfe zu einer konkreten Haupttat noch schwieriger nachzuweisen ist. Ungeachtet dessen erfasst die strafrechtliche Ahndung unter dem Gesichtspunkt der Beihilfe in der Regel nicht hinreichend den aktiven Charakter der Tathandlung, die die Grundlagen der Underground-Economy schafft.

Auch eine Zurechnung von Einzeltaten unter dem Gesichtspunkt einer bandenmäßigen Tatbegehung ist häufig nicht möglich, da in der Regel kriminelle Foren und Marktplätze der Underground Economy von nur einer Person oder zwei Personen geführt werden. Bei Foren und Marktplätzen mit mehreren Personen in der Führungsebene ist überdies zu berücksichtigen, dass sich die Betreiber regelmäßig nicht persönlich kennen und oftmals kein übergeordnetes, homogenes Interesse vorliegt. Ist im Einzelfall eine Bande im strafrechtlichen Sinne anzunehmen, ist im Weiteren für jede einzelne Tat nach den allgemeinen Kriterien festzustellen, ob sich die anderen Bandenmitglieder hieran als Mittäter, Anstifter oder Gehilfen beteiligt oder ob sie gegebenenfalls überhaupt keinen strafbaren Tatbeitrag geleistet haben. Letzteres kann insbesondere dann in Betracht kommen, wenn einzelne Betreiber nur für die Aufrechterhaltung und Wartung der technischen Infrastruktur oder die Administration nicht strafrechtlich relevanter Bereiche zuständig sind und glaubhaft versichern, keine Kenntnis von oder jedenfalls kein Interesse an den über das Forum abgeschlossenen oder angebahnten illegalen Verkaufstätigkeiten gehabt zu haben. In derartigen Konstellationen kommt auch die Annahme eines uneigentlichen Organisationsdelikts

durch den Aufbau und die Aufrechterhaltung eines auf Straftaten ausgerichteten Geschäftsbetriebs regelmäßig nicht in Betracht.

Eine effektive Strafverfolgung kommt schließlich auch unter dem Gesichtspunkt der Bildung einer kriminellen Vereinigung im Sinne des § 129 StGB nicht stets in Betracht. Die Anforderungen an den Nachweis konkreter Einzeltaten sind bei dem abstrakten Gefährdungsdelikt zwar erleichtert, in der Regel wird jedoch die für den Tatbestand erforderliche Festigkeit der Struktur nicht erreicht. Dies gilt ungeachtet der durch das 54. Gesetz zur Änderung des Strafgesetzbuches – Umsetzung des Rahmenbeschlusses 2008/841/JI des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität vom 17. Juli 2017 (BGBl. I S. 2440) erfolgten Ausweitung des Vereinigungsbegriffs im Sinne des § 129 Absatz 2 StGB, denn Voraussetzung einer Vereinigung ist weiterhin ein organisierter Zusammenschluss. Dies erfordert zumindest eine gewisse Organisationsstruktur sowie eine instrumentelle Vorausplanung und Koordinierung. Zusammenschlüsse, die sich zufällig zur unmittelbaren Begehung einer Straftat bilden, wie dies bei den hier relevanten Cyberstrukturen oft der Fall ist, dürften dem Vereinigungsbegriff des § 129 Absatz 2 StGB nicht unterfallen.

Weil der Zugang zu den einschlägigen Angeboten in der Regel keinen besonderen technischen Anforderungen unterliegt und die Erreichbarkeit zwar beschränkt, aber ohne erheblichen technischen Aufwand möglich ist, bieten die Handelsplattformen somit einen niedrigschwelligen Zugriff auf logistische Infrastrukturen für die Begehung von Straftaten auch für Personen, die herkömmliche Beschaffungswege für Waffen, Betäubungsmittel oder kriminelle Dienstleistungen nicht beschreiten. Diese Angebote erhöhen durch die Verbreitung des illegalen Angebots gezielt die Gefahren für die durch das Verbot der Waren und Dienstleistungen geschützten Rechtsgüter und stellen damit eine darüber hinausgehende eigenständige erhebliche Gefahr für die öffentliche Sicherheit dar, ohne dass es nach der geltenden Rechtslage ausreichende Möglichkeiten für eine angemessene strafrechtliche Verfolgung gibt.

Diese Lücke soll durch die Einführung der neuen Vorschrift geschlossen werden. Der Entwurf zielt darauf, das Betreiben von auf die Förderung illegaler Zwecke ausgerichteten Plattformen unabhängig von dem Nachweis der Beteiligung an einzelnen konkreten Handelsgeschäften unter Strafe zu stellen. Die Vorschrift soll die öffentliche Sicherheit und die staatliche Ordnung schützen, daher erfolgt die Aufnahme in den sechsten Abschnitt. Die Aufnahme eines Tatbestands in das Strafgesetzbuch fördert eine einheitliche Rechtsanwendung und erscheint daher gegenüber spezialgesetzlichen Einzelregelungen vorzugswürdig. Soweit vereinzelt bereits Strafvorschriften das Verschaffen einer Gelegenheit zur Begehung von Straftaten erfassen, z. B. § 29 Absatz 1 Nr. 10 BtMG, regelt § 126a StGB-E den Sonderfall der Tatbegehung mittels internetbasierter Leistungen. Dem Konkurrenzverhältnis wird insoweit durch eine Subsidiaritätsklausel in § 126a Absatz 1 S. 1 StGB-E Rechnung getragen.

Im Sinne einer aus Gründen der Verhältnismäßigkeit angezeigten Beschränkung erfasst § 126a StGB-E nur bestimmte, als für das geschützte Rechtsgut besonders gefährlich einzustufende szenetypische Delikte im Sinne des § 126a Absatz 1 S. 2 StGB-E. Die dort genannten Delikte bergen aufgrund der Gefährlichkeit der gehandelten Waren und Dienstleistungen bereits für sich eine besondere Gefahr für die öffentliche Sicherheit. Diese Gefahr wird durch die Begehung mittels internetbasierter Leistungen erheblich erhöht, da die Angebote ohne Beschränkung zugänglich sind. Der potentielle Adressatenkreis ist damit praktisch unbegrenzt. Die Täter des § 126a StGB-E eröffnen durch die Handelsplattformen einen örtlich, zeitlich und sachlich unbegrenzten Zugang zu illegalen Waren und Dienstleistungen, der in der analogen Welt auch nicht annähernd vergleichbar besteht oder möglich wäre und Grundlage weiterer digitaler oder analoger Handelsketten sein kann.

Die Vorschrift beschränkt sich auf einen bestimmten Ausschnitt des kriminellen Online-Handels. Erfasst werden nur durch technische Vorkehrungen hinsichtlich Zugang und Erreichbarkeit beschränkte Angebote. Zugangs- und Erreichbarkeitsbeschränkungen können sich etwa durch die beschriebene Nutzung des Tor-Browsers im Darknet oder bei ähnlichen Zugangsbeschränkungen, z. B. durch vor Zulassung erforderliche Keuschheitsproben, ergeben. Zur Abgrenzung der durch den Tatbestand erfassten Angebote von legalen Handelsplattformen, die ohne den Willen der Betreiber für strafrechtlich relevante Zwecke genutzt werden, wird – in Anlehnung an die Formulierung des § 129 StGB – überdies auf den Zweck und die Ausrichtung der Tätigkeit abgestellt. Damit sind Betreiber, deren Angebote ohne entsprechende Zielrichtung zur Förderung von Straftaten genutzt werden, vom Tatbestand ausgenommen. Dies gewährleistet eine Beschränkung schon des Tatbestands auf strafwürdige Online-Angebote. Die Prüfung der Ausrichtung der Plattform hat anhand des konkreten Einzelfalls zu erfolgen und ist allgemein verbindlichen Kriterien nicht zugänglich. Auf Grundlage der bisherigen praktischen Erfahrungen dürften indizielle Bedeutung in diesem Zusammenhang erlangen z. B. das tatsächliche Angebot einer Online-Plattform, der Umgang mit Hinweisen auf Handel mit illegalen Waren und Dienstleistungen und auch die etwa in Allgemeinen Geschäftsbedingungen (AGB) enthaltenen Vorgaben. Schon im Rahmen der Prüfung eines Anfangsverdachts dürften diese Umstände ohne erheblichen Aufwand feststellbar sein.

Im Zusammenspiel mit den zum 1. Juli 2017 durch das Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung vom 13. April 2017 (BGBl. I S. 872) neu gefassten Abschöpfungsvorschriften sichert die Einführung des neuen Tatbestands zudem die effektive Bekämpfung auch der wirtschaftlichen Grundlagen der Underground-Economy.

Die Grundtatbestand des § 126a Absatz 1 StGB-E ist aufgrund der wertungsmäßig einer Beteiligung entsprechenden Begehungsart und der Vorverlagerung der Strafbarkeit mit Geldstrafe oder Freiheitsstrafe von bis zu drei Jahren bedroht. Bei erhöhten Strafdrohungen in anderen Tatbeständen, z. B. § 29 Absatz 1 Nr. 10 BtMG, greift

die Subsidiaritätsklausel des § 126a Absatz 1 S. 1 StGB-E. Aus Gründen der Verhältnismäßigkeit begrenzt § 126a Absatz 2 StGB-E die Strafdrohung auf die für die Katalogtat im Sinne von § 126a Absatz 1 S. 2 StGB-E angedrohte Strafe. Neben dem Grundtatbestand sieht § 126a Absatz 3 StGB-E bei gewerbsmäßiger Begehung aufgrund der erhöhten kriminellen Energie eine mit im Mindestmaß erhöhter Strafdrohung bewehrte Qualifikation vor. Die Erfahrungen der Praxis zeigen, dass nicht jede Tathandlung im Sinne des § 126a StGB-E gewerbsmäßig begangen wird, Anbieter stellen Handelsmöglichkeiten auch oft kostenfrei zur Mehrung des eigenen Ansehens in der Szene bereit. Das Kriterium der Gewerbsmäßigkeit rechtfertigt daher die in der Qualifikation vorgesehene höhere Strafdrohung.

Die erhöhte Strafdrohung verdeutlicht überdies, dass die Qualifikation des § 126a Absatz 3 StGB-E dem Bereich der schweren Kriminalität zuzurechnen ist. Dies begründet in Verbindung mit den Besonderheiten der Tatbegehung mittels internetbasierter Leistung die Aufnahme des Qualifikationstatbestands in den Katalog der Ermittlungsmaßnahme des § 100a Absatz 2 Nr. 1 d) StPO. Die Ermittlungen wegen eines ausschließlich den Grundtatbestand des § 126a Absatz 1 StGB-E erfüllenden Sachverhalts dürften zwar ohne die technischen Überwachungsmaßnahme des § 100a StPO nachhaltig erschwert werden, aus Gründen der Verhältnismäßigkeit ist jedoch die Aufnahme nur der Qualifikation sachgerecht.

II. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 74 Absatz 1 Nummer 1 Grundgesetz.

III. Auswirkungen

Durch die Ausweitung der Strafbarkeit kann ein Mehraufwand für die Strafverfolgungsbehörden entstehen, dessen Umfang derzeit nicht quantifizierbar ist. Im Übrigen werden jedoch keine Mehrkosten entstehen. Für Bürgerinnen und Bürger und die Unternehmen entsteht kein Erfüllungsaufwand.

B.
Zu den einzelnen Vorschriften

Zu Artikel 1 (Änderung des Strafgesetzbuchs)

Zu Nummer 1 (Inhaltsübersicht)

Infolge der Einfügung eines neuen § 126a StGB in das Gesetz ist die Inhaltsübersicht entsprechend anzupassen.

Zu Nummer 2

(§ 126a Absatz 1 - neu -)

Der besonderen Gefährlichkeit des Betreibens von zugangsbeschränkten, insbesondere Darknet-Angeboten, die sich ohne zeitliche, sachliche oder räumliche Grenzen an Personen jeden Alters richten, gegenüber anderen Online-Angeboten wird durch die Fokussierung des Tatbestands auf internetbasierte Leistungen Rechnung getragen, die typischerweise besonderen technischen Beschränkungen hinsichtlich des Zugangs und der Erreichbarkeit unterliegen, z. B. der Nutzung des Tor-Browsers oder vergleichbarer Anforderungen. Das Erfordernis einer bloßen Zugangskennung zur Nutzung einer Leistung, ohne weitere Einschränkung, erfüllt die Anforderungen an eine besondere technische Vorkehrung nicht. Von einer technikoffenen Erfassung aller in Betracht kommenden Kommunikationsmittel, die eingesetzt werden könnten, ohne dass die Beteiligten gleichzeitig körperlich an einem bestimmten Ort anwesend sind, z. B. offene Internetplattformen und -foren, Telemedien, E-Mails und Mobilfunkkontakten, wird aus Gründen der Begrenzung der Strafbarkeit abgesehen.

Der Begriff der Leistung beschreibt alle Angebote, die sich an einen oder mehrere Nutzer richten, ohne stets auf Dauer und wiederholte Nutzung abzuzielen. Zur Abgrenzung der vom Tatbestand erfassten von den nicht strafwürdigen Angeboten ist auf die Ausrichtung des Zwecks oder der Tätigkeit abzustellen. So soll sichergestellt werden, dass ordnungsgemäß eingerichtete Online-Angebote, die entgegen ihrer Zielsetzung auch für den Handel mit illegalen Waren oder Dienstleistungen genutzt werden, nicht der Gefahr strafrechtlicher Verfolgung ausgesetzt werden. Ziel des Angebots im Sinne des § 126a Absatz 1 StGB-E muss das Ermöglichen oder die Förderung von Taten im Sinne des Satzes 2 sein, die eine besondere Gefahr für den Rechtsfrieden darstellen. Dem steht nicht entgegen, dass auch legale Aktivitäten abgewickelt werden sollen, soweit dies lediglich dem Verschleiern der tatsächlichen Zielrichtung dient. Die Prüfung der Ausrichtung einer Online-Plattform hat anhand des konkreten Einzelfalls zu erfolgen und ist allgemein verbindlichen Kriterien nicht zugänglich. Auf Grundlage der bisherigen praktischen Erfahrungen dürften indizielle Bedeutung in diesem Zusammenhang erlangen z. B. das tatsächliche Angebot einer Online-Plattform, der Umgang mit Hinweisen auf Handel mit illegalen Waren und Dienstleistungen und auch die etwa in Allgemeinen Geschäftsbedingungen (AGB) enthaltenen Vorgaben. Schon im Rahmen der Prüfung eines Anfangsverdachts dürften diese Umstände ohne erheblichen Aufwand aufzuklären sein.

Im Sinne einer aus Gründen der Verhältnismäßigkeit angezeigten Beschränkung erfasst § 126a StGB-E nur bestimmte, als für das geschützte Rechtsgut besonders gefährlich einzustufende szenetypische Delikte im Sinne des § 126a Absatz 1 S. 2 StGB-E. Die dort genannten Tatbestände bergen aufgrund der Gefährlichkeit der gehandelten Waren und Dienstleistungen bereits für sich eine besondere Gefahr für die öffentliche Sicherheit. Die Erfahrungen in der Praxis zeigen, dass Schwerpunkte des

illegalen Online-Handels die Bereiche Betäubungsmittel, Waffen, Falschgeld bzw. gefälschte Urkunden, Kinderpornographie und Cyberwerkzeuge, insbesondere Hacker-Programme, sind.

Der größte Anteil der Handelsaktivitäten fällt nach den praktischen Erfahrungen im Bereich der Betäubungsmittel an. Im Bereich gefälschter Urkunden sind besonders Identitätsnachweise zu nennen, die vor allem für betrügerische Bestellungen und die Anlage finanztransaktionsverschleiernder Tarnkonten genutzt werden. Abgeschottete Plattformen im Netz sind zudem einer der vorherrschenden Absatz- und Verteilmechanismen kinderpornographischer Schriften, deren Verbreitungsgrad ohne die dahinterstehenden technischen Infrastrukturen kaum denkbar wäre. Der Bereich der Cyberwerkzeuge wird durch die in § 126a Absatz 1 S. 2 Nr. 7 StGB-E genannten Delikte der §§ 202a, 202b, 202c, 303a und 303b StGB abgedeckt. So werden über Online-Plattformen z. B. Schadsoftwareprogramme angeboten, mit denen Schwachstellen von IT-Systemen ausgenutzt und Sicherungen überwunden werden können. Ebenso wird sogenannte Ransomware, d. h. Software, die Nutzdaten verschlüsselt, um von den Nutzern Zahlungen zur Aufhebung der Verschlüsselung zu erlangen, angeboten. Des Weiteren wird die unmittelbare Durchführung von Cyberangriffen als Dienstleistung offeriert. Hier stehen die sog. Botnetze im Fokus, d. h. eine Vielzahl gekaperter Drittrechner, die unter Täterkontrolle koordinierte Überlastangriffe auf legitime Webseiten und -services durchführen.

Die Begrenzung der Anknüpfungsdelikte auf als besonders gefährlich eingestufte szenetypische Delikte erleichtert die Abgrenzung zu den nicht dem Tatbestand unterfallenden legalen Handelsplattformen. Überdies werden so mögliche Abgrenzungsprobleme im Bereich der beruflichen Handlungen der in § 53 Absatz 1 S. 1 Nr. 5 StPO genannten Personen vermieden. Besonderer tatbestandsausschließender Regelungen, wie etwa in § 202d Absatz 3 StGB, bedarf es nicht.

(§ 126a Absatz 2 - neu -)

Aus Gründen der Verhältnismäßigkeit begrenzt § 126a Absatz 2 StGB-E die Strafdrohung auf die für die Katalogtat im Sinne von § 126a Absatz 1 S. 2 StGB-E angedrohte Strafe. Dieses Vorgehen orientiert sich an den Regelungen in vergleichbaren Vorschriften, z. B. §§ 202d Absatz 2, 257 Absatz 2, 258 Absatz 3 StGB. Relevant werden kann diese Regelung angesichts der Strafdrohungen der Katalogtaten für die in § 126a Absatz 1 Satz 2 Nr. 7 StGB-E genannten Fälle der §§ 149, 202b, 202c, 275, 276 und 303a StGB. Die übrigen Taten enthalten jeweils Höchststrafdrohungen von mindestens drei Jahren Freiheitsstrafe.

(§ 126a Absatz 3 - neu -)

Neben dem Grundtatbestand sieht § 126a Absatz 3 StGB-E bei gewerbsmäßiger Begehung aufgrund der erhöhten kriminellen Energie eine mit im Mindestmaß erhöhter Strafdrohung bewehrte Qualifikation vor. Die Erfahrungen der Praxis zeigen, dass nicht jede Tathandlung im Sinne des § 126a StGB-E gewerbsmäßig begangen wird, Anbieter stellen Handelsmöglichkeiten auch oft kostenfrei zur Mehrung des eigenen Ansehens in der Szene bereit. Das Kriterium der Gewerbsmäßigkeit rechtfertigt daher die vorgesehene höhere Strafdrohung, die zudem verdeutlicht, dass die Qualifikation des § 126a Absatz 3 StGB-E dem Bereich der schweren Kriminalität zuzurechnen ist.

Der Strafrahmen orientiert sich auf Grundlage der erhöhten kriminellen Energie von auf Dauer angelegten, gewinnorientierten Strukturen an denen für vergleichbare Delikte bei gewerbsmäßiger Begehungsweise, z. B. § 260 Absatz 1 Nr. 1 StGB (Hehlerei), § 263 Absatz 3 S. 2 Nr. 1 StGB (Betrug) - auch in Verbindung mit § 263a Absatz 2 StGB (Computerbetrug) -, § 267 Absatz 3 S. 2 Nr. 1 StGB (Urkundenfälschung) und
§ 303b Absatz 4 S. 2 Nr. 2 StGB (Computersabotage). Das Delikt ist, anders als einige der vorgenannten Beispiele, als Qualifikation ausgestaltet, um dem Umstand Rechnung zu tragen, dass Online-Plattformen für illegale Waren und Dienstleistungen den Nährboden weiter Bereiche des Cybercrime darstellen. Die Bedeutung der Plattformen entspricht dabei der vergleichbarer Einrichtungen im legalen Bereich. Der Unternehmensgegenstand zahlreicher, auch international erfolgreicher Unternehmen besteht im Unterhalt einer Infrastruktur für den örtlich und zeitlich ungebundenen Austausch von Waren und Dienstleistungen. Ebenso stellen sich Funktion und Bedeutung der illegalen Plattformen dar, denen eine erhebliche Ausstrahlwirkung im Bereich des Cybercrime zukommt.

Zu Artikel 2 (Änderung der Strafprozessordnung)

(§ 100a Absatz 2 Nummer 1 Buchstabe d - neu -)

Für eine effektive Verfolgung von mittels internetbasierter Kommunikation begangener Taten ist es regelmäßig erforderlich, die Kommunikationswege der Beteiligten nachzuvollziehen. Andere Ermittlungsmethoden führen nicht zur Aufklärung der Tatstrukturen, die sich ohne reelle Kontakte mit etwaigen Beteiligten in der analogen Welt gestalten. Diese Notwendigkeit rechtfertigt indes nicht die Eröffnung eingriffsintensiver Ermittlungsmaßnahmen für alle Fälle der Informations- und Kommunikationskriminalität. Mit Blick auf das durch Maßnahmen gemäß § 100a StPO betroffene Grundrecht aus Art. 10 GG gebietet der Grundsatz der Verhältnismäßigkeit eine Abwägung im Einzelfall, ob bestimmte Straftaten durch den Gesetzgeber im Rahmen seines Beurteilungsspielraums als derart schwer eingestuft werden, dass ein entsprechender Tatverdacht Grundrechtseingriffe rechtfertigen kann (zu vgl. *BVerfG*

NJW 2012, 833 – Rnr. 203 ff.). Dabei sind insbesondere das geschützte Rechtsgut und dessen Bedeutung für die Rechtsgemeinschaft in den Blick zu nehmen.

Die in § 126a Absatz 3 StGB-E geregelte Qualifikation im Falle gewerbsmäßigen Handelns weist gegenüber dem Grundtatbestand aufgrund der auf Dauer ausgelegten Tatbegehung zur Erzielung einer nicht nur vorübergehenden Einnahmequelle einen deutlich gesteigerten Unrechtsgehalt auf, der auch in anderen Deliktsbereichen zu einer erhöhten Strafdrohung führt, z. B. § 260 Absatz 1 Nr. 1 StGB. Damit werden die Gefahren für die bereits durch den Grundtatbestand und die Katalogtaten geschützten Rechtsgüter weiter und dauerhaft erhöht. In diesen Fällen, in denen ein Täter nicht nur gelegentlich oder ohne eigennütziges finanzielles Interesse gezielt Strukturen der kriminellen Infrastruktur schafft, handelt es sich demnach bereits um einen schwere Straftat im Sinne des § 100a StPO.

Zu Artikel 3 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.