Rat der
Europäischen Union

Brüssel, den 14. September 2017
(OR. en)

12209/17

DROIPEN 121
TELECOM 210
JAI 788
CYBER 130

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	13. September 2017
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2017) 474 final
Betr.:	BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT über den Umfang, in dem die Mitgliedstaaten die für die Einhaltung der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI erforderlichen Maßnahmen getroffen haben

Die Delegationen erhalten in der Anlage das Dokument COM(2017) 474 final.

Anl.: COM(2017) 474 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 13.9.2017
COM(2017) 474 final

BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über den Umfang, in dem die Mitgliedstaaten die für die Einhaltung der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI erforderlichen Maßnahmen getroffen haben

Inhaltsverzeichnis

1. Einleitung

Nach der von Europol vorgenommenen Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (IOCTA) 2016 wird die Cyberkriminalität immer aggressiver und ist in zunehmendem Maße auf Konfrontation ausgerichtet. Dies ist aus den verschiedenen Formen der Cyberkriminalität, einschließlich der Angriffe auf Informationssysteme ersichtlich.[1] Zu den ernst zu nehmenden Angriffsformen, die von Europol genannt werden, zählt der Einsatz von Schadsoftware und Social-Engineering-Methoden, um in ein Informationssystem einzudringen und die Kontrolle über dieses zu erlangen, um Nachrichten abzufangen und um Netzangriffe großen Ausmaßes, auch gegen kritische Infrastrukturen, zu starten. Solche Angriffe werden als ernsthafte Bedrohung für unsere Gesellschaft betrachtet.

Angesichts der zunehmenden Menge an Informationen, die in Clouds gespeichert werden, und der heutigen extremen Mobilität von Informationen und Straftätern ist die grenzüberschreitende Zusammenarbeit zwischen Strafverfolgungsbehörden für die meisten Ermittlungen im Bereich der Cyberkriminalität unverzichtbar geworden.

Um diese Verbrechen wirksam zu bekämpfen, müssen die Mitgliedstaaten gemeinsam definieren, welche Handlungen als Angriffe auf Informationssysteme zu erachten sind. Sie müssen ferner Art und Umfang ihrer Sanktionen angleichen und über entsprechende operative Mittel verfügen, um Straftaten melden und um Informationen zwischen Behörden austauschen zu können. Vor diesem Hintergrund haben das Europäische Parlament und der Rat am 12. August 2013 die Richtlinie 2013/40/EU (im Folgenden „Richtlinie“) über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates[2] erlassen.

1.1 Ziele und Anwendungsbereich der Richtlinie

Zu den Zielen der Richtlinie zählen die Angleichung des Strafrechts der Mitgliedstaaten[3] im Bereich Angriffe auf Informationssysteme und die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden. Dies soll durch die Erarbeitung von Mindestvorschriften zur Definition von Straftaten und die Festlegung einschlägiger Strafen im Bereich der Angriffe auf Informationssysteme sowie durch die Einrichtung operativer nationaler Kontaktstellen realisiert werden, die an sieben Wochentagen 24 Stunden täglich zur Verfügung stehen.

[1] Europol, *2016 Internet Organised Crime Threat Assessment (IOCTA)*, abrufbar unter: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf.

[2] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32013L0040&qid=1502108317397&from=DE

[3] Sofern nicht ausdrücklich etwas anderes angegeben ist, bezieht sich im Folgenden der Begriff „Mitgliedstaaten“ oder „alle Mitgliedstaaten“ auf die Mitgliedstaaten, die durch die Richtlinie gebunden sind, d. h. auf alle Mitgliedstaaten mit Ausnahme Dänemarks, das sich nach den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) beigefügten Protokolls über die Position Dänemarks nicht an der Annahme der Richtlinie beteiligt hat. Nach Artikel 3 des Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands haben sich beide Mitgliedstaaten an der Annahme der Richtlinie beteiligt und sind durch sie gebunden.

Die **Begriffsbestimmungen** der Richtlinie enthalten die folgenden Definitionen:

- „Informationssystem“ (Artikel 2 Buchstabe a)[4]. Diese Begriffsbestimmung entspricht zum größten Teil der Definition des Begriffs „Computersystem“ in Artikel 1 Buchstabe a des Übereinkommens des Europarats über Computerkriminalität vom 23. November 2001 (im Folgenden „Budapester Übereinkommen“), mit dem Unterschied, dass die Richtlinie ausdrücklich auch Computerdaten an sich einbezieht.
- „Computerdaten“ (Artikel 2 Buchstabe b). Die Begriffsbestimmung entspricht der Definition in Artikel 1 Buchstabe b des Budapester Übereinkommens, außer dass sie sich auf ein Informationssystem und nicht auf ein Computersystem bezieht.
- „juristische Person“ (Artikel 2 Buchstabe c). Die Definition zielt darauf ab, die Verantwortlichkeit natürlicher und juristischer Personen zu gewährleisten, während Staaten, andere Körperschaften des öffentlichen Rechts und öffentlich-rechtliche internationale Organisationen ausgenommen sind.
- „unbefugt“ (Artikel 2 Buchstabe d). Die Definition bezieht sich auf einen allgemeinen Grundsatz des Strafrechts und zielt darauf ab, eine strafrechtliche Verantwortung von Personen zu verhindern, deren Handeln entweder nach den nationalen Rechtsvorschriften zulässig ist oder vom Eigentümer oder einem anderen Rechtsinhaber des Informationssystems oder eines Teils dieses Systems gestattet wurde.

Es werden besondere Straftatbestände definiert, und zwar:

- Rechtswidriger Zugang zu Informationssystemen (Artikel 3).
- Rechtswidriger Systemeingriff (Artikel 4); dazu zählt jeder rechtswidrige Zugang zu einem Informationssystem, durch den eine schwere Behinderung oder Störung des Betriebs dieses Systems verursacht wird.
- Rechtswidriger Eingriff in Daten (Artikel 5) meint jeden unrechtmäßigen Eingriff in Computerdaten wie beispielsweise die Beeinträchtigung ihrer Integrität oder ihrer Zugänglichkeit.
- Rechtswidriges Abfangen (Artikel 6) nichtöffentlicher Computerdaten und elektromagnetischer Abstrahlungen aus einem Informationssystem, das Träger solcher Daten ist.
- Rechtswidrige Bereitstellung von Tatwerkzeugen zur Begehung der genannten Straftaten (Artikel 7). In diesem Zusammenhang können die Tatwerkzeuge aus einem Computerprogramm sowie aus einem Computerpasswort oder anderen Daten bestehen, die den Zugang zu einem Informationssystem ermöglichen.

Darüber hinaus **weitet** die Richtlinie die **strafrechtliche Verantwortung** auf die Anstiftung und Beihilfe zur Begehung einer der oben genannten Straftaten sowie auf den Versuch zur Begehung dieser Straftaten seitens einer natürlichen und/oder juristischen Person **aus** (Artikel 8). Dabei beziehen sich Anstiftung und Beihilfe auf alle Straftaten im Sinne der Artikel 3 bis 7, während der Versuch ausschließlich im Hinblick auf die Straftaten im Sinne der Artikel 4 und 5 strafbar ist.

[4] Bei allen genannten Artikeln handelt es sich um Artikel der Richtlinie, sofern nichts anderes angegeben ist.

Artikel 9 macht Mindestvorgaben hinsichtlich der **Höchststrafen** für die Straftaten im Sinne der Richtlinie und zwar:

- Als Grundstrafe wird für alle Straftaten, außer der im Sinne des Artikels 8, eine Freiheitsstrafe im Höchstmaß von mindestens zwei Jahren festgelegt (Artikel 9 Absatz 2).
- Straftaten im Sinne der Artikel 4 und 5 werden mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet, wenn durch sie eine beträchtliche Anzahl von Informationssystemen beeinträchtigt wurde (allgemein als Botnetz-Kriminalität bezeichnet; Artikel 9 Absatz 3).
- Eine Freiheitsstrafe im Höchstmaß von mindestens fünf Jahren ist für alle Straftaten im Sinne der Artikel 4 und 5 vorzusehen, wenn diese von einer kriminellen Vereinigung begangen wurden (Artikel 9 Absatz 4 Buchstabe a), einen schweren Schaden verursachen (Artikel 9 Absatz 4 Buchstabe b) oder gegen ein Informationssystem einer kritischen Infrastruktur verübt wurden (Artikel 9 Absatz 4 Buchstabe c).
- Wurde eine Straftat nach den Artikeln 4 und 5 im Zusammenhang mit dem Missbrauch der personenbezogenen Daten einer anderen Person begangen, müssen die Mitgliedstaaten sicherstellen, dass dies als erschwerender Umstand eingestuft werden kann, soweit der betreffende Umstand nicht bereits eine andere Straftat darstellt (Artikel 9 Absatz 5).

Die darauffolgenden Artikel machen Mindestvorgaben in Bezug auf die **Verantwortlichkeit juristischer Personen** (Artikel 10) und listen Beispiele für mögliche Sanktionen gegen diese juristischen Personen auf (Artikel 11).

In Anbetracht der Tatsache, dass die oben genannten Straftaten an einem Ort begangen (im Sinne von „ausgeführt“) werden können, an dem der Straftäter tatsächlich handelt, die Auswirkungen auf das angegriffene Informationssystem unter Umständen jedoch an einem anderen Ort festgestellt werden, macht Artikel 12 Vorgaben in Bezug auf die Begründung der **gerichtlichen Zuständigkeit**, wobei unterschieden wird zwischen:

- dem Ort, an dem sich der Straftäter bei der Begehung der Straftat physisch aufhält,
- dem Ort, an dem sich das angegriffene Informationssystem befindet,
- der Staatsangehörigkeit des Straftäters,
- seinem gewöhnlichen Aufenthaltsort und
- dem Ort der Niederlassung der juristischen Person, zu deren Gunsten der die Straftat begangen wird.

Was den Informationsaustausch betrifft, müssen die Mitgliedstaaten nach Artikel 13 Absatz 1 sicherstellen, dass sie über operative nationale **Kontaktstellen** verfügen, die an sieben Wochentagen 24 Stunden täglich zur Verfügung stehen, damit sie in der Lage sind, bei dringenden Ersuchen ausländischer Behörden innerhalb von 8 Stunden zu antworten.

Darüber hinaus müssen die Mitgliedstaaten die erforderlichen Maßnahmen treffen, um die **Meldung** der oben aufgeführten Straftaten bei den zuständigen nationalen Behörden zu **ermöglichen** (Artikel 13 Absatz 3) und um eine Mindestmenge an **statistischen Daten** zu diesen Straftaten erheben und übermitteln zu können (Artikel 14).

1.2 Zweck und Methodik dieses Berichts

Nach Artikel 16 müssen die Mitgliedstaaten die erforderlichen Rechts- und Verwaltungsvorschriften in Kraft setzen, um der Richtlinie bis zum 4. September 2015 nachzukommen, und der Kommission den Wortlaut der Maßnahmen übermitteln.

Mit diesem Bericht erfüllt die Kommission ihre Verpflichtung aus Artikel 17 der Richtlinie, dem Europäischen Parlament und dem Rat einen Bericht darüber vorzulegen, inwieweit die Mitgliedstaaten die zur Einhaltung der Richtlinie erforderlichen Maßnahmen ergriffen haben. Der Bericht soll demnach einen knappen, aber informativen Überblick über die wichtigsten Umsetzungsmaßnahmen geben, die von den Mitgliedstaaten getroffen wurden.

Im Zuge der Umsetzung der Richtlinie in den Mitgliedstaaten mussten Informationen über die einschlägigen Rechtsvorschriften und Verwaltungsmaßnahmen erhoben und analysiert sowie neue Rechtsvorschriften oder – in den meisten Fällen – Änderungsrechtsakte erarbeitet, bis zu ihrer Verabschiedung weiterverfolgt und schließlich der Kommission mitgeteilt werden.

Bis zum Ablauf der Umsetzungsfrist hatten 22 Mitgliedstaaten die Kommission über die vollständige Umsetzung der Richtlinie unterrichtet. Im November 2015 leitete die Kommission gegen die übrigen 5 Mitgliedstaaten Vertragsverletzungsverfahren wegen Nichtmitteilung nationaler Umsetzungsmaßnahmen ein: BE, BG, EL, IE und SI[5]. Am 31. Mai 2017 waren die Vertragsverletzungsverfahren wegen Nichtmitteilung nationaler Umsetzungsmaßnahmen gegen BE, BG und IE noch anhängig.[6]

Die Beschreibungen und Analysen in diesem Bericht basieren auf den Informationen, die von den Mitgliedstaaten bis zum 31. Mai 2017 vorgelegt wurden.[7] Die nach diesem Tag eingegangenen Mitteilungen wurden nicht berücksichtigt. Dagegen wurden alle Maßnahmen berücksichtigt, die zu nationalen Rechtsvorschriften und Gerichtsentscheidungen sowie – gegebenenfalls – zur allgemein anerkannten Rechtstheorie mitgeteilt wurden. Darüber hinaus hat die Kommission die Mitgliedstaaten im Zuge der Analyse direkt kontaktiert, sofern zusätzliche Informationen oder Klarstellungen erforderlich und angemessen schienen. Alle Informationen, die zusammengetragen wurden, wurden in die Analyse einbezogen.

Infolgedessen ist es möglich, dass in diesem Bericht weitere Probleme bei der Umsetzung und andere Bestimmungen, die der Kommission nicht mitgeteilt wurden, sowie weitere legislative und nicht legislative Entwicklungen nicht erfasst sind. Daher behält sich die Kommission vor, ungeachtet dieses Berichts einige Bestimmungen weiter zu evaluieren und die Mitgliedstaaten auch weiterhin bei der Umsetzung der Richtlinie zu unterstützen.

[5] Die diesem Bericht verwendeten Länderkürzel richten sich nach den folgenden Vorgaben: http://publications.europa.eu/code/de/de-5000600.htm.

[6] Informationen über die Beschlüsse der Kommission in Bezug auf Vertragsverletzungsverfahren können abgerufen werden unter: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=de.

[7] IE hat die vollständige Umsetzung der Richtlinie am 31. Mai 2017 mitgeteilt.

2. Umsetzungsmaßnahmen

2.1 Begriffsbestimmungen (Artikel 2 der Richtlinie)

Artikel 2 der Richtlinie enthält die Legaldefinitionen für „Informationssystem“ (Buchstabe a), „Computerdaten (Buchstabe b), „juristische Person“ (Buchstabe c) und „unbefugt“ (Buchstabe d). Nur CY und UK (Gibraltar) haben Rechtsvorschriften erlassen, die alle Aspekte der genannten Definitionen abdecken. Dies bedeutet im Einzelnen:

a) Informationssystem

Die in der Richtlinie angeführte Begriffsbestimmung baut auf der Definition des Begriffs „Computersystem“ in Artikel 1 Buchstabe a des Budapester Übereinkommens auf, wobei zusätzlich die Computerdaten selbst als Teil des Informationssystems in die Definition einbezogen werden. CY, EL, IE, FI, HR, MT, PT und UK (Gibraltar) haben Rechtsvorschriften erlassen, die eine Definition des Begriffs Informationssystem umfassen; DE, ES, FR, LU, LV, PL, SE und SK haben keine aufschlussreichen Informationen übermittelt. In den übrigen Mitgliedstaaten – d. h. AT, BE, BG, CZ, EE, HU, IT, LT, NL, RO, SI und UK (außer Gibraltar) – wird der Begriff „Computerdaten“ in den Begriffsbestimmungen nicht ausdrücklich genannt. Dies deutet darauf hin, dass diese Mitgliedstaaten auf Artikel 1 Buchstabe a des Budapester Übereinkommens mit einem der Definition von „Computersystem“ entsprechenden Anwendungsbereich Bezug nehmen.

b) Computerdaten

Der Begriff „Computerdaten“ wurde von AT, BG, CY, CZ, DE, EE, EL IE, FI, HR, LT, MT, NL, PT, RO und UK (Gibraltar) in die Rechtsvorschriften aufgenommen; ES, FR, IT, LU, LV, PL, SE, SK und UK (außer Gibraltar) haben keine aufschlussreichen Informationen übermittelt. Allerdings macht in SE der spezifische Aufbau der bezugnehmenden Artikel diese Begriffsbestimmung überflüssig. Was die übrigen Mitgliedstaaten betrifft, so bezieht HU die Definition des Begriffs „Computerdaten“ lediglich auf die in Artikel 4 und 5 der Richtlinie beschriebenen Straftaten; BE und SI haben versäumt, den Passus „einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann“ in die Definition des Begriffs „Computerdaten“ einzubeziehen.

c) Juristische Person

Außer in LU (das keine Informationen übermittelt hat, die Aufschluss über die Umsetzung von Artikel 2 Buchstabe c geben) hat die Umsetzung der Definition von „juristische Person“ keine Probleme bereitet. Dies ist allgemein darauf zurückzuführen, dass dieser Begriff bereits in den meisten zivil- oder handelsrechtlichen Bestimmungen der Mitgliedstaaten definiert ist. Nur CY hat eine besondere Bestimmung in die zur Umsetzung der Richtlinie erlassenen Maßnahmen aufgenommen.

d) Unbefugt

Was die Bestimmung des Begriffs „unbefugt“ (Artikel 2 Buchstabe d) betrifft, so haben nur CY, IE, RO und UK (Gibraltar) entsprechende Umsetzungsmaßnahmen mitgeteilt. Das bedeutet, dass 23 Mitgliedstaaten keine Umsetzungsmaßnahmen in Bezug auf diese Definition getroffen haben. Allerdings ist darauf hinzuweisen, dass in allen Mitgliedstaaten der allgemeine Grundsatz gilt, dass niemand für eine Handlung strafrechtlich zur Verantwortung gezogen werden kann, die mit einer entsprechenden Befugnis vorgenommen wurde.

2.2 Besondere Straftatbestände (Artikel 3 bis 7 der Richtlinie)

a) Rechtswidriger Zugang zu Informationssystemen
Der Straftatbestand des rechtswidrigen Zugangs zu einem Informationssystem (Artikel 3 der Richtlinie) wurde in den nationalen Rechtsvorschriften von AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE und SK umgesetzt.

In allen übrigen Mitgliedstaaten, d. h. BE, BG, DE, EE, HR, HU, IT, LV, MT, RO, SI und UK, unterscheidet die diesbezügliche Beschreibung in der jeweiligen nationalen Rechtsvorschrift nicht, ob der Zugang zu dem Informationssystem als Ganzem oder nur zu einem Teil des Systems erlangt wurde, obwohl dies von der Richtlinie ausdrücklich vorgegeben wird. Darüber hinaus ist in der Umsetzung von DE nicht der reine Zugang zur Computer-Hardware erfasst; AT und LU haben zusätzliche Anforderungen hinsichtlich einer besonderen Absicht (Erlangung von Kenntnissen, Zufügen von Nachteilen oder betrügerische Absicht) aufgenommen; LV knüpft die Erfüllung des Tatbestands an die Verursachung eines erheblichen Schadens. Der Anwendungsbereich der nationalen Rechtsvorschriften von BE, BG, FR, HR, LU, MT, PT, RO, SI und UK ist weiter gefasst als der der Richtlinie, da keine Verletzung von Sicherheitsmaßnahmen erforderlich ist, um eine strafrechtliche Verantwortung zu begründen. Die übrigen Mitgliedstaaten verweisen entweder wortgetreu darauf, dass die Straftat durch eine Verletzung von Sicherheitsmaßnahmen (CY, EL und SK) begangen worden sein muss, oder sie verwenden eine ähnliche Formulierung, um diesen Aspekt zu beschreiben (AT, CZ, DE, EE, ES, FI, HU, IT, LT, LV, NL, PL und SE).

b) Rechtswidriger Systemeingriff
Artikel 4 der Richtlinie betrifft rechtswidrige Systemeingriffe. Die Richtlinie nennt 8 mögliche Handlungen (Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern, Unterdrücken und Unzugänglichmachen von Computerdaten) und 2 mögliche Folgen dieser Handlungen (schwere Behinderung oder Störung des Betriebs eines Informationssystems). BE, CY, CZ, EL, IE, FR, HR, LU, MT, PT, SE und UK (außer Gibraltar) haben entsprechende legislative Maßnahmen getroffen. BG bezieht sich lediglich auf das Platzieren eines Virus, während die übrigen Mitgliedstaaten (AT, DE, EE, ES, HU, IT, LV, NL, PL, RO, SI, SK und UK) 1 bzw. bis zu 4 der in der Richtlinie genannten möglichen Handlungen nicht ausdrücklich nennen. In diesem Zusammenhang ist festzustellen, dass die meisten Probleme bei den Begriffen „Beeinträchtigen“ (keine Erwähnung in 8 Fällen) und „Unzugänglichmachen“ (fehlt in 9 Fällen) zu beobachten sind.

c) Rechtswidriger Eingriff in Daten
Artikel 5 der Richtlinie befasst sich mit dem rechtswidrigen Eingriff in Daten und führt die folgenden 6 möglichen Handlungen auf: Löschen, Beschädigen, Beeinträchtigen, Verändern, Unterdrücken und Unzugänglichmachen von Computerdaten. CY, EL, IE und MT haben den Wortlaut der Bestimmung übernommen; BE, CZ, LT, PT und SE haben allgemeinere Begriffe verwendet, um alle angeführten möglichen Handlungen zu erfassen. Die Umsetzungsmaßnahmen aller anderen Mitgliedstaaten decken nicht jede mögliche Handlungen ab, sondern beziehen sich nur auf 5 (FI und SK) oder weniger der genannten Alternativen (AT, BG, DE, EE, FR, HR, HU, IT, LU, NL, PL, RO, SI und UK). Die meisten Probleme ergaben sich bei den Handlungen „Beschädigen“ (fehlt in 8 Fällen), „Beeinträchtigen“ (13 Fälle), „Unterdrücken“ (11 Fälle) und „Unzugänglichmachen“ (13 Fälle). Zusätzlich zum Wortlaut der Richtlinie setzt FI für die Begründung der strafrechtlichen Verantwortung das Vorliegen einer „Absicht, Schaden oder finanziellen Verlust herbeizuführen“ voraus, während LT und LV die Anforderung stellen, dass „die Handlung eine ernste Beeinträchtigung oder einen erheblichen Schaden verursacht“.

d) Rechtswidriges Abfangen von Daten
Artikel 6 betrifft das rechtswidrige Abfangen von Daten und schützt die nichtöffentliche Übermittlung von Computerdaten und elektromagnetische Abstrahlungen aus einem Informationssystem, das Träger solcher Daten ist. CY, CZ, DE, ES, IE, FI, HR, LV, MT, RO, SE, SK und UK (Gibraltar) haben Rechtsvorschriften erlassen, mit denen Artikel 6 vollständig umsetzt wird. Der allgemeine Anwendungsbereich der Richtlinie, der sich auf das Abfangen von Computerdaten bezieht, wurde auf Mitteilungen (AT und BG), auf die Beobachtung einer Person (EE) oder auf Schriftwechsel (FR und HU) begrenzt. Darüber hinaus decken die Umsetzungsmaßnahmen der folgenden Mitgliedstaaten nicht das Abfangen elektromagnetischer Abstrahlungen ab: BE, BG, EE, FR, HU, IT, LT, LU, NL, PL, PT, SI und UK (außer Gibraltar). Einige Mitgliedstaaten setzen zudem eine besondere Absicht (wie beispielsweise die Erlangung von Kenntnissen oder eines wirtschaftlichen Gewinns oder die Verursachung von Nachteilen – AT, EL, HU) oder besondere zusätzliche Handlungen voraus (wie beispielsweise die Aufzeichnung oder die Zurkenntnisnahme des abgefangenen Inhalts – BG und HU).

e) Tatwerkzeuge
Artikel 7 stellt eine Reihe von Handlungen im Zusammenhang mit Computerprogrammen oder Zugangscodes unter Strafe, wenn diese zur Begehung der in den Artikeln 3 bis 6 genannten Straftaten vorgenommen werden: das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten und anderweitige Verfügbarmachen dieser Instrumente. AT, BE, CY, DE, EL, IE und SK haben entsprechende nationale Rechtsvorschriften erlassen. Einige Mitgliedstaaten decken nicht alle aufgeführten Straftaten ab (EE, IT, MT, PL und SI). Einige Mitgliedstaaten weisen nicht darauf hin, dass der Täter im Sinne des Artikels 7 eine andere Person sein kann als diejenige, die die in den Artikeln 3 bis 6 genannten Straftaten begeht (CZ und SI). Einige setzen eine besondere Absicht (Zufügen von Schaden oder betrügerisches Handeln – FI, IT und LU), eine besondere Folge wie zum Beispiel Geheimnisverletzung (BG) oder zumindest die Vorbereitung der genannten Straftaten (SE) voraus. Letztlich sind die Unterschiede zwischen Artikel 7 und den nationalen Maßnahmen darin begründet, dass nicht alle der aufgeführten möglichen Handlungen umgesetzt wurden. Dies trifft auf BG, CZ, EE, ES, FR, HR, HU, IT, LT, LU, LV, PL, PT, RO, SI und UK zu. So erwähnt LU in seinen Rechtsvorschriften fünf der sechs in der Richtlinie genannten Handlungen, während die anderen Mitgliedstaaten nur vier oder weniger ausdrücklich erwähnen.

Nur ES hat die Handlung „Beschaffen zwecks Gebrauchs“ umgesetzt.

2.3 Allgemeine Vorschriften in Bezug auf die genannten Straftaten (Artikel 8 bis 12 der Richtlinie)

a) Anstiftung und Beihilfe
Nach Artikel 8 Absatz 1 müssen die Mitgliedstaaten sicherstellen, dass die Anstiftung oder Beihilfe zur Begehung einer Straftat im Sinne der Artikel 3 bis 7 unter Strafe gestellt wird. Nicht alle Mitgliedstaaten haben diese Bestimmung umgesetzt.

b) Versuch
Nach Artikel 8 Absatz 2 ist der Versuch der Begehung einer Straftat im Sinne der Artikel 4 und 5 unter Strafe zu stellen. PT hat nicht alle Arten des Versuchs der Begehung von Straftaten im Sinne des Artikels 4 einbezogen, und SE begründet keine strafrechtliche Verantwortung für die versuchte Straftat der „Verletzung des Kommunikationsgeheimnisses“;

alle anderen Mitgliedstaaten haben Rechtsvorschriften erlassen, durch die diese Bestimmung umgesetzt wird.

c) Strafen

aa) Allgemeine Bestimmung

Nach Artikel 9 Absatz 1 müssen die Mitgliedstaaten generell sicherstellen, dass die in der Richtlinie genannten Straftaten mit wirksamen, angemessenen und abschreckenden Strafen geahndet werden. Zwar wird angenommen, dass fast alle Mitgliedstaaten dieser Bestimmung nachgekommen sind, jedoch erfüllen AT, BE, BG, IT, PT, SE und SI nicht in jedem Fall die Anforderungen an die in Artikel 9 Absatz 2 genannte Mindesthöhe der Höchststrafen (siehe oben Abschnitt 1.1). Dies stellt die Umsetzung von Artikel 9 Absatz 1 infrage, da davon auszugehen ist, dass die in Artikel 9 Absatz 2 genannte Mindesthöhe eine Mindestvoraussetzung ist, um die Wirksamkeit, Angemessenheit und abschreckende Wirkung der Strafen zu gewährleisten.

bb) Allgemeine Mindesthöhe der Höchststrafen

Nach Artikel 9 Absatz 2 sind die in den Artikeln 3 bis 7 genannten Standardstraftaten mit einer Freiheitsstrafe im Höchstmaß von mindestens 2 Jahren zu ahnden. Die meisten Mitgliedstaaten haben diese Bestimmung umgesetzt. Nur in 6 Mitgliedstaaten sind gewisse Abweichungen festzustellen: AT (Freiheitsstrafe im Höchstmaß von 6 Monaten), BG (Freiheitsstrafe im Höchstmaß von 1 Jahr für alle Straftaten außer für das rechtswidrige Abfangen von Daten), IT (Freiheitsstrafe im Höchstmaß von 1 Jahr für die Straftat im Sinne des Artikels 7 Buchstabe b), PT (Freiheitsstrafe im Höchstmaß von 1 Jahr für die Straftat im Sinne des Artikels 3), SE (Freiheitsstrafe im Höchstmaß von 1 Jahr für das „Zufügen von Schaden“) und SI (Freiheitsstrafe im Höchstmaß von 1 Jahr für die Straftaten im Sinne der Artikel 3, 6 und 7). In BE werden Straftaten im Sinne der Artikel 3, 6 und 7 nur dann mit der Mindesthöchststrafe geahndet, wenn die Straftaten in betrügerischer Absicht begangen wurden.

cc) Beträchtliche Anzahl von beeinträchtigten Informationssystemen

Artikel 9 Absatz 3 hebt die Mindesthöchststrafe auf eine Freiheitsstrafe von 3 Jahren an, sofern eine beträchtliche Anzahl von Informationssystemen durch eine Straftat im Sinne der Artikel 4 und 5 beeinträchtigt wurde. Im Allgemeinen haben die Mitgliedstaaten entsprechende Rechtsvorschriften erlassen. DE nimmt lediglich auf Informationssysteme Bezug, „die für einen anderen von wesentlicher Bedeutung“ sind, in FI muss die Straftat „als Ganzes“ bewertet werden, um sie mit dem höheren Strafmaß zu ahnden, und LV bezieht sich nicht auf eine beträchtliche Anzahl von Informationssystemen (oder eine ähnliche Formulierung), sondern lediglich auf die Verursachung eines „erheblichen Schadens“. BG und SI haben keine aufschlussreichen Informationen übermittelt.

dd) Kriminelle Vereinigungen

Nach Artikel 9 Absatz 4 Buchstabe a werden Straftaten im Sinne der Artikel 4 und 5 mit Freiheitsstrafen im Höchstmaß von mindestens 5 Jahren geahndet, wenn sie sie im Rahmen einer kriminellen Vereinigung im Sinne des Rahmenbeschlusses 2008/841/JI begangen wurden.

Wieder haben die meisten Mitgliedstaaten die Bestimmung des Artikels 9 Absatz 4 Buchstabe a umgesetzt. Im Strafrecht von LU und SI decken die Bestimmungen zu Straftaten, die von einer kriminellen Vereinigung begangen werden, nicht die Cyberkriminalität ab. Die Rechtsvorschriften von BE sehen für Straftaten im Sinne des Artikels 5 eine Freiheitsstrafe im Höchstmaß von nur 3 Jahren vor, die Rechtsvorschriften von DE schließen natürliche Personen als Opfer der Straftaten aus, die Rechtsvorschriften von FI erfordern eine

zusätzliche Bewertung der Straftat „als Ganzes“, und die Rechtsvorschriften von SE sehen eine Freiheitsstrafe im Höchstmaß von 4 Jahren für das „Zufügen eines schweren Schadens“ vor.

ee) Verursachung eines schweren Schadens

Nach Artikel 9 Absatz 4 Buchstabe b kommt für alle Straftaten im Sinne der Artikel 4 und 5 eine Freiheitsstrafe im Höchstmaß von mindestens 5 Jahren zur Anwendung, wenn durch sie ein schwerer Schaden verursacht wird. Obwohl nicht definiert wird, was als schwerer Schaden zu betrachten ist, haben alle Mitgliedstaaten außer BG, DE, FI, HU, LU und SE Rechtsvorschriften erlassen, die mit der Richtlinie übereinstimmen. HU hat keine aufschlussreichen Informationen übermittelt. BG sieht keine Mindesthöchststrafe von 5 Jahren vor; LU verweist auf eine allgemeine strafrechtliche Bestimmung hinsichtlich der Verursachung eines schweren Schadens, die sich nicht auf Cyberkriminalität erstreckt. Geringfügige Abweichungen sind festzustellen in DE (keine Einbeziehung natürlicher Personen als Opfer der Straftaten), FI (für ein höheres Strafmaß zusätzliche Bewertung der Straftat „als Ganzes“ erforderlich) und SE (Freiheitsstrafe im Höchstmaß von 4 Jahren für das „Zufügen eines schweren Schadens“).

ff) Informationssysteme einer kritischen Infrastruktur

Die Einbeziehung von Angriffen gegen Informationssysteme einer kritischen Infrastruktur als Straftat im Sinne der Artikel 4 und 5 hat zur Folge, dass diese – wie in Artikel 9 Absatz 4 Buchstabe c festgelegt – mit einer Freiheitsstrafe im Höchstmaß von mindestens 5 Jahren geahndet werden.

Während die meisten Mitgliedstaaten diese Bestimmung umgesetzt haben, hat BG keine diesbezüglichen Informationen über die Umsetzung übermittelt. BE hat für Straftaten im Sinne des Artikels 5 eine Höchststrafe von 3 Jahren festgelegt. DE schließt natürliche Personen als Opfer der Straftaten aus. FI fordert eine zusätzliche Bewertung der Straftat „als Ganzes“, IT setzt voraus, dass eine tatsächliche „Zerstörung“ verursacht wird, PT setzt einen „schwerwiegenden und dauerhaften“ Angriff voraus und nimmt nicht Bezug auf Artikel 5, und SE erfüllt die Anforderungen der Richtlinie nur für den Straftatbestand der „schweren Sabotage“.

gg) Identitätsdiebstahl und andere identitätsbezogene Straftaten

Nach Artikel 9 Absatz 5 müssen die Mitgliedstaaten sicherstellen, dass bei der Begehung von Straftaten im Sinne der Artikel 4 und 5 der Missbrauch der personenbezogenen Daten einer anderen Person mit dem Ziel, das Vertrauen eines Dritten zu gewinnen, wodurch dem rechtmäßigen Identitätseigentümer ein Schaden zugefügt wird, als erschwerender Umstand eingestuft werden kann, soweit der betreffende Umstand nicht bereits eine andere Straftat darstellt. Aufgrund des großen Handlungsspielraums haben die Mitgliedstaaten diese Bestimmung äußerst unterschiedlich umgesetzt. BE und EL haben keine Umsetzung mitgeteilt; das Strafgesetzbuch von CZ enthält keine entsprechende Bestimmung. Der Ansatz des „erschwerenden Umstands“ wurde von AT, CY, ES, IE, MT, PT und SE gewählt (wobei in SE der erschwerende Umstand eine „besondere Planung“ voraussetzt). Alle anderen Mitgliedstaaten verweisen auf für diesen Straftatbestand geltende Zusatzbestimmungen. Bei den Mitgliedstaaten, die auf spezifische Zusatzbestimmungen verweisen, sind folgende Umsetzungsprobleme festzustellen: BG und NL setzen eine besondere Absicht voraus („Verschaffung eines Vorteils“ und „das Ziel, die Identität zu verschleiern oder zu missbrauchen“); DE hat lediglich „personenbezogene Daten, die nicht allgemein zugänglich sind“ einbezogen; FR nimmt nur auf den Namen einer Person und nicht auf andere personenbezogene Daten Bezug; LV setzt voraus, dass ein „erheblicher Schaden“ entstanden

ist; RO nimmt nur auf die Verwendung „eines Dokuments“ Bezug und setzt eine Betrugsabsicht voraus.

d) Verantwortlichkeit juristischer Personen

aa) Im Allgemeinen

Artikel 10 Absatz 1 bestimmt, dass juristische Personen für Straftaten im Sinne der Artikel 3 bis 8 verantwortlich gemacht werden können, wenn der Straftäter a) eine Befugnis zur Vertretung der juristischen Person, b) eine Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder c) eine Kontrollbefugnis innerhalb der juristischen Person hat. Alle Mitgliedstaaten haben Rechtsvorschriften erlassen, die mit diesem Artikel übereinstimmen, wobei nur die folgenden geringfügigen Probleme festzustellen sind: BG deckt nicht die Straftat im Sinne des Artikels 6 ab, und HR nimmt nicht Bezug auf einen Straftäter, der eine Kontrollbefugnis innerhalb der juristischen Person hat (Artikel 10 Absatz 1 Buchstabe c).

bb) Wegen mangelnder Überwachung oder Kontrolle

Nach Artikel 10 Absatz 2 müssen die Mitgliedstaaten sicherstellen, dass juristische Personen verantwortlich gemacht werden können, wenn mangelnde Überwachung oder Kontrolle seitens einer in Artikel 10 Absatz 1 genannten Personen die Begehung einer Straftat nach den Artikeln 3 bis 8 ermöglicht hat. Fast alle Mitgliedstaaten haben diese Bestimmung umgesetzt; LU hat keine aufschlussreichen Informationen übermittelt, und BG nimmt nicht auf eine Straftat im Sinne des Artikels 6 Bezug.

e) Sanktionen gegen juristische Personen

aa) Obligatorische Sanktionen

Nach Artikel 11 Absatz 1 der Richtlinie müssen die Mitgliedstaaten Geldstrafen oder Geldbußen als wirksame, verhältnismäßige und abschreckende Sanktionen für juristische Personen vorsehen. Außer IE und UK haben alle Mitgliedstaaten die Umsetzung entsprechender nationaler Maßnahmen mitgeteilt. In IE und UK bleibt der Höchstbetrag möglicher Geldstrafen oder Geldbußen unbestimmt, da hinreichend konkrete Rechtsvorschriften fehlen. Aus diesem Grund kann weder die Wirksamkeit noch die Verhältnismäßigkeit noch die abschreckende Wirkung dieser Geldstrafen oder Geldbußen beurteilt werden.

bb) Fakultative Sanktionen

In Artikel 11 Absatz 1 sind ferner mögliche zusätzliche Sanktionen gegen juristische Personen aufgeführt. Dazu gehören: Ausschluss von öffentlichen Zuwendungen oder Hilfen (CY, CZ, EL, ES, HR, HU, LU, MT, PL, PT und SK), vorübergehendes oder ständiges Verbot der Ausübung einer Handelstätigkeit (AT, BE, CY, CZ, EL, ES, FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI und SK), richterliche Aufsicht (CY, ES, FR, MT, PT und RO), richterlich angeordnete Eröffnung des Liquidationsverfahrens (CY, CZ, EL, ES, FR, HR, HU, LT, LU, LV, MT, PT, RO, SI und SK) und vorübergehende oder endgültige Schließung von Einrichtungen, die zur Begehung der Straftat genutzt wurden (BE, CY, WS, FR, LT, MT, PT und RO). Demnach haben BG, DE, EE, IE, FI, NL und UK von keiner der Optionen Gebrauch gemacht.

cc) Sanktionen wegen Unterlassung

Nach Artikel 11 Absatz 2 müssen die Mitgliedstaaten sicherstellen, dass wirksame, angemessene und abschreckende Sanktionen gegen juristische Personen verhängt werden können, die für Unterlassungen im Sinne des Artikels 10 Absatz 2 verantwortlich sind. LU hat keine aufschlussreichen Informationen übermittelt. Außer IE und UK haben alle übrigen

Mitgliedstaaten entsprechende legislative Maßnahmen getroffen. Für IE und UK stellen sich dieselben Probleme wie in Bezug auf Artikel 11 Absatz 1 (siehe oben Abschnitt aa).

f) Gerichtliche Zuständigkeit

aa) Erforderliche Zuständigkeitskriterien

Nach Artikel 12 Absätze 2 und 3 der Richtlinie müssen die Mitgliedstaaten ihre Zuständigkeit für die in den Artikeln 3 bis 8 genannten Straftaten begründen, wenn diese Straftaten ganz oder teilweise in ihrem Hoheitsgebiet begangen wurden – sei es, dass sich der Täter bei der Begehung der Straftat physisch in ihrem Hoheitsgebiet aufgehalten hat oder dass die Straftat gegen ein Informationssystem in ihrem Hoheitsgebiet gerichtet war – oder wenn die Straftaten von einem ihrer Staatsangehörigen im Ausland begangen wurden. Die meisten Mitgliedstaaten haben entsprechende nationale Rechtsvorschriften erlassen. IT begründet in seinen Rechtsvorschriften keine Zuständigkeit für Staatsangehörige, die im Ausland Grunddelikte begehen, die Rechtsvorschriften von LV und SI verweisen auf unklare Bestimmungen hinsichtlich hoheitsgebietlicher Aspekte, die Frage der gerichtlichen Zuständigkeit von MT für teilweise in seinem Hoheitsgebiet begangene Straftaten ist unklar, und UK nimmt Bezug auf ein Computersystem anstatt auf ein Informationssystem.

bb) Sonstige Zuständigkeitskriterien

Nach Artikel 12 Absatz 3 unterrichten die Mitgliedstaaten die Kommission über die Begründung einer gerichtlichen Zuständigkeit in Fällen, in denen der gewöhnliche Aufenthalt des Straftäters in ihrem Hoheitsgebiet liegt (AT, CY, CZ, IE, FI, HR, LT, LV, NL, SE und SK) oder die Straftat zugunsten einer in seinem Hoheitsgebiet niedergelassenen juristischen Person begangen wird (CY, CZ, LV, PT, RO und SK).

2.4 Operative Angelegenheiten (Artikel 13 und 14 der Richtlinie)

a) Bestimmung zu operativen nationalen Kontaktstellen

Nach Artikel 13 Absatz 1 müssen die Mitgliedstaaten zum Zweck des Informationsaustauschs über Straftaten im Sinne der Artikel 3 bis 8 operative nationale Kontaktstellen einrichten. Auf Grundlage dieser Bestimmung müssen die Mitgliedstaaten sicherstellen, dass Verfahren vorhanden sind, die es der zuständigen Behörde ermöglichen, innerhalb von 8 Stunden nach Eingang eines dringenden Ersuchens um Unterstützung zu antworten. Den mitgeteilten Informationen zufolge haben die meisten Mitgliedstaaten die erforderliche Infrastruktur aufgebaut. IE und RO erklären, dass die betreffenden Kontaktstellen nur für eine begrenzte Zahl von Stunden pro Tag zur Verfügung stehen, was es der Behörde nicht ermöglichen würde, in jedem möglichen Fall innerhalb von 8 Stunden nach Eingang eines Ersuchens zu reagieren. Mehrere Mitgliedstaaten haben darauf hingewiesen, dass sie bestehende Netze operativer Kontaktstellen nutzen, die über das G7-Netzwerk oder nach dem Budapester Übereinkommen des Europarats über Computerkriminalität errichtet wurden.

b) Informationen über die errichteten operativen nationalen Kontaktstellen

Nach Artikel 13 Absatz 2 müssen die Mitgliedstaaten der Kommission die Kontaktdaten ihrer Kontaktstellen mitteilen, die diese Angaben dann an die anderen Mitgliedstaaten weiterleitet. Alle Mitgliedstaaten haben die erforderlichen Informationen übermittelt.

c) Meldekanäle

Nach Artikel 13 Absatz 3 müssen die Mitgliedstaaten sicherstellen, dass geeignete Meldekanäle zur Verfügung stehen, damit die Meldung der in den Artikeln 3 bis 6 aufgeführten Straftaten an die zuständigen nationalen Behörden erfolgen kann. HR, IT, IE und PT haben keine aufschlussreichen Informationen übermittelt. Die übrigen Mitgliedstaaten haben offensichtlich unterschiedliche Ansätze für die Umsetzung der Anforderungen an die

Meldekanäle gewählt. Die meisten Mitgliedstaaten (BE, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK und UK) haben Maßnahmen zur Bereitstellung von Kanälen mitgeteilt, die die erste Meldung einer Straftat durch eine Person oder Organisation, die Opfer eines Cyberangriffs geworden ist, erleichtern (wobei die tatsächlichen Meldekanäle von LV weiter unklar sind). Andere Mitgliedstaaten (AT, ES und LU) haben jedoch Informationen übermittelt, die mit denen zur Umsetzung von Artikel 13 Absätze 1 und 2 identisch sind, was darauf hindeutet, dass die getroffenen Maßnahmen hauptsächlich die Kommunikation zwischen Behörden erleichtern werden.

d) Erhebung statistischer Daten
Nach Artikel 14 Absätze 1 und 2 müssen die Mitgliedstaaten sicherstellen, dass ein System für die Aufzeichnung, Erstellung und Bereitstellung statistischer Daten (die zumindest Daten über die Zahl der in den Mitgliedstaaten erfassten Straftaten im Sinne der Artikel 3 bis 7 und über die Zahl der Personen, die wegen einer Straftat im Sinne der Artikel 3 bis 7 verfolgt und verurteilt worden sind, umfassen müssen) bereitsteht. Den eingegangenen Mitteilungen zufolge haben die meisten Mitgliedstaaten sowohl legislative als auch administrative Maßnahmen getroffen, um die Erhebung der Informationen sicherzustellen – in der Regel auf der Grundlage eines allgemeinen nationalen elektronischen Systems. Eine Reihe von Mitgliedstaaten hat keine aufschlussreichen Informationen übermittelt (EL, IE, UK (Gibraltar, Nordirland und Schottland)). Ein Grund dafür ist, dass die Informationen über die Straftaten im Sinne der Richtlinie unter Umständen nicht separat erhoben werden (BE, DE und SE) oder dass die erhobenen Informationen nicht alle in der Richtlinie genannten Straftaten umfassen (RO).

e) Übermittlung der statistischen Daten an die Kommission
Nach Artikel 14 Absatz 3 müssen die Mitgliedstaaten die entsprechenden statistischen Daten der Kommission übermitteln. Alle Mitgliedstaaten, die Maßnahmen mitgeteilt haben (außer UK (Gibraltar, Nordirland und Schottland) und HU), haben die Umsetzung legislativer oder/und administrativer Maßnahmen bestätigt, um dieser Verpflichtung nachzukommen. EL, ES, LU und SI haben keine aufschlussreichen Informationen übermittelt.

3. Schlussfolgerung und nächste Schritte

Die Richtlinie hat erhebliche Fortschritte bei der Angleichung der Einstufung von Cyberangriffen als Straftaten in den Mitgliedstaaten bewirkt, wodurch eine grenzüberschreitende Zusammenarbeit der Strafverfolgungsbehörden, die diese Art von Straftaten untersuchen, ermöglicht wird. Die Mitgliedstaaten haben Strafgesetzbücher und andere einschlägige Rechtsvorschriften geändert, Verfahren gestrafft und Regelungen für die Zusammenarbeit eingeführt oder verbessert. Die Kommission erkennt die erheblichen Anstrengungen der Mitgliedstaaten zur Umsetzung der Richtlinie an.

Es besteht allerdings noch beträchtlicher Spielraum, um das Potenzial der Richtlinie durch vollständige Umsetzung aller Bestimmungen durch die Mitgliedstaaten voll auszuschöpfen. Die Analyse hat bisher gezeigt, dass zu den wichtigsten Verbesserungen, die die Mitgliedstaaten erzielen müssen, die Anwendung der Begriffsbestimmungen (Artikel 2) zählt, die Auswirkungen auf den Anwendungsbereich der Straftaten hat, die im nationalen Recht auf der Grundlage der Richtlinie definiert werden. Darüber hinaus hatten die Mitgliedstaaten offensichtlich Probleme, bei der Definition der als Straftat zu wertenden Handlungen alle Möglichkeiten einzubeziehen (Artikel 3 bis 7) und die gemeinsamen Standards für das Strafmaß für Cyberangriffe zu berücksichtigen (Artikel 9). Andere Probleme scheinen bei der Umsetzung der administrativen Bestimmungen zu den geeigneten Meldekanälen (Artikel 13

Absatz 3) und in Sachen Kontrolle und Statistiken in Bezug auf die in der Richtlinie genannten Straftaten zu bestehen (Artikel 14).

Die Kommission wird die Mitgliedstaaten auch weiterhin bei der Umsetzung der Richtlinie unterstützen. Angesichts des potenziellen Beitrags zur grenzüberschreitenden Zusammenarbeit betrifft dies insbesondere die operativen Bestimmungen der Richtlinie zum Informationsaustausch (Artikel 13 Absätze 1 und 2), zu den Meldekanälen (Artikel 13 Absatz 3) und zu Kontrolle und Statistiken (Artikel 14). Zu diesem Zweck wird die Kommission den Mitgliedstaaten im zweiten Halbjahr 2017 weiter Gelegenheit geben, bewährte Verfahren zu ermitteln und auszutauschen.

Die Kommission sieht es derzeit nicht als notwendig an, Änderungen zu der Richtlinie vorzuschlagen. In diesem Zusammenhang und auch zur Unterstützung strafrechtlicher Ermittlungen im Falle von Angriffen auf Informationssysteme sowie von durch den Cyberspace ermöglichten und anderen Arten von Straftaten prüft die Kommission zurzeit Maßnahmen zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln für strafrechtliche Ermittlungen, darunter auch ein Vorschlag für legislative Maßnahmen, der Anfang 2018 vorgelegt werden soll.[8] Die Kommission beschäftigt sich auch mit der Rolle der Verschlüsselung bei strafrechtlichen Ermittlungen und wird im Oktober 2017 über ihre Erkenntnisse Bericht erstatten.[9]

Die Kommission ist bestrebt zu gewährleisten, dass die Umsetzung der Richtlinie in allen Mitgliedstaaten abgeschlossen wird und ihre Bestimmungen korrekt umgesetzt werden. Dies schließt die Kontrolle der Vereinbarkeit der nationalen Maßnahmen mit den entsprechenden Bestimmungen der Richtlinie ein. Gegebenenfalls wird die Kommission von den ihr aus den Verträgen erwachsenden Durchsetzungsbefugnissen Gebrauch machen, indem sie Vertragsverletzungsverfahren einleitet.

[8] Folgenabschätzung in der Anfangsphase zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln vom 4. August 2017, abrufbar unter: ec.europa.eu.

[9] *Communication on the Eighth progress report towards an effective and genuine Security Union* (COM(2017) 354 final).