RAT DER EUROPÄISCHEN UNION

Brüssel, den 30. Mai 2011 (06.06)
(OR. en)

10751/11

Interinstitutionelles Dossier: 2010/0273 (COD)

DROIPEN 47
TELECOM 82
CODEC 915

VERMERK

des	Vorsitzes
für den	AStV / Rat
Nr. Vordok.:	10357/11 DROIPEN 42 TELECOM 74 CODEC 851
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates – Allgemeine Ausrichtung

I. HINTERGRUNDINFORMATIONEN

Die Kommission hat dem Europäischen Parlament und dem Rat am 30. September 2010 einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates unterbreitet.

Gemäß Artikel 3 Absatz 1 des den Verträgen beigefügten Protokolls (Nr. 21) haben das Vereinigte Königreich und Irland dem Rat mitgeteilt, dass sie sich an der Annahme und Anwendung der Richtlinie beteiligen wollen. Gemäß dem den Verträgen beigefügten Protokoll (Nr. 22) beteiligt sich Dänemark nicht an der Annahme dieses Gesetzgebungsakts.

UK und FR haben einen Parlamentsvorbehalt eingelegt. DE, SI, FR und SE haben einen allgemeinen Prüfungsvorbehalt eingelegt.

Der Vorschlag wurde dem Rat auf seiner Tagung vom 8./9. November 2010 vorgelegt.

Der Koordinierungsausschuss für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (CATS) wurde in drei seiner Sitzungen um strategische Vorgaben für die Beratungen in der Gruppe "Materielles Strafrecht" ersucht. Am 13. Dezember 2010, zu Beginn der Verhandlungen, gab der CATS allgemeine Leitlinien für die künftigen Beratungen vor. Am 11. Februar 2011 prüfte der CATS Artikel 10 Absatz 3 des Kommissionsvorschlags, mit dem ein neuer erschwerender Umstand bei Angriffen auf Informationssysteme eingeführt wird, nämlich der Umstand, dass sie unter Verschleierung der wahren Identität des rechtmäßigen Identitätseigentümers begangen wurden. Am 22. März 2011 schließlich wurde der CATS zu vier noch offenen Fragen konsultiert: Anwendungsbereich der Bestimmungen, mit denen leichte Fälle ausgenommen werden, Tatbestandsmerkmale der Straftat nach Artikel 3, Strafmaß und gerichtliche Zuständigkeit auf der Grundlage der Staatsangehörigkeit.

Die Gruppe "Materielles Strafrecht" hat den Vorschlag in ihren Sitzungen vom 13./14. und 28. Januar 2011 sowie vom 2./3. und 29. März 2011 erörtert. Am 29. März 2011 hat sie eine dritte Lesung des Textes abgeschlossen.

Der Rat hat am 25. Februar 2011 Kenntnis vom Stand der Erörterungen genommen. Am 12. April 2011 hat der Rat Kenntnis von der vorläufigen Einigung über die Artikel 1 bis 6 und die Artikel 11 bis 19 des Richtlinienentwurfs genommen. Außerdem gab er Leitlinien zu mehreren noch offenen Fragen vor und legte so den politischen Rahmen für die weiteren Beratungen über den Vorschlag, die in den Vorbereitungsgremien des Rates geführt werden, fest.

II. VORSCHLAG FÜR EIN KOMPROMISSPAKET

Der Text in der Anlage stellt einen Kompromissvorschlag dar, wie er sich aus den Sitzungen der JI-Referenten vom 13. Mai 2011 und der Freunde des Vorsitzes vom 24. Mai 2011 ergibt.

Im Verlauf der Beratungen wurde der ursprüngliche Kommissionsvorschlag mehrfach angepasst, um den Standpunkten der Delegationen so weit wie möglich Rechnung zu tragen. Der Vorsitz war ferner bestrebt, den Gründen, die dem Kommissionsvorschlag zugrunde liegen, nämlich für effizientere strafrechtliche Maßnahmen auf EU-Ebene gegen die neuen Bedrohungen der Cyberkriminalität, wie beispielsweise breit angelegte Cyberangriffe, zu sorgen, gleichermaßen Rechnung zu tragen.

A. Diesbezüglich möchte der Vorsitz die Hauptbestandteile des Kompromisspakets in Erinnerung rufen, die der Rat auf seiner Tagung vom 12. April 2011 vorläufig gebilligt hat.

1. Strafbarkeit (Artikel 3-7)

- Die Bezugnahme auf "leichte Fälle" wurde auf alle in der Richtlinie aufgeführten Straftatbestände (Artikel 3 bis Artikel 7) ausgeweitet. Leichte Fälle werden daher vollständig vom Geltungsbereich der Richtlinie ausgenommen. Ob ein leichter Fall vorliegt oder nicht, wird nach einzelstaatlichem Recht oder nach einzelstaatlicher Praxis (siehe Erwägungsgrund 6a) festgelegt, wobei ferner entsprechende Beispiele aufgeführt werden.
- Der Geltungsbereich des Artikels 3 "Rechtswidriger Zugang zu Informationssystemen" wurde auf Fälle beschränkt, in denen der Verstoß gegen eine Sicherheitsmaßnahme ein Tatbestandsmerkmal ist. Das Übereinkommen von Budapest sieht diese Möglichkeit als Option vor, sie wurde jedoch nicht in den ursprünglichen Kommissionsvorschlag aufgenommen.
- Der Besitz von Instrumenten, die zu Angriffen auf Informationssysteme verwendet werden, wurde vom Geltungsbereich des Artikels 7 ausgenommen.
- Die Strafbarkeit des Versuchs wurde auf die in den Artikeln 4 und 5 genannten Straftaten begrenzt.

2. Sanktionen (Artikel 9)

- Der Vorschlag der Kommission betreffend das Strafmaß für Grundtatbestände (siehe Artikel 9 Absatz 2), d.h. Freiheitsstrafen im Höchstmaß von mindestens zwei Jahren, wird beibehalten. Der Grund hierfür liegt insbesondere in der begrenzten Strafbarkeit, wie sie sich aus den Beratungen in den Vorbereitungsgremien des Rates ergibt. Der Geltungsbereich der Vorschrift wurde weiter beschränkt, und zwar auf die Artikel 3 bis 6, während für Artikel 7 mithin nicht mehr die Verpflichtung gilt, dieses spezifische Strafmaß vorzusehen.
- Der Kompromissvorschlag sieht ein größeres Maß an Flexibilität in Bezug auf die Sanktionen bei Vorliegen erschwerender Umstände vor: Freiheitsstrafen im Höchstmaß von mindestens drei bzw. fünf Jahren (Artikel 9 Absatz 3 bzw. Artikel 9 Absatz 4), um die Schwere der Straftaten zu berücksichtigen, wobei die Anwendung der Bestimmungen außerdem kompromisshalber auf die Artikel 4 und 5 beschränkt wurde.

3. Gerichtliche Zuständigkeit (Artikel 13)

- Die Begründung der gerichtlichen Zuständigkeit für eigene Staatsangehörige wird mit einer positiven doppelten Strafbarkeitsüberprüfung verknüpft (Artikel 13 Absatz 1 Buchstabe b).
- Die Voraussetzungen für die Ausübung der einzelstaatlichen gerichtlichen Zuständigkeit sind nicht Gegenstand der Richtlinie (siehe Präambel, Erwägungsgrund 10a).

4. Informationsaustausch über Straftaten im Richtlinienentwurf (Artikel 14)

- Die Frist von acht Stunden für die Beantwortung dringender Ersuchen wird beibehalten; allerdings wurde der Text geändert, um klarzustellen, wozu der ersuchte Staat verpflichtet ist, nämlich dass die zuständige Behörde binnen der festgesetzten Frist zumindest mitteilen muss, ob sie in der Lage ist, eine Antwort zu erteilen, und dass sie – wenn dies der Fall ist – zudem einige vorläufige Details zur voraussichtlichen Antwort angeben muss, etwa in welcher Form und wann diese Antwort wahrscheinlich erfolgen wird.

B. Die Arbeit an dem Vorschlag wurde im Lichte der vom Rat am 12. April 2011 vorgegeben politischen Leitlinien fortgesetzt. Daher sollten auch die folgenden neuen Bestandteile in dem Gesamtkompromisspaket geprüft werden:

1. Tatwerkzeuge – Artikel 7

- Der Anwendungsbereich des Artikels 7 wurde weiter eingeschränkt. Daher wurde auch das Herstellen oder Verfügbarmachen jener Vorrichtungen, die zur Durchführung von Cyberangriffen benutzt werden könnten, ebenfalls vom Anwendungsbereich des Vorschlags ausgenommen.
- In der Richtlinie ist der in Artikel 7 genannte Begriff "Instrument" eng gefasst, im Unterschied zu seiner Verwendung im Kommissionsvorschlag, wo der Begriff weiter ausgelegt wurde und z.B. spezielle Hardware als Instrument zur Durchführung von Cyberangriffen umfasste.

2. Erschwerende Umstände bei breit angelegten Cyberangriffen – Artikel 9

- Der Kernbestandteil des Kommissionsvorschlags, der breit angelegte Cyberangriffe als erschwerenden Umstand behandelt, wurde, wenn auch in wesentlich geänderter Fassung, beibehalten. Es ist hervorzuheben, dass bei breit angelegten Cyberangriffen nach zwei alternativen kennzeichnenden Aspekten unterschieden wird – Angriffe, die auf eine große Anzahl von Informationssystemen gerichtet sind, bzw. Angriffe, die schweren Schaden verursachen. Diese beiden Aspekte werden in Artikel 9 Absatz 3 bzw. Artikel 9 Absatz 4 Buchstabe b behandelt.

- Um den Bedenken mehrerer Delegationen Rechnung zu tragen, die das Erfordernis betreffen, eine klare Verknüpfung zu den derzeitigen Bedrohungen herzustellen, die von den Methoden ausgehen, die Kriminelle zur Durchführung von breit angelegten Cyberangriffen verwenden, wie beispielsweise die Schaffung und Verwendung von "Botnetzen"[1], wurden entsprechende Formulierungen in die Erwägungsgründe des Vorschlags aufgenommen (siehe Erwägungsgründe 3 und 7). Der Vorsitz hat diesen Ansatz gewählt, damit Flexibilität und technische Neutralität, soweit die zur Durchführung breit angelegter Cyberangriffe verwendeten Methoden betroffen sind, im verfügenden Teil der Richtlinie beibehalten werden. Letzteres ist insofern von besonderer Relevanz, als die technologische Entwicklung immer weiter voranschreitet und diese Kriminalitätsart sich stets weiterentwickelt.

- Im Interesse eines Kompromisses wurde Artikel 9 Absatz 5 betreffend die missbräuchliche Verwendung personenbezogener Daten einer anderen Person, um das Vertrauen eines Dritten zwecks erleichterter Durchführung von Cyberangriffen zu gewinnen, gestrichen. Dies geschah aufgrund der von einigen Delegationen beständig vorgetragenen Ansicht, dass dieses Phänomen in einem spezifischen Rechtsinstrument über die Bekämpfung des Identitätsdiebstahls umfassend behandelt werden sollte.

---

[1] Die Verwendung sogenannter "Botnetze" ist dadurch gekennzeichnet, dass die strafbare Handlung in aufeinander folgenden Stufen erfolgt, wobei jede Stufe für sich eine erhebliche Gefahr für die öffentlichen Interessen darstellen kann. Diesbezüglich zielt die Richtlinie unter anderem darauf ab, strafrechtliche Sanktionen hinsichtlich der Stufe einzuführen, in der das "Botnetz" geschaffen wird, nämlich wenn eine ferngesteuerte Kontrolle über eine bedeutende Anzahl von Computern hergestellt wird, indem diese durch gezielte Cyberangriffe mit Schadsoftware infiziert werden. Auf einer späteren Stufe kann das infizierte Netz von Computern, die das "Botnetz" bilden, ohne Wissen der Computerbenutzer aktiviert werden, um breit angelegte Cyberangriffe zu starten, die gewöhnlich die Fähigkeit haben, erheblichen Schaden anzurichten, wie er in dieser Richtlinie beschrieben wird.

3. Gerichtliche Zuständigkeit (Erwägungsgrund 10a)

- Im überarbeiteten Wortlaut des Erwägungsgrunds 10a wird eine klare Unterscheidung zwischen den Bedingungen für die Begründung der Zuständigkeit nach Artikel 13 und den Bedingungen für die Ausübung der Zuständigkeit vorgenommen.

Der AStV wird ersucht,
a) die neuen Elemente des Kompromisses als integralen Bestandteil des Vorschlags für ein Gesamtkompromisspaket zu prüfen und
b) zu bestätigen, dass der Text in der Fassung der Anlage dem Rat im Hinblick auf die Festlegung einer allgemeinen Ausrichtung zu dem Vorschlag unterbreitet werden sollte, damit der beigefügte Text als Grundlage für die künftigen Beratungen mit dem Europäischen Parlament gemäß Artikel 294 AEUV dienen kann.

ANLAGE

2010/0273 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 83 Absatz 1,
auf Vorschlag der Europäischen Kommission[2],
nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,
nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses,
nach Stellungnahme des Ausschusses der Regionen,
gemäß dem ordentlichen Gesetzgebungsverfahren,
in Erwägung nachstehender Gründe:

(1) Ziel dieser Richtlinie ist die Angleichung der einzelstaatlichen Strafvorschriften für Angriffe auf Informationssysteme, indem Mindestvorschriften für die Definition von Straftaten und für die Sanktionen bei Angriffen auf Informationssysteme festgelegt werden, sowie die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden einschließlich der Polizei und anderer spezialisierter Strafverfolgungsbehörden der Mitgliedstaaten.

(2) Angriffe auf Informationssysteme – insbesondere im Rahmen der organisierten Kriminalität – werden zunehmend zu einer Bedrohung, und es wächst die Besorgnis über mögliche Terroranschläge oder politisch motivierte Attacken auf Informationssysteme, die Teil der kritischen Infrastruktur der Mitgliedstaaten und der Union sind. Hierdurch wird das Ziel einer sichereren Informationsgesellschaft und eines Raums der Freiheit, der Sicherheit und des Rechts gefährdet, so dass Gegenmaßnahmen auf Ebene der Europäischen Union erforderlich sind.

[2] ABl. C […] vom […], S. […].

(2a) Es gibt in der Union eine Reihe wichtiger Infrastrukturen, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen hätte. Da die Fähigkeit zum Schutz kritischer Infrastrukturen in ganz Europa verbessert werden muss, sollte die Bekämpfung von Angriffen auf Informationssysteme durch schwere strafrechtliche Sanktionen, die der Schwere derartiger Angriffe Rechnung tragen, ergänzt werden. Als kritische Infrastrukturen sind in einem Mitgliedstaat gelegene Anlagen, Systeme oder Teile derselben zu verstehen, die beispielsweise von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten.

(3) Es besteht eine Tendenz zu immer gefährlicheren und häufigeren Großangriffen auf Informationssysteme, die für den Staat oder für bestimmte Funktionen im öffentlichen oder privaten Sektor oft unverzichtbar sein können. Diese Tendenz geht einher mit der Entwicklung immer ausgefeilterer (…) Methoden, wie etwa der Schaffung und Verwendung von sogenannten "Botnetzen". Bei letzterer erfolgt die kriminelle Handlung in aufeinander folgenden Stufen, wobei jede Stufe für sich eine ernsthafte Gefahr für die öffentlichen Interessen darstellen kann. Diesbezüglich zielt die Richtlinie unter anderem darauf ab, strafrechtliche Sanktionen hinsichtlich der Stufe einzuführen, in der das "Botnetz" geschaffen wird, nämlich wenn eine ferngesteuerte Kontrolle über eine bedeutende Anzahl von Computern hergestellt wird, indem diese durch gezielte Cyberangriffe mit Schadsoftware infiziert werden. Auf einer späteren Stufe kann das infizierte Netz von Computern, die das "Botnetz" bilden, ohne Wissen der Computerbenutzer aktiviert werden, um breit angelegte Cyberangriffe zu starten, die gewöhnlich die Fähigkeit haben, erheblichen Schaden anzurichten, wie er in dieser Richtlinie beschrieben wird. Die Mitgliedstaaten können festlegen, was gemäß ihrem nationalen Recht und ihrer nationalen Praxis als erheblicher Schaden gilt; dazu können gestörte Systemdienste von erheblicher öffentlicher Bedeutung oder größere finanzielle Kosten oder der Verlust personenbezogener Daten gehören.

(4) Für eine einheitliche Strategie in den Mitgliedstaaten bei der Anwendung dieser Richtlinie sind gemeinsame Definitionen in diesem Bereich und insbesondere Definitionen von Informationssystemen und Computerdaten wichtig.

(5) Es sollten gemeinsame Straftatbestände für den rechtswidrigen Zugang zu Informationssystemen, den rechtswidrigen Systemeingriff, den rechtswidrigen Eingriff in Daten und das rechtswidrige Abfangen von Daten festgelegt werden, wozu es einer Einigung über die Tatbestandsmerkmale bedarf.

(6) Angriffe auf Informationssysteme sollten von den Mitgliedstaaten unter Strafe gestellt werden. Die Sanktionen sollten wirksam, verhältnismäßig und abschreckend sein.

(6a) Diese Richtlinie sieht zumindest dann strafrechtliche Sanktionen vor, wenn kein leichter Fall vorliegt. Die Mitgliedstaaten können festlegen, was gemäß ihrem einzelstaatlichen Recht und ihrer einzelstaatlichen Praxis als leichter Fall gilt. Ein Fall kann beispielsweise dann als leicht eingestuft werden, wenn der damit verbundene Schaden und/oder die damit verbundene Gefahr für öffentliche oder private Interessen, wie etwa die Integrität eines Computersystems oder von Computerdaten oder die Integrität, die Rechte und andere Interessen einer Person geringfügig oder so geartet ist, dass die die Verhängung einer strafrechtlichen Sanktion innerhalb der gesetzlichen Grenzen oder die Begründung einer strafrechtlichen Verantwortung nicht notwendig ist.

(7) Schwerere Strafen sollten vorgesehen werden bei Angriffen auf ein Informationssystem, die von einer kriminellen Vereinigung im Sinne des Rahmenbeschlusses 2008/841/JI des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität[3] verübt werden, oder bei groß angelegten Angriffen, bei denen eine beträchtliche Anzahl von Informationssystemen geschädigt wird oder mit denen schwere Schäden verursacht werden, einschließlich in Fällen, in denen der Angriff dazu diente, ein "Botnetz" zu schaffen, oder mittels eines "Botnetzes" durchgeführt wurde und so zu schweren Schäden führte (...).

(8) In den Schlussfolgerungen des Rates vom 27./28. November 2008 wurde die Ausarbeitung einer neuen Strategie in Zusammenarbeit mit den Mitgliedstaaten und der Kommission angekündigt, in die auch das Übereinkommen des Europarats über Computerkriminalität aus dem Jahr 2001 einfließen soll. Dieses Übereinkommen ist der rechtliche Bezugsrahmen für die Bekämpfung der Cyberkriminalität und damit auch der Angriffe auf Informationssysteme. Die vorliegende Richtlinie baut auf dem Übereinkommen auf.

(9) Angesichts der unterschiedlichen Art und Weise, wie Cyberangriffe ausgeführt werden können, und der raschen Entwicklung bei der Hard- und Software ist in dieser Richtlinie die Rede von "Instrumenten", die zur Begehung der in dieser Richtlinie aufgeführten Straftaten verwendet werden können. Bei solchen Instrumenten kann es sich beispielsweise um Schadsoftware einschließlich jener handeln, mit der Botnetze geschaffen werden können, die für Cyberangriffe verwendet werden. Da mit dieser Richtlinie Mindestvorschriften festgelegt werden, können die Mitgliedstaaten strafrechtliche Sanktionen für Straftaten anderer Art in Bezug auf Instrumente, die zur Begehung von Straftaten verwendet werden, vorsehen, wie etwa der Besitz derartiger Instrumente oder das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen aller anderen Vorrichtungen, einschließlich Hardware, die in erster Linie dafür ausgelegt oder hergerichtet wurden, eine Straftat im Sinne dieser Richtlinie zu begehen.

---

[3] ABl L 300 vom 11.11.2008, S. 42.

(10) Mit dieser Richtlinie soll keine strafrechtliche Haftung in Fällen begründet werden, in denen die Handlungen ohne kriminelle Absicht, beispielsweise zum genehmigten Testen oder zum Schutz eines Informationssystems, vorgenommen werden, oder wenn die betreffende Person nicht wusste, dass sie kein Zugangsrecht hatte.

(10a) Diese Richtlinie enthält keine Bestimmungen über die Voraussetzungen, die erfüllt sein sollten, damit die Gerichtsbarkeit über die in den Artikeln 3 bis 8 genannten Straftaten ausgeübt werden kann, wie etwa eine am Tatort erstattete Anzeige des Opfers oder eine Anzeige des Staates, in dem sich der Tatort befindet, oder die Tatsache, dass der Täter am Tatort nicht verfolgt wurde.

(11) Diese Richtlinie stärkt die Rolle von Netzwerken wie des G8-Netzes oder des Netzes der Kontaktstellen des Europarats, die an sieben Wochentagen 24 Stunden täglich für den Informationsaustausch zur Verfügung stehen, um verfügbare einschlägige Informationen für Ermittlungen und Verfahren wegen Straftaten im Zusammenhang mit Informationssystemen und -daten, die den ersuchenden Mitgliedstaat betreffen, bereitstellen zu können. Angesichts der Schnelligkeit, mit der Großangriffe ausgeführt werden können, sollten die Mitgliedstaaten in der Lage sein, prompt auf dringende Ersuchen dieser Kontaktstellen um Unterstützung zu reagieren. In diesen Fällen kann es zweckmäßig sein, dass neben dem Informationsersuchen auch telefonisch Kontakt aufgenommen wird, um dafür zu sorgen, dass der ersuchte Staat das Ersuchen zügig bearbeitet und dass innerhalb der Frist von acht Stunden eine Rückmeldung erfolgt, mit der der Eingang des Ersuchens bestätigt und zugleich mitgeteilt wird, ob es beantwortet wird und wann mit Antwort zu rechnen ist.

(12) Um sich ein vollständigeres Bild von der Problematik auf Ebene der Union machen und auf diese Weise zur Gestaltung effizienterer Lösungen beitragen zu können, müssen Daten über Straftaten, die unter diese Richtlinie fallen, erfasst werden. Diese Daten werden auch Agenturen wie Europol oder der Europäischen Agentur für Netz- und Informationssicherheit dabei helfen, das Ausmaß der Cyberkriminalität und den Stand der Netz- und Informationssicherheit in Europa besser einzuschätzen.

(13) Größere Abweichungen und Diskrepanzen zwischen den einschlägigen Rechtsvorschriften der Mitgliedstaaten können die Bekämpfung der organisierten Kriminalität und des Terrorismus behindern und unter Umständen eine wirksame polizeiliche und justizielle Zusammenarbeit bei der Abwehr von Angriffen auf Informationssysteme erschweren. Der länder- und grenzübergreifende Charakter moderner Informationssysteme bedeutet, dass auch Angriffe auf solche Systeme eine grenzüberschreitende Dimension annehmen, was den dringenden Bedarf an weiteren Maßnahmen zur Angleichung der einschlägigen Strafvorschriften unterstreicht. Die Koordinierung der Strafverfolgung bei solchen Angriffen sollte mithilfe des Rahmenbeschlusses 2009/948/JI des Rates zur Vermeidung und Beilegung von Kompetenzkonflikten in Strafverfahren erleichtert werden.

(14) Da die Ziele dieser Richtlinie, nämlich Angriffe auf Informationssysteme in allen Mitgliedstaaten mit wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen Sanktionen zu ahnden und die justizielle Zusammenarbeit durch Beseitigung möglicher Hemmnisse zu verbessern und zu fördern, auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden können, sondern – da es dazu gemeinsamer, kompatibler Regeln bedarf – besser auf Unionsebene zu erreichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union niedergelegten Subsidiaritätsprinzip tätig werden. Diese Richtlinie geht nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.

(15) Alle im Zusammenhang mit der Anwendung dieser Richtlinie verarbeiteten Daten sollten nach Maßgabe des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden[4], soweit dieser Rahmenbeschluss einschlägig ist, und gemäß der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[5] geschützt werden.

---

4 ABl L 350 vom 30.12.2008, S. 60.
5 ABl L 8 vom 12.1.2001, S. 1.

(16) Diese Richtlinie steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden, namentlich der Schutz personenbezogener Daten, die Meinungs- und Informationsfreiheit, das Recht auf ein faires Verfahren, die Unschuldsvermutung und die Gewährleistung der Verteidigungsrechte sowie das Gesetzlichkeits- und Verhältnismäßigkeitsprinzip in Bezug auf Straftaten und Sanktionen. Diese Richtlinie, mit der die uneingeschränkte Wahrung dieser Rechte und Grundsätze gewährleistet werden soll, ist entsprechend umzusetzen.

(17) Gemäß Artikel (…) 3 (…) des Protokolls über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts im Anhang zum Vertrag über die Arbeitsweise der Europäischen Union haben das Vereinigte Königreich und Irland mitgeteilt, dass sie sich an der Annahme und Anwendung dieser Richtlinie beteiligen wollen.

(18) Gemäß den Artikeln 1 und 2 des dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Richtlinie, die daher für diesen Staat nicht verbindlich und ihm gegenüber nicht anwendbar ist.

(19) Mit dieser Richtlinie sollen die Bestimmungen des Rahmenbeschlusses 2005/222/JI geändert und ausgeweitet werden. Da die vorzunehmenden Änderungen sowohl bezüglich der Zahl als auch hinsichtlich des Inhalts erheblich sind, sollte der Rahmenbeschluss aus Gründen der Klarheit für die sich an der Annahme dieser Richtlinie beteiligenden Mitgliedstaaten vollständig ersetzt werden.

(20) Nach Nummer 34 der Interinstitutionellen Vereinbarung über bessere Rechtsetzung[6] sind die Mitgliedstaaten aufgefordert, für ihre eigenen Zwecke und im Interesse der Union eigene Tabellen aufzustellen, aus denen im Rahmen des Möglichen die Entsprechungen zwischen dieser Richtlinie und ihren Umsetzungsmaßnahmen zu entnehmen sind, und diese zu veröffentlichen –

---

[6] ABl. C 321 vom 31.12.2003, S. 1.

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1

Gegenstand

Mit dieser Richtlinie werden Mindestvorschriften für die Definition von Straftaten und für die Sanktionen bei Angriffen auf Informationssysteme festgelegt. Die Richtlinie soll überdies die Verhinderung derartiger Straftaten erleichtern und die Zusammenarbeit zwischen Justizbehörden und anderen zuständigen Behörden verbessern.

Artikel 2

Begriffsbestimmungen

Im Sinne dieser Richtlinie bezeichnet der Ausdruck

a) "Informationssystem" eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen Computerdaten;

b) "Computerdaten" jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann;

c) "juristische Person" jedes Rechtssubjekt, das diesen Status nach geltendem Recht besitzt, mit Ausnahme von Staaten oder anderen Körperschaften des öffentlichen Rechts in der Ausübung ihrer hoheitlichen Rechte und von öffentlich-rechtlichen internationalen Organisationen;

d) "unbefugt" einen Zugang, einen Eingriff, ein Abfangen von Daten oder jede andere in dieser Richtlinie genannte Handlung, die vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder eines Teils des Systems nicht gestattet wurde oder der nach den einzelstaatlichen Rechtsvorschriften nicht zulässig ist.

Artikel 3

Rechtswidriger Zugang zu Informationssystemen

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche unbefugte Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon zumindest dann unter Strafe gestellt wird, wenn er durch eine Verletzung von Sicherheitsmaßnahmen erfolgt und kein leichter Fall vorliegt.

Artikel 4

Rechtswidriger Systemeingriff

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die schwere Behinderung oder Störung des Betriebs eines Informationssystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten zumindest dann unter Strafe gestellt wird, wenn sie vorsätzlich und unbefugt erfolgt und kein leichter Fall vorliegt.

Artikel 5

Rechtswidriger Eingriff in Daten

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche unbefugte Löschen, Beschädigen, Beeinträchtigen, Verändern, Unterdrücken oder Unzugänglichmachen von Computerdaten eines Informationssystems zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 6

Rechtswidriges Abfangen von Daten

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche, mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Informationssystem, aus einem Informationssystem oder innerhalb eines Informationssystems einschließlich elektromagnetischer Abstrahlungen aus einem Informationssystem, das Träger solcher Computerdaten ist, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.

Artikel 7

Tatwerkzeuge

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche unbefugte Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen folgender Instrumente, die dazu bestimmt sind, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt:

a) eines Computerprogramms, das in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen;

b) eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon ermöglichen.

Artikel 8

Anstiftung, Beihilfe und Versuch

1. Die Mitgliedstaaten stellen sicher, dass die Anstiftung oder Beihilfe zur Begehung einer Straftat im Sinne der Artikel 3 bis 7 unter Strafe gestellt wird.

2. Die Mitgliedstaaten stellen sicher, dass der Versuch der Begehung einer Straftat im Sinne der Artikel 4 und 5 unter Strafe gestellt wird.

Artikel 9

Sanktionen

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten im Sinne der Artikel 3 bis 8 mit wirksamen, angemessenen und abschreckenden strafrechtlichen Sanktionen geahndet werden.

2. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 3 bis 6 mit Freiheitsstrafen im Höchstmaß von mindestens zwei Jahren geahndet werden.

3. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die Straftaten im Sinne der Artikel 4 und 5 bei vorsätzlicher Begehung mit Freiheitsstrafen im Höchstmaß von mindestens drei Jahren geahndet werden, wenn (…) eine beträchtliche Anzahl von Informationssystemen unter Verwendung eines in Artikel 7 Absatz 1 genannten Instruments, das in erster Linie dafür ausgelegt oder hergerichtet wurde, geschädigt wird[7].

4. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 4 und 5 mit Freiheitsstrafen im Höchstmaß von mindestens fünf Jahren geahndet werden, wenn

a) sie im Rahmen einer kriminellen Vereinigung im Sinne des Rahmenbeschlusses 2008/841/JI ungeachtet des dort genannten Strafmaßes verübt wurden oder
b) einen schweren Schaden verursachen[8] oder
c) gegen ein Informationssystem verübt wurden, das Teil der kritischen Infrastruktur ist.

(…)

[…]

Artikel 11

Verantwortlichkeit juristischer Personen

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person für eine Straftat im Sinne der Artikel 3 bis 8 verantwortlich gemacht werden kann, die zu ihren Gunsten von einer Person begangen wurde, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt hat und die eine Führungsposition innerhalb der juristischen Person innehat aufgrund

a) einer Befugnis zur Vertretung der juristischen Person,

[7] Prüfungsvorbehalt von FR, ES und EE. LV kann diesen Vorschlag nicht unterstützen.
[8] Prüfungsvorbehalt von RO zu Artikel 9 Absatz 4 Buchstabe b.

b) einer Befugnis, Entscheidungen im Namen der juristischen Person zu treffen, oder

c) einer Kontrollbefugnis innerhalb der juristischen Person.

2. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle durch die in Absatz 1 genannte Person die Begehung einer Straftat nach den Artikeln 3 bis 8 zugunsten der juristischen Person durch eine ihr unterstellte Person ermöglicht hat.

3. Die Verantwortlichkeit der juristischen Personen nach den Absätzen 1 und 2 schließt die strafrechtliche Verfolgung natürlicher Personen als Täter, Anstifter oder Gehilfen bei einer Straftat im Sinne der Artikel 3 bis 8 nicht aus.

Artikel 12

Sanktionen gegen juristische Personen

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 11 Absatz 1 verantwortliche juristische Person wirksame, verhältnismäßige und abschreckende Sanktionen verhängt werden können, zu denen Geldbußen oder Geldstrafen gehören und zu denen andere Sanktionen gehören können, beispielsweise:
   a) Ausschluss von öffentlichen Zuwendungen oder Hilfen,
   b) vorübergehendes oder ständiges Verbot der Ausübung einer Handelstätigkeit,
   c) richterliche Aufsicht,
   d) richterlich angeordnete Eröffnung des Liquidationsverfahrens oder
   e) vorübergehende oder endgültige Schließung von Einrichtungen, die zur Begehung der Straftat genutzt wurden.
2. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass gegen eine im Sinne von Artikel 11 Absatz 2 verantwortliche juristische Person wirksame, angemessene und abschreckende Sanktionen oder Maßnahmen verhängt werden können.

Artikel 13

Gerichtliche Zuständigkeit[9]

1. Jeder Mitgliedstaat begründet seine Zuständigkeit für die in den Artikeln 3 bis 8 genannten Straftaten, wenn diese

   a) ganz oder teilweise in seinem Hoheitsgebiet oder

   b) von einem seiner Staatsangehörigen begangen wurden, zumindest in den Fällen, in denen die Tat an dem Ort, an dem sie begangen wurde, eine Straftat darstellt.

2. Bei der Begründung seiner Zuständigkeit gemäß Absatz 1 Buchstabe a stellt jeder Mitgliedstaat sicher, dass sich die Zuständigkeit auch auf Fälle erstreckt, in denen

   a) sich der Täter bei der Begehung der Straftat physisch im Hoheitsgebiet dieses Mitgliedstaats aufhält, unabhängig davon, ob sich die Straftat gegen ein Informationssystem innerhalb oder außerhalb seines Hoheitsgebiets richtet, oder

   b) sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, unabhängig davon, ob sich der Täter bei der Begehung der Straftat physisch im Hoheitsgebiet dieses Mitgliedstaats aufhält.

3. Ein Mitgliedstaat unterrichtet die Kommission über seine Entscheidung, eine weitere gerichtliche Zuständigkeit für Straftaten nach den Artikeln 3 bis 8, die außerhalb seines Hoheitsgebiets begangen wurden, zu begründen, zum Beispiel in Fällen, in denen

   a) der gewöhnliche Aufenthalt des Straftäters in seinem Hoheitsgebiet liegt

   b) die Straftat zugunsten einer in seinem Hoheitsgebiet niedergelassenen juristischen Person begangen wird.

---

[9] UK hält an einem Prüfungsvorbehalt zu diesem Artikel fest.

Artikel 14

Informationsaustausch[10]

1. Zum Zwecke des Informationsaustauschs über Straftaten nach den Artikeln 3 bis 8 nutzen die Mitgliedstaaten das bestehende Netz der operativen Kontaktstellen, die an sieben Wochentagen 24 Stunden täglich zur Verfügung stehen. Die Mitgliedstaaten sorgen dafür, dass Verfahren vorhanden sind, mit sie denen bei dringenden Ersuchen binnen höchstens acht Stunden zumindest mitteilen können, ob das Ersuchen um Unterstützung beantwortet wird und in welcher Form und wann dies voraussichtlich erfolgen wird.

2. Die Mitgliedstaaten teilen der Kommission ihre Kontaktstelle für den Informationsaustausch über Straftaten im Sinne der Artikel 3 bis 8 mit. Die Kommission leitet diese Information an die anderen Mitgliedstaaten weiter.

Artikel 15

Kontrolle und Statistiken[11]

1. Die Mitgliedstaaten sorgen dafür, dass ein System für die Aufzeichnung, Erstellung und Bereitstellung statistischer Daten zu den Straftaten im Sinne der Artikel 3 bis 7 bereitsteht.

2. Die statistischen Daten gemäß Absatz 1 umfassen zumindest die vorhandenen Daten über die Anzahl der in den Mitgliedstaaten erfassten Straftaten im Sinne der Artikel 3 bis 7 und die Anzahl der Personen, die wegen einer Straftat im Sinne der Artikel 3 bis 7 verfolgt und verurteilt worden sind.

3. Die Mitgliedstaaten übermitteln der Kommission die nach Maßgabe dieses Artikels erfassten Daten. Die Kommission sorgt dafür, dass eine konsolidierte Zusammenfassung dieser statistischen Berichte veröffentlicht wird.

---

10 Prüfungsvorbehalt von ES.
11 Prüfungsvorbehalte von ES.

Artikel 16

Ersetzung des Rahmenbeschlusses 2005/222/JI[12]

Der Rahmenbeschluss 2005/222/JI wird in Bezug auf die Mitgliedstaaten ersetzt, die sich an der Annahme dieser Richtlinie beteiligen, unbeschadet der Pflichten der Mitgliedstaaten im Zusammenhang mit den Fristen für die Umsetzung des Rahmenbeschlusses in innerstaatliches Recht.

In Bezug auf die Mitgliedstaaten, die sich an der Annahme dieser Richtlinie beteiligen, gelten Verweise auf den Rahmenbeschluss 2005/222/JI als Verweise auf die vorliegende Richtlinie.

Artikel 17

Umsetzung

1. Die Mitgliedstaaten setzen die erforderlichen Rechts- und Verwaltungsvorschriften in Kraft, um dieser Richtlinie bis [zwei Jahre nach ihrem Erlass] nachzukommen.

2. Die Mitgliedstaaten übermitteln der Kommission den Wortlaut der innerstaatlichen Rechtsvorschriften zur Umsetzung ihrer Verpflichtungen aus dieser Richtlinie.

3. Bei Erlass dieser Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

Artikel 18

Berichterstattung

1. Die Kommission berichtet dem Europäischen Parlament und dem Rat bis [VIER JAHRE NACH ERLASS DER RICHTLINIE], inwieweit die Mitgliedstaaten die zur Einhaltung dieser Richtlinie notwendigen Maßnahmen ergriffen haben, und unterbreitet erforderlichenfalls Gesetzgebungsvorschläge.

(…)

12 UK erhält Prüfungsvorbehalte aufrecht.

Artikel 19

Inkrafttreten

Diese Richtlinie tritt am Tag ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Artikel 20

Adressaten

Diese Richtlinie ist gemäß den Verträgen an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*