EUROPÄISCHE KOMMISSION

Brüssel, den 30.9.2010
KOM(2010) 517 endgültig

2010/0273 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

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

{SEK(2010) 1122 final}
{SEK(2010) 1123 final}

BEGRÜNDUNG

1. GRÜNDE FÜR DEN VORSCHLAG UND ZIELSETZUNG

Der Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme[1] soll durch den vorliegenden Vorschlag ersetzt werden. Ziel des Rahmenbeschlusses war, wie es in den Erwägungsgründen heißt, durch Angleichung der einzelstaatlichen Strafvorschriften für Angriffe auf Informationssysteme die Zusammenarbeit zwischen den Justiz- und sonstigen zuständigen Behörden, einschließlich der Polizei und anderer spezialisierter Strafverfolgungsbehörden der Mitgliedstaaten, zu verbessern. Er führte Vorschriften für Straftaten wie rechtswidriger Zugang zu Informationssystemen, rechtswidriger Systemeingriff und rechtswidriger Dateneingriff ein sowie besondere Regeln für die Haftung juristischer Personen, die gerichtliche Zuständigkeit und den Informationsaustausch. Die Mitgliedstaaten mussten dem Rahmenbeschluss bis zum 16. März 2007 nachkommen.

Am 14. Juli 2008 gab die Kommission einen Bericht über die Umsetzung des Rahmenbeschlusses heraus[2]. Den Schlussfolgerungen dieses Berichts zufolge sind in den meisten Mitgliedstaaten beachtliche Fortschritte erzielt worden, so dass der Umsetzungsstand relativ gut ist, doch ist die Umsetzung in einigen Mitgliedstaaten noch nicht abgeschlossen. Weiter heißt es in dem Bericht: „Nach Annahme des RB haben in jüngster Zeit Angriffe auf Informationssysteme in Europa mehrere neue Gefahren verdeutlicht, insbesondere massive gleichzeitige Angriffe auf Informationssysteme und eine zunehmende kriminelle Nutzung so genannter Botnets.“ Diese Angriffe standen nicht im Mittelpunkt des Interesses, als der Rahmenbeschluss angenommen wurde. Um diesen Entwicklungen entgegenzutreten, wird die Kommission prüfen, mit welchen Maßnahmen besser auf die Bedrohung durch Botnetze reagiert werden kann (was unter einem „Botnet“ bzw. „Botnetz“ zu verstehen ist, wird unter dem folgenden Gliederungspunkt erläutert).

Wie wichtig eine entschlossenere Bekämpfung der Cyberkriminalität ist, wurde schon im Haager Programm von 2004 zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union und anschließend im Stockholmer Programm von 2009 und in dem dazugehörigen Aktionsplan betont[3]. Auch in der kürzlich vorgestellten Digitalen Agenda für Europa[4] – der ersten Leitinitiative, die im Rahmen der Strategie Europa 2020 angenommen wurde – wird die Notwendigkeit anerkannt, dem Aufkommen neuer Formen der Kriminalität, insbesondere der Cyberkriminalität, auf europäischer Ebene Einhalt zu gebieten. Die Kommission ist entschlossen, Cyberangriffen auf Informationssysteme entgegenzutreten, da Vertrauen und Sicherheit für diesen Bereich unabdingbar sind.

Auf internationaler Ebene gilt das Übereinkommen des Europarats über Computerkriminalität vom 23. November 2001 als zurzeit vollständigster internationaler Standard, da das Übereinkommen eine umfassende, kohärente Regelung der verschiedenen Aspekte der Cyberkriminalität bietet[5]. Das Übereinkommen ist von allen 27 EU-Mitgliedstaaten

---

1 ABl. L 69 vom 16.3.2005, S. 68.

2 Bericht der Kommission an den Rat auf der Grundlage von Artikel 12 des Rahmenbeschlusses des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, KOM(2008) 448 endg.

3 ABl. C 198 vom 12.8.2005, ABl. C 115 vom 4.5.2010, KOM(2010) 171 vom 20.4.2010.

4 Mitteilung der Kommission, KOM(2010) 245 vom 19.5.2010.

5 Übereinkommen des Europarats über Computerkriminalität, Budapest 23.11.2001, SEV-Nr. 185.

unterzeichnet worden, aber nur 15 Mitgliedstaaten haben es bislang ratifiziert[6]. Das Übereinkommen ist am 1. Juli 2004 in Kraft getreten. Die EU selbst hat das Übereinkommen nicht unterzeichnet. Angesichts der Bedeutung dieses Übereinkommens wirkt die Kommission aktiv darauf hin, dass die Ratifizierung in den verbleibenden EU-Mitgliedstaaten so rasch wie möglich abgeschlossen wird.

- **Allgemeiner Kontext**

Cyberkriminalität ist in erster Linie auf die Anfälligkeit der Systeme zurückzuführen, die durch mehrere Faktoren bedingt ist. Inadäquate Strafverfolgungsverfahren tragen zum Fortbestehen der Cyberkriminalität bei und verschärfen die Probleme, da diese Art von Straftaten nicht an nationalen Grenzen haltmacht. Auch werden solche Straftaten oft nicht angezeigt, weil sie entweder nicht bemerkt werden oder weil die Opfer (Geschäftsleute und Unternehmen) fürchten, dass eine Anzeige ihrem Ruf schaden und ihre Geschäftsaussichten – durch das Bekanntwerden ihrer Schwachstellen – beeinträchtigen könnte.

Darüber hinaus können Unterschiede im nationalen Straf- und Prozessrecht eine unterschiedliche Behandlung solcher Straftaten durch die Strafverfolgungsbehörden und die Gerichte zur Folge haben. Die Entwicklungen im Bereich der Informationstechnologie haben diese Probleme weiter verschärft; es ist für Straftäter leichter geworden, Software (Schadprogramme und Botnetze) zu produzieren und zu verbreiten und dabei ihre Anonymität zu wahren und sich dank unterschiedlicher gerichtlicher Zuständigkeiten der Verantwortung zu entziehen. Wegen der Schwierigkeiten bei der Strafverfolgung kann die organisierte Kriminalität relativ risikolos beträchtliche Gewinne erzielen.

Dieser Vorschlag trägt den neuen Methoden der Internetkriminalität, insbesondere dem Einsatz von Botnetzen, Rechnung. Der Ausdruck „Botnetz“ bezeichnet ein Computernetz, das mit einer Schadsoftware (Computervirus) infiziert wurde. Ein solches Netzwerk aus infizierten Computern („Zombies“) kann ferngesteuert bestimmte Handlungen ausführen beispielsweise Informationssysteme angreifen (Cyberangriffe). Diese „Zombies“ können von einem anderen Computer kontrolliert werden – häufig ohne Wissen der Nutzer dieser infizierten Computer. Die Kontrolle über ein Botnetz übt ein sogenannter „Master-Server“ – auch als „Command-and-Control-Server“ bezeichnet – aus. Die Personen, die diesen Server kontrollieren, sind zum Täterkreis zu rechnen, da sie die infizierten Computer zum Angriff auf Informationssysteme nutzen. Es ist sehr schwierig, diesen Tätern auf die Spur zu kommen, da sich das Botnetz, das die Attacke ausführt, an einem anderen Ort befinden kann als die Täter.

Attacken eines Botnetzes sind häufig größeren Umfangs. Bei solchen Großangriffen handelt es sich entweder um Angriffe, die mit einer Software ausgeführt werden, die eine Vielzahl von Informationssystemen (Computern) schädigt, oder um Angriffe, die beispielsweise eine Störung elektronischer Dienste, finanzielle Verluste oder Verluste persönlicher Daten verursachen. Der hierdurch verursachte Schaden hat beträchtliche Auswirkungen auf das Funktionieren des anvisierten Systems bzw. beeinträchtigt dessen Arbeitsumgebung. In diesem Zusammenhang ist unter einem großen Botnetz ein Netzwerk zu verstehen, das in der Lage ist, einen schweren Schaden zu verursachen. Botnetze anhand ihrer Größe zu bestimmen, ist nicht einfach. Bei den größten bekannten Botnetzen wurde geschätzt, dass sie

---

[6] Informationen über den Ratifikationsstand des Übereinkommens (SEV-Nr. 185) sind auf folgender Internetseite erhältlich: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

in einem Zeitraum von 24 Stunden[7] 40 000 bis 100 000 Verbindungen (d. h. infizierte Computer) umfassen.

- **Bestehende Rechtsvorschriften auf diesem Gebiet**

Der Rahmenbeschluss hat durch die EU-weite Einführung von Straftatbeständen im Bereich der Cyberkriminalität (z. B. rechtswidriger Zugang zu Informationssystemen, rechtswidriger Systemeingriff und rechtswidriger Dateneingriff sowie Anstiftung, Beihilfe und Versuch dazu) zu einem Mindestmaß an strafrechtlicher Harmonisierung in den Mitgliedstaaten geführt.

Die Bestimmungen des Rahmenbeschlusses wurden zwar von den Mitgliedstaaten im Großen und Ganzen umgesetzt, doch weist der Beschluss angesichts der zu beobachtenden Tendenzen, was Umfang und Anzahl der Cyberangriffe anbelangt, einige Unzulänglichkeiten auf. Die Harmonisierung beschränkt sich auf eine begrenzte Anzahl von Straftatbeständen, wird aber der potenziellen Bedrohung, die von groß angelegten Cyberattacken auf die Gesellschaft ausgeht, nicht gerecht. Auch der Schwere der Straftaten und den entsprechenden Sanktionen wurde nicht hinreichend Rechnung getragen.

Mit Internetattacken, Netzsicherheit und Sicherheit der Internetnutzer befassen sich auch andere bereits laufende oder geplante EU-Initiativen und -Programme. Hierzu zählen Maßnahmen, die von Programmen wie „Kriminalprävention und Kriminalitätsbekämpfung“[8], „Strafjustiz“[9], „Sicheres Internet“[10] und der Initiative „Kritische Informationsinfrastrukturen“[11] gefördert werden. Eine weitere relevante Regelung für diesen Bereich ist der Rahmenbeschluss 2004/68/JI zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie.

Die Manipulation von Computern und deren Umwandlung in Botnetze ist in verwaltungsrechtlicher Hinsicht bereits durch das Datenschutzrecht der EU verboten[12]. Vor allem die nationalen Verwaltungen arbeiten bereits im Rahmen des Europäischen Kontaktnetzes der für die Spam-Bekämpfung zuständigen Behörden zusammen. Die Mitgliedstaaten sind danach verpflichtet, das Abfangen von Nachrichten, die über öffentliche Kommunikationsnetze und mit öffentlich zugänglichen elektronischen Kommunikationsdiensten übertragen werden, durch andere Personen als die Nutzer zu verbieten, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, diese anderen Personen sind gesetzlich dazu ermächtigt.

Dieser Vorschlag steht im Einklang mit diesen Vorschriften. Die Mitgliedstaaten sollten darauf achten, dass die Zusammenarbeit zwischen Verwaltungs- und Strafverfolgungsbehörden in Fällen verbessert wird, die sowohl verwaltungs- als auch strafrechtliche Sanktionen nach sich ziehen können.

---

7 Zur Bestimmung der Größe eines Botnetzes wird allgemein die Anzahl der Verbindungen in einem 24-Stunden-Intervall herangezogen.

8 Siehe: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm.

9 Siehe: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm.

10 Siehe: http://ec.europa.eu/information_society/activities/sip/index_en.htm.

11 Siehe: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

12 Datenschutzrichtlinie für elektronische Kommunikation (ABl. L 201 vom 31.7.2002) in der Fassung der Richtlinie 2009/136/EG (ABl. L 337 vom 18.12.2009).

- **Vereinbarkeit mit anderen Politikbereichen und Zielen der Union**

Die mit diesem Vorschlag verfolgten Ziele stehen im Einklang mit der Politik der EU in den Bereichen Bekämpfung der organisierten Kriminalität, Erhöhung der Abwehrfähigkeit von Computernetzen, Schutz kritischer Informationsinfrastrukturen und Datenschutz. Die Ziele stehen auch im Einklang mit dem Programm „Sicheres Internet“, das zur Förderung der sicheren Nutzung des Internet und der neuen Online-Techniken sowie zur Bekämpfung illegaler Inhalte aufgelegt wurde.

Dieser Vorschlag ist gründlich daraufhin geprüft worden, dass seine Bestimmungen mit den Grundrechten und insbesondere dem Schutz personenbezogener Daten, der Freiheit der Meinungsäußerung und der Informationsfreiheit, dem Recht auf ein faires Verfahren, der Unschuldsvermutung und den Verteidigungsrechten sowie – in Bezug auf Straftaten und Sanktionen – dem Gesetzlichkeits- und Verhältnismäßigkeitsprinzip voll im Einklang stehen.

2. ANHÖRUNG INTERESSIERTER KREISE UND FOLGENABSCHÄTZUNG

- **Anhörung interessierter Kreise**

Es fanden mehrere Sitzungen zu den diversen Aspekten der Bekämpfung der Cyberkriminalität einschließlich deren strafrechtlicher Verfolgung statt, an denen Sachverständige unterschiedlicher Provenienz – u. a. Vertreter des öffentlichen und des privaten Sektors der Mitgliedstaaten, fachlich spezialisierte Richter und Staatsanwälte, Vertreter von internationalen Organisationen, europäischen Agenturen und Fachverbänden – teilnahmen. Im Anschluss an diese Sitzungen haben mehrere Sachverständige und Organisationen Beiträge und Informationen übermittelt.

Die Konsultation hat folgende wichtige Ergebnisse gebracht:

– Es besteht Handlungsbedarf auf EU-Ebene.

– Bestimmte Arten von Straftaten, insbesondere neue Formen von Cyberangriffen (Botnetzen), die im geltenden Rahmenbeschluss nicht erfasst sind, müssen unter Strafe gestellt werden.

– Hindernisse für die Ermittlung und Strafverfolgung in grenzübergreifenden Fällen müssen beseitigt werden.

Die während der Konsultation eingegangenen Beiträge sind in die Folgenabschätzung eingeflossen.

Einholung und Nutzung von Expertenwissen

Expertenwissen wurde bei den Zusammenkünften mit den Beteiligten eingebracht.

Folgenabschätzung

Es wurden verschiedene Optionen zur Verwirklichung der angestrebten Ziele geprüft.

- Option (1): Status quo / Keine neuen Maßnahmen auf EU-Ebene

Bei dieser Option würde die EU keine weiteren Maßnahmen ergreifen, um gegen Angriffe auf Informationssysteme als besonderer Form der Internetkriminalität vorzugehen. Laufende Maßnahmen, insbesondere die Programme zur Stärkung des Schutzes kritischer Informationsinfrastrukturen und zur Verbesserung der Zusammenarbeit des öffentlichen und des privaten Sektors bei der Bekämpfung der Cyberkriminalität, würden fortgesetzt.

- Option (2): Ausarbeitung eines Programms zur Stärkung der Abwehr von Angriffen auf Informationssysteme durch nichtlegislative Maßnahmen

Nichtlegislative Maßnahmen würden zusätzlich zu dem Programm zum Schutz kritischer Informationsinfrastrukturen bei der grenzübergreifenden Strafverfolgung und der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor ansetzen. Diese nicht rechtsverbindlichen Instrumente würden auf die Förderung weiterer konzertierter Aktionen auf EU-Ebene und die Stärkung des bestehenden 24/7-Netzwerks der Kontaktstellen der Strafverfolgungsbehörden abzielen. Des Weiteren wäre an die Einrichtung eines EU-Netzes von öffentlich-privaten Kontaktstellen zu denken, dem Experten auf dem Gebiet der Internetkriminalität und die Strafverfolgungsbehörden angehören, an die Ausarbeitung eines EU-Mustervertrags für die Zusammenarbeit der Strafverfolgungsbehörden mit dem privaten Sektor und an eine Förderung für Schulungsprogramme zur Internetkriminalität für die Strafverfolgungsbehörden.

- Option (3): Gezielte Aktualisierung des Rahmenbeschlusses (neue Richtlinie, die den geltenden Rahmenbeschluss ersetzt), um die Bedrohung abzuwenden, die von groß angelegten Angriffen auf Informationssysteme (Botnetzen) ausgeht, und die Effizienz des Kontaktnetzes der mitgliedstaatlichen Strafverfolgungsbehörden bei Straftaten zu verbessern, die unter Verschleierung der wahren Identität des Täters und Schädigung des rechtmäßigen Identitätseigentümers begangen werden; gleichzeitig soll auch die statistische Erfassung von Cyberangriffen verbessert werden.

Diese Option beinhaltet die Einführung spezifischer (d. h. begrenzter) Rechtsvorschriften, die Großangriffen auf Informationssysteme vorbeugen sollen. Flankiert würden diese Rechtsvorschriften von nichtlegislativen Maßnahmen, die die operative grenzübergreifende Zusammenarbeit zur Abwehr solcher Attacken stärken und auf diese Weise die Umsetzung der legislativen Maßnahmen erleichtern sollen. Ziel dieser Maßnahmen wäre es, die Notfallvorsorge, Sicherheit und Abwehrfähigkeit kritischer Informationsinfrastrukturen zu stärken und bewährte Praktiken auszutauschen.

- Option (4): Einführung einer umfassenden EU-Regelung gegen Cyberkriminalität

Diese Option würde eine neue umfassende EU-Regelung bedeuten. Zusätzlich zu den in Option 2 vorgesehenen nicht verbindlichen Maßnahmen und der Aktualisierung der geltenden Bestimmungen nach Option 3 würden auch andere rechtliche Probleme, die sich bei der Internetnutzung stellen, angegangen. Diese Maßnahmen würden sich nicht nur gegen Cyberangriffe richten, sondern beispielsweise auch gegen Finanzkriminalität mithilfe des Internet und illegale Internetinhalte. Geregelt würden auch die Erhebung, Speicherung und Weitergabe elektronischer Beweismittel, und es würden detailliertere Zuständigkeitsvorschriften festgelegt. Die Regelung würde parallel zum Übereinkommen des Europarats über Computerkriminalität gelten. Die vorgenannten nichtlegislativen Maßnahmen kämen begleitend hinzu.

- Option (5): Aktualisierung des Übereinkommens des Europarats über Computerkriminalität

Diese Option würde eine grundlegende Neuverhandlung des geltenden Übereinkommens erfordern, was sehr zeitaufwändig wäre und deshalb mit den Zeitvorgaben in der Folgenabschätzung nicht vereinbar wäre. Auf internationaler Ebene ist derzeit keine Bereitschaft zur Neuverhandlung des Übereinkommens erkennbar. Eine Aktualisierung des Übereinkommens ist keine realistische Option, da diese den vorgegebenen Zeitrahmen sprengen würde.

Bevorzugte Option: Kombination aus nichtlegislativen Maßnahmen (Option 2) und einer gezielten Aktualisierung des Rahmenbeschlusses (Option 3)

Eine Analyse der wirtschaftlichen und sozialen Auswirkungen sowie der Auswirkungen auf die Grundrechte ergab, dass sich die Probleme am wirkungsvollsten mit den Optionen 2 und 3 angehen lassen, die zur Verwirklichung der Ziele des Vorschlags führen dürften.

Zur Vorbereitung des Vorschlags hat die Kommission eine Folgenabschätzung durchgeführt.

3. RECHTLICHE ASPEKTE

- **Zusammenfassung des Vorschlags**

Durch die Richtlinie wird zwar der Rahmenbeschluss 2005/222/JI aufgehoben, dessen Bestimmungen bleiben aber erhalten. Zusätzlich werden folgende neue Bestimmungen eingefügt:

– Allgemeines materielles Strafrecht:

A. Das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen von Vorrichtungen/Instrumenten, die zur Begehung der betreffenden Straftaten genutzt werden, werden unter Strafe gestellt.

B. Einführung von Bestimmungen über erschwerende Umstände: Als erschwerender Umstand gilt

- der Einsatz von Botnetzen oder ähnlichen Instrumenten (Cyber-Großangriff) bei der Begehung von Straftaten, die im geltenden Rahmenbeschluss aufgeführt sind;

- die Verschleierung der wahren Identität des Täters bei Cyberangriffen, wenn dadurch der rechtmäßige Identitätseigentümer geschädigt wird. Die betreffenden Bestimmungen müssen dem Gesetzlichkeits- und Verhältnismäßigkeitsprinzip in Bezug auf Straftaten und Sanktionen entsprechen und mit den geltenden Datenschutzvorschriften im Einklang stehen[13].

C. Einführung des Straftatbestands „rechtswidriges Abfangen von Daten“.

[13] Vgl. u. a. die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37 (wird zurzeit überarbeitet), und die allgemeine Datenschutzrichtlinie 95/46/EG.

D. Einführung von Maßnahmen zur Verbesserung der Zusammenarbeit der europäischen Strafjustiz durch Ausbau des vorhandenen 24/7-Netzwerks[14]:

- Die operativen Kontaktstellen (Artikel 14 des Richtlinienvorschlags) werden verpflichtet, einem Antrag auf Unterstützung innerhalb einer bestimmten Frist nachzukommen. Das Übereinkommen über Computerkriminalität enthält hierzu keine verbindliche Regelung. Mit dieser Maßnahme soll erreicht werden, dass die Kontaktstellen innerhalb einer bestimmten Frist mitteilen, ob und bis wann sie in der Lage sind, dem Antrag auf Unterstützung zu entsprechen. In welcher Form die Unterstützung gewährt wird, ist nicht geregelt.

E. Einführung einer Verpflichtung für die Mitgliedstaaten, ein geeignetes System für die Aufzeichnung, Erstellung und Bereitstellung statistischer Angaben zu den im geltenden Rahmenbeschluss aufgeführten Straftatbeständen bereitzustellen, um dem Bedarf an einer statistischen Erfassung der Cyberkriminalität zu entsprechen, und Einfügung des neuen Straftatbestands „rechtswidriges Abfangen von Daten".

Die Definitionen der Straftatbestände in den Artikeln 3, 4 und 5 (rechtswidriger Eingriff in Informationssysteme, rechtswidriger Systemeingriff, rechtswidriger Eingriff in Daten) enthalten eine Bestimmung, wonach die Mitgliedstaaten bei der Umsetzung in innerstaatliches Recht die Verwirklichung dieser Straftatbestände zumindest dann unter Strafe stellen müssen, „wenn kein leichter Fall vorliegt". Diese Flexibilität soll es den Mitgliedstaaten erlauben, Fälle auszunehmen, die zwar theoretisch von der Grunddefinition erfasst würden, aber nicht als Schädigung des geschützten rechtlichen Interesses angesehen werden. Hierunter fallen beispielsweise Handlungen junger Leute, die ihre Kenntnisse in der Informationstechnologie unter Beweis stellen wollen. Die Möglichkeit, die Strafbarkeit einzuschränken, darf jedoch nicht dazu führen, dass zusätzlich zu den in der Richtlinie bereits aufgeführten Tatbestandsmerkmalen weitere Kriterien eingeführt werden. Andernfalls hätte dies zur Folge, dass nur Straftaten erfasst würden, bei denen erschwerende Umstände vorliegen. Die Mitgliedstaaten sollten bei der Umsetzung insbesondere davon absehen, weitere Tatbestandsmerkmale wie die Absicht, aus der Straftat einen unrechtmäßigen Erlös zu erzielen, oder eine bestimmte Wirkung wie die Verursachung eines erheblichen Schadens aufzunehmen.

- **Rechtsgrundlage**

Artikel 83 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union[15].

- **Subsidiaritätsprinzip**

Das Handeln der Europäischen Union unterliegt dem Subsidiaritätsprinzip. Die Ziele des Vorschlags können aus folgenden Gründen von den Mitgliedstaaten allein nicht vollständig realisiert werden:

Internetkriminalität und insbesondere Angriffe auf Informationssysteme haben eine beträchtliche grenzübergreifende Dimension, was bei Cyber-Großangriffen am deutlichsten sichtbar ist, da sie häufig von verschiedenen Standorten in verschiedenen Ländern ausgehen.

---

[14] Eingerichtet durch das Übereinkommen über Computerkriminalität und den Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme.

[15] ABl. C 83 vom 30.3.2010, S. 49.

Dies erfordert ein Vorgehen auf EU-Ebene, um dem gegenwärtigen Trend zu groß angelegten Computerattacken in Europa und weltweit entgegenzuwirken. Maßnahmen auf EU-Ebene und eine Aktualisierung des Rahmenbeschlusses 2005/222/JI wurden auch in den Schlussfolgerungen des Rates vom November 2008[16] gefordert, da die Mitgliedstaaten allein nicht in der Lage sind, die Bürger wirksam vor Cyberangriffen zu schützen.

Die Ziele des Vorschlags können aus folgenden Gründen besser durch Maßnahmen der Europäischen Union erreicht werden:

Durch den Vorschlag werden das materielle Strafrecht und die Verfahrensvorschriften der Mitgliedstaaten stärker als durch den derzeitigen Rahmenbeschluss angenähert, was sich positiv auf die Bekämpfung dieser Straftaten auswirken wird. Erstens werden Straftäter auf diese Weise davon abgehalten, sich in Mitgliedstaaten zu begeben, in denen Cyberangriffe weniger hart bestraft werden. Zweitens ermöglichen einheitliche Definitionen den Austausch von Informationen und die Erhebung und den Abgleich relevanter Daten. Drittens erhöht sich so die Wirkung von Präventivmaßnahmen in der EU und die internationale Zusammenarbeit wird gestärkt.

Der Vorschlag steht daher mit dem Subsidiaritätsprinzip im Einklang.

- **Grundsatz der Verhältnismäßigkeit**

Der Vorschlag steht aus folgendem Grund mit dem Grundsatz der Verhältnismäßigkeit im Einklang:

Er beschränkt sich auf das zur Erreichung seiner Ziele auf europäischer Ebene erforderliche Mindestmaß und geht angesichts der Notwendigkeit einer präzisen Strafgesetzgebung nicht über das zu diesem Zweck Erforderliche hinaus.

- **Wahl des Instruments**

Vorgeschlagenes Instrument: Richtlinie.

Andere Instrumente wären aus folgendem Grund nicht angemessen:

Die Rechtsgrundlage erfordert eine Richtlinie.

Nichtlegislative Maßnahmen und Selbstregulierung würden die Situation zwar in einigen Bereichen, in denen es auf die Umsetzung ankommt, verbessern, in anderen Bereichen aber, in denen neue Rechtsvorschriften unabdingbar sind, wären die Vorteile nur gering.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Die Auswirkungen des Vorschlags auf den EU-Haushalt sind gering. Über 90 % der geschätzten Kosten von 5 913 000 EUR würden von den Mitgliedstaaten übernommen. Sie könnten EU-Mittel beantragen, um ihre Kosten zu reduzieren.

---

[16] „Eine konzertierte Arbeitsstrategie und konkrete Maßnahmen zur Bekämpfung der Cyberkriminalität“, 2987. Tagung des Rats Justiz und Inneres, Brüssel 27./28. November 2008.

5. WEITERE ANGABEN

- **Aufhebung geltender Rechtsvorschriften**

Durch die Annahme des Vorschlags werden die bestehenden Rechtsvorschriften aufgehoben.

- **Räumlicher Geltungsbereich**

Die Richtlinie ist gemäß den Verträgen an die Mitgliedstaaten gerichtet.

2010/0273 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Angriffe auf Informationssysteme und zur Aufhebung 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[17],

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 sowie die Verbesserung der Zusammenarbeit zwischen den Justiz- und sonstigen 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 Europäischen 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.

(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 unverzichtbar sind. Diese Tendenz geht einher mit der Entwicklung immer ausgefeilterer Instrumente, die von Kriminellen zu Cyberangriffen unterschiedlichster Art genutzt werden können.

[17] ABl. C […] vom […], S. […].

(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.

(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[18] verübt werden, bei groß angelegten Angriffen oder bei Straftaten, die unter Verschleierung der wahren Identität des Täters begangen werden und den rechtmäßigen Identitätseigentümer schädigen. Es ist ferner angemessen, schwerere Strafen vorzusehen, wenn ein solcher Angriff schwere Schäden verursacht oder wesentliche Interessen beeinträchtigt hat.

(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 Botnetzen handeln, die für Cyberangriffe verwendet werden.

(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.

(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 sofortige Unterstützung bei Ermittlungen und Verfahren wegen Straftaten im Zusammenhang mit Informationssystemen und –daten oder bei der Erhebung von Beweismaterial in elektronischer Form für eine Straftat leisten 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. Diese Unterstützung sollte die Erleichterung oder die unmittelbare

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

Durchführung folgender Maßnahmen einschließen: fachliche Beratung, Sicherung von Daten, Erhebung von Beweismaterial, Erteilung von Rechtsauskünften und Ausfindigmachen verdächtiger Personen.

(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[19], 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[20] geschützt werden.

(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

---

19 ABl. L 350 vom 30.12.2008, S. 60.

20 ABl. L 8 vom 12.1.2001, S. 1.

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 den Artikeln 1, 2, 3 und 4 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] ODER [Unbeschadet des Artikels 4 des Protokolls über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts beteiligen sich das Vereinigte Königreich und Irland nicht an der Annahme dieser Richtlinie, die daher für sie nicht bindend und ihnen gegenüber nicht anwendbar ist].

(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 –

HABEN FOLGENDE RICHTLINIE ERLASSEN:

Artikel 1
Gegenstand

Diese Richtlinie legt Straftatbestände für Angriffe auf Informationssysteme und Mindestvorschriften für Sanktionen fest. Sie enthält überdies gemeinsame Vorschriften, um solchen Angriffen entgegenzuwirken und die europäische justizielle Zusammenarbeit in Strafsachen auf diesem Gebiet zu 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 oder Eingriff, der 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 kein leichter Fall vorliegt.

Artikel 4
Rechtswidriger Systemeingriff

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die vorsätzliche unbefugte 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 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, unter Strafe gestellt wird.

Artikel 7
Tatwerkzeuge

Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche unbefugte Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Besitzen, Verbreiten oder anderweitige Verfügbarmachen folgender Instrumente, die zur Begehung von Straftaten im Sinne der Artikel 3 bis 6 genutzt werden, unter Strafe gestellt werden:

a) einer Vorrichtung einschließlich eines Computerprogramms, die 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 3 bis 6 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 7 mit Freiheitsstrafen im Höchstmaß von mindestens zwei Jahren geahndet werden.

Artikel 10
Erschwerende Umstände

1. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 3 bis 7 mit Freiheitsstrafen im Höchstmaß von mindestens fünf Jahren geahndet werden, wenn sie im Rahmen einer kriminellen Vereinigung im Sinne des Rahmenbeschlusses 2008/841/JI begangen wurden.

2. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 3 bis 6 mit Freiheitsstrafen im Höchstmaß von mindestens fünf Jahren geahndet werden, wenn sie mit einem Instrument begangen wurden, das dazu bestimmt ist, Angriffe auszulösen, die eine beträchtliche Anzahl von Informationssystemen schädigen oder einen erheblichen Schaden unter anderem in Form gestörter elektronischer Dienste, finanzieller Verluste oder des Verlusts persönlicher Daten verursachen.

3. Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass Straftaten im Sinne der Artikel 3 bis 6 mit Freiheitsstrafen im Höchstmaß von mindestens fünf Jahren geahndet werden, wenn sie durch Verschleierung der wahren Identität des Täters und Schädigung des rechtmäßigen Identitätseigentümers begangen wurden.

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,

   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 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

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,

   b) von einem seiner Staatsangehörigen oder einer Person, die ihren gewöhnlichen Aufenthalt in seinem Hoheitsgebiet hat, oder

   c) zugunsten einer juristischen Person, die ihren Sitz im Hoheitsgebiet dieses Mitgliedstaats hat,

   begangen wurden.

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.

Artikel 14
Informationsaustausch

1. Zum Zwecke des Informationsaustauschs über Straftaten nach den Artikeln 3 bis 8 nutzen die Mitgliedstaaten im Einklang mit den Datenschutzbestimmungen 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 denen dringende Ersuchen binnen höchstens acht Stunden beantwortet werden können. In der Antwort ist mindestens anzugeben, ob, in welcher Form und wann das Ersuchen um Unterstützung erledigt 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

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 8 bereitsteht.

2. Die statistischen Daten gemäß Absatz 1 geben zumindest Aufschluss über die Anzahl der in den Mitgliedstaaten angezeigten Straftaten im Sinne der Artikel 3 bis 8 und die weitere Behandlung dieser Anzeigen sowie – auf Jahresbasis – über die Anzahl der Fälle, in denen Ermittlungen durchgeführt werden, die Anzahl der Personen, gegen die ermittelt wird, und die Anzahl der Personen, die wegen einer Straftat im Sinne der Artikel 3 bis 8 verurteilt worden sind.

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

Artikel 16
Aufhebung des Rahmenbeschlusses 2005/222/JI

Der Rahmenbeschluss 2005/222/JI wird unbeschadet der Pflichten der Mitgliedstaaten im Zusammenhang mit den Fristen für die Umsetzung in innerstaatliches Recht aufgehoben.

Verweise auf den aufgehobenen Rahmenbeschluss gelten als Verweise auf die vorliegende Richtlinie.

Artikel 17
Umsetzung

1. Die Mitgliedstaaten setzen die erforderlichen Rechts- und Verwaltungsvorschriften in Kraft, um dieser Richtlinie spätestens bis [zwei Jahre nach ihrem Erlass] nachzukommen. Sie teilen der Kommission unverzüglich den Wortlaut dieser Rechtsvorschriften mit und fügen eine Tabelle der Entsprechungen zwischen der Richtlinie und diesen innerstaatlichen Rechtsvorschriften bei. 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 der Bezugnahme.

2. Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten innerstaatlichen Rechtsvorschriften mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

Artikel 18
Berichterstattung

1. Bis [VIER JAHRE NACH ANNAHME DER RICHTLINIE] und danach jeweils alle drei Jahre legt die Kommission dem Europäischen Parlament und dem Rat einen Bericht über die Anwendung dieser Richtlinie in den Mitgliedstaaten gegebenenfalls mit Änderungsvorschlägen vor.

2. Die Mitgliedstaaten übermitteln der Kommission alle Angaben, die für die Erstellung des in Absatz 1 genannten Berichts dienlich sind. Dazu gehört auch eine ausführliche Beschreibung der zur Umsetzung dieser Richtlinie verabschiedeten gesetzgeberischen und sonstigen Maßnahmen.

Artikel 19

Inkrafttreten

Diese Richtlinie tritt am zwanzigsten Tag nach 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*