Vorschlag für einen Rahmenbeschluss des Rates über Angriffe auf Informationssysteme

(2002/C 203 E/16)

KOM(2002) 173 endg. — 2002/0086(CNS)

(Von der Kommission vorgelegt am 19. April 2002)

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 29, 30 Absatz 1 Buchstabe a), 31 und 34 Absatz 2 Buchstabe b)

auf Vorschlag der Kommission,

nach Stellungnahme des Europäischen Parlaments,

in Erwägung nachstehender Gründe:

(1) Es finden nachweislich — und insbesondere im Rahmen der organisierten Kriminalität — Angriffe auf Informationssysteme statt, und die Furcht vor Terroranschlägen auf Informationssysteme, die Teil der kritischen Infrastruktur der Mitgliedstaaten sind, wächst. Das Ziel des Aufbaus einer sichereren Informationsgesellschaft und eines Raumes der Freiheit, der Sicherheit und des Rechts wird hierdurch gefährdet. Daher bedarf es Gegenmaßnahmen auf Ebene der Europäischen Union.

(2) Um diesen Gefahren wirksam begegnen zu können, ist ein umfassender Ansatz zur Gewährleistung der Sicherheit der Netze und Informationen erforderlich, wie dies im Aktionsplan „*e*Europe", in der Mitteilung der Kommission „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz" [1] und in der Entschließung des Rates vom 6. Dezember 2001 zu einem gemeinsamen Ansatz und spezifischen Maßnahmen im Bereich der Netz- und Informationssicherheit hervorgehoben wurde.

(3) Das Europäische Parlament hat in seiner Entschliessung vom 5. September 2001 [2] auf die Notwendigkeit einer stärkeren Sensibilisierung für die Probleme der Informationsgesellschaft und der Gewährung von praktischer Hilfe hingewiesen.

(4) Die Bekämpfung der organisierten Kriminalität und des Terrorismus wird durch beträchtliche Unterschiede und Diskrepanzen zwischen den einschlägigen Rechtsvorschriften der Mitgliedstaaten erschwert, die einer wirksamen polizeilichen und justiziellen Zusammenarbeit gegen Angriffe auf Informationssysteme im Wege stehen. Der länder- und grenzübergreifende Charakter moderner elektronischer Kommunikationsnetze führt dazu, dass Angriffe auf Informationssysteme häufig eine internationale Dimension annehmen, was den dringenden Bedarf an weiteren Maßnahmen zur Angleichung der einschlägigen Strafrechtsvorschriften unterstreicht.

(5) Der Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raumes der Freiheit, der Sicherheit und des Rechts [3], der Europäische Rat von Tampere vom 15./16. Oktober 1999, der Europäische Rat von Santa Maria da Feira vom 19./20. Juni 2000, die Kommission im Anzeiger der Fortschritte [4] und das Europäische Parlament in seiner Entschließung vom 19. Mai 2000 [5] haben legislative Maßnahmen (einschließlich gemeinsamer Definitionen, Tatbestandsmerkmale und Sanktionen) gegen die High-Tech-Kriminalität genannt oder gefordert.

(6) Die von internationalen Organisationen und insbesondere vom Europarat geleisteten Arbeiten zur Angleichung des Strafrechts sowie die Arbeiten der G8 zum Thema grenzüberschreitende Zusammenarbeit im Bereich der High-Tech-Kriminalität müssen durch einen gemeinsamen Ansatz der Europäischen Union für diesen Bereich ergänzt werden. Diese Anforderung wurde in der Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zur „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität" [6] näher ausgeführt.

(7) Das Strafrecht im Bereich schwerwiegender Angriffe auf Informationssysteme muss angeglichen werden, um eine möglichst effiziente polizeiliche und justizielle Zusammenarbeit bei Straftaten in Verbindung mit Angriffen auf Informationssysteme sicherzustellen und einen Betrag zur Bekämpfung der organisierten Kriminalität und des Terrorismus zu leisten.

---

[1] KOM(2001) 298.

[2] Entschliessung des Europäischen Parlaments zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI)).

[3] ABl. C 19 vom 23.1.1999.

[4] KOM(2001) 278 endg.

[5] A5-0127/2000.

[6] KOM(2000) 890.

(8) Die Bezugnahmen auf die Computerkriminalität im Rahmenbeschluss über den Europäischen Haftbefehl, im Anhang zum Europol-Übereinkommen und im Beschluss des Rates über die Einrichtung von Eurojust bedürfen einer genaueren Definition. Im Sinne dieser Instrumente sollte der Begriff „Computerkriminalität" so verstanden werden, daß er auch Angriffe gegen Informationssysteme gemäß der Definition im Rahmenbeschluss einschließt, denn auf diese Weise lässt sich eine viel stärkere Angleichung der Tatbestandsmerkmale dieser Delikte erreichen. Dieser Rahmenbeschluss ergänzt zudem den Rahmenbeschluss zur Terrorismusbekämpfung, der u. a. Terrorhandlungen abdeckt, die weit reichende Zerstörungen von Infrastruktureinrichtungen einschließlich Informationssystemen verursachen und dadurch menschliches Leben gefährden oder großen wirtschaftlichen Schaden anrichten können.

(9) Alle Mitgliedstaaten haben das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 ratifiziert. Die im Zusammenhang mit der Umsetzung dieses Rahmenbeschlusses verarbeiteten Daten werden gemäss den Grundsätzen des Übereinkommens geschützt werden.

(10) Gemeinsame Definitionen in diesem Bereich und insbesondere Definitionen von Informationssystemen und Computerdaten sind im Hinblick auf einen einheitlichen Ansatz in den Mitgliedstaaten für die Umsetzung dieses Rahmenbeschlusses von großer Bedeutung.

(11) Es gilt, eine gemeinsame Definition des unberechtigten Zugangs zu Informationssystemen sowie des unrechtmäßigen Eingriffs in ein Informationssystem festzulegen, um so zu einem gemeinsamen Ansatz im Hinblick auf die Tatbestandsmerkmale von Straftaten zu gelangen.

(12) Eine Überkriminalisierung insbesondere von geringfügigen oder Bagatelldelikten ist zu vermeiden; ebenso gilt es zu verhindern, dass Rechteinhaber und Zugangsberechtigte (z. B. rechtmäßige private oder geschäftliche Nutzer, Verantwortliche, Aufsichtspersonen und Netz- oder Systembetreiber, rechtmäßige wissenschaftliche Forscher sowie unternehmensinterne oder um extern ernannte Zugangsberechtigte, die die Erlaubnis besitzen, die Sicherheit eines Systems zu testen) als Kriminelle eingestuft werden.

(13) Die Mitgliedstaaten müssen Angriffe auf Informationssysteme unter Strafe stellen, wobei diese Strafen wirksam, angemessen und abschreckend sein und in schweren Fällen auch Freiheitsstrafen einschließen müssen.

(14) Für Fälle, in denen ein Angriff auf ein Informationssystem aufgrund der Begleitumstände eine noch größere Gefahr für die Gesellschaft darstellt, sind schwerere Strafen vorzusehen. In solchen Fällen sollten die gegen die Täter verhängten Strafen so beschaffen sein, dass Angriffe auf Informationssysteme in den Anwendungsbereich der geltenden Rechtsakte zur Bekämpfung der organisierten Kriminalität fallen, so beispielsweise in den Anwendungsbereich der Gemeinsamen Maßnahme 98/733/JI vom 21. Dezember 1998 — vom Rat aufgrund von Artikel K.3 des Vertrags über die Europäische Union angenommen — betreffend die Strafbarkeit der Beteiligung an einer kriminellen Vereinigung in den Mitgliedstaaten der Europäischen Union ([1]).

(15) Es sind Maßnahmen zu treffen, damit juristische Personen für die von ihnen zu ihrem eigenen Vorteil begangenen Straftaten, auf die sich dieser Akt bezieht, zur Verantwortung gezogen werden und sichergestellt ist, dass jeder Mitgliedstaat für Straftaten zuständig ist, die gegen Informationssysteme in Situationen begangen werden, in denen sich der Straftäter physisch im Hoheitsgebiet dieses Mitgliedstaates aufhält bzw. in denen sich das Informationssystem im Hoheitsgebiet dieses Staates befindet.

(16) Ferner sind Maßnahmen zur Zusammenarbeit zwischen den Mitgliedstaaten im Hinblick auf eine wirksame Vorgehensweise gegen Angriffe auf Informationssysteme vorzusehen. Zum Zwecke des Informationsaustausches sind operative Kontaktstellen einzurichten.

(17) Die Mitgliedstaaten können nicht hinreichend dafür sorgen, dass Angriffe auf Informationssysteme in allen Mitgliedstaaten mit wirksamen, angemessen und abschreckenden Strafen geahndet werden, und die justizielle Zusammenarbeit durch Beseitigung möglicher Hindernisse in ausreichendem Maße verbessern und fördern. Es bedarf dazu gemeinsamer, miteinander zu vereinbarender Regeln. Diese Ziele können daher auf Unionsebene besser verwirklicht werden. Die Union kann in Übereinstimmung mit dem Subsidiaritätsprinzip gemäß Artikel 2 EU-Vertrag, wie in Artikel 5 EG-Vertrag bestimmt, geeignete Maßnahmen treffen. Gemäß dem Grundsatz der Verhältnismäßigkeit gehen die Maßnahmen in Übereinstimmung mit letztgenanntem Artikel nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus.

(18) Dieser Rahmenbeschluss berührt die Befugnisse der Europäischen Gemeinschaft nicht.

(19) Dieser Rahmenbeschluss wahrt die Grundrechte und achtet die Grundsätze, die insbesondere in der Charta der Grundrechte der Europäischen Union, vor allem in den Kapiteln II und VI, anerkannt werden —

HAT FOLGENDEN RAHMENBESCHLUSS ANGENOMMEN:

Artikel 1

Anwendungsbereich und Ziel des Rahmenbeschlusses

Dieser Rahmenbeschluss stellt darauf ab, durch Angleichung der einzelstaatlichen Strafrechtsvorschriften für Angriffe auf Informationssysteme die Zusammenarbeit zwischen den Justiz- und sonstigen zuständigen Behörden der Mitgliedstaaten einschließlich der Polizei und anderen spezialisierten Strafverfolgungsbehörden der Mitgliedstaaten zu verbessern.

([1]) ABl. L 351 vom 29.12.1998, S. 1.

Artikel 2

Begriffsbestimmungen

Für die Anwendung dieses Rahmenbeschlusses bedeuten die Ausdrücke

a) „Elektronisches Kommunikationsnetz" — Übertragungssysteme und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelte, einschließlich Internet) und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hör- und Fernsehfunk sowie Kabelfernsehnetze, unabhängig von der Art der übertragenen Informationen.

b) „Computer" — ein Gerät oder eine Gruppe vernetzter oder miteinander verbundener Geräte, von denen eines oder mehrere nach einem vorgegebenen Programm Computerdaten automatisch verarbeitet bzw. verarbeiten.

c) „Computerdaten" — die Darstellung von Tatsachen, Informationen oder Konzepten, die in einer für die Verarbeitung in einem Informationssystem geeigneten Form erzeugt oder in eine entsprechende Form gebracht werden, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann.

d) „Informationssystem" — Computer und elektronische Kommunikationsnetze sowie die von ihnen zum Zweck des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen Computerdaten.

e) „Juristische Person" — Jedes Rechtssubjekt, das diesen Status nach dem jeweils geltenden innerstaatlichen Recht besitzt, mit Ausnahme von Staaten oder anderen Körperschaften des öffentlichen Rechts in der Ausübung ihrer hoheitlichen Rechte, und von öffentlich-rechtlichen internationalen Organisationen.

f) „Befugte Personen" — Natürliche oder juristische Personen, die vertraglich oder kraft Gesetzes berechtigt sind bzw. die rechtmäßige Erlaubnis besitzen, ein Informationssystem zu nutzen, zu verwalten, zu kontrollieren, zu erproben, im rechtlich zulässigen Rahmen wissenschaftlich zu erforschen oder anderweitig zu betreiben, und die aufgrund dieses Rechts bzw. dieser Erlaubnis handeln.

g) „Unrechtmäßig" — Handlungen von Berechtigten oder andere Handlungen, die nach dem nationalen Recht als rechtmäßig gelten, sind ausgeschlossen.

Artikel 3

Rechtswidriger Zugang zu Informationssystemen

Die Mitgliedstaaten stellen sicher, dass der vorsätzliche und unrechtmäßige Zugang zu einem Informationssystem oder einem Teil eines Informationssystems unter Strafe gestellt wird, sofern diese Handlung

i) gegen einen Teil eines spezifischen Schutzmaßnahmen unterliegenden Informationssystems gerichtet ist oder

ii) mit der Absicht begangen wird, einer natürlichen oder juristischen Person Schaden zuzufügen, oder

iii) mit der Absicht begangen wird, einen wirtschaftlichen Vorteil zu bewirken.

Artikel 4

Rechtswidriger Eingriff in Informationssysteme

Die Mitgliedstaaten stellen sicher, dass die nachstehenden vorsätzlichen und unrechtmäßigen Handlungen unter Strafe gestellt werden:

a) schwere Behinderung oder Störung des Betriebs eines Informationssystems durch Eingabe, Übermittlung, Beschädigung, Löschung, Verstümmelung, Veränderung, Unterdrückung oder Blockierung von Computerdaten;

b) Löschung, Verstümmelung, Veränderung, Unterdrückung oder Blockierung von Computerdaten eines Informationssystems, sofern dies in der Absicht geschieht, einer natürlichen oder einer juristischen Person Schaden zuzufügen.

Artikel 5

Anstiftung, Beihilfe und Versuch

(1) Die Mitgliedstaaten stellen sicher, dass die Anstiftung oder Beihilfe zur Begehung einer der in den Artikeln 3 und 4 genannten Straftaten unter Strafe gestellt wird.

(2) Die Mitgliedstaaten stellen sicher, dass der Versuch der Begehung einer der in den Artikeln 3 und 4 beschriebenen Straftaten unter Strafe gestellt wird.

Artikel 6

Strafen

(1) Die Mitgliedstaaten stellen sicher, dass die in den Artikeln 3, 4 und 5 genannten Straftaten in schweren Fällen durch wirksame, verhältnismäßige und abschreckende Strafen einschließlich Freiheitsstrafen im Höchstmaß von mindestens einem Jahr geahndet werden. Fälle, in denen durch die betreffende Handlung kein Schaden oder wirtschaftlicher Vorteil bewirkt wurde, gelten nicht als schwere Fälle.

(2) Die Mitgliedstaaten sehen die Möglichkeit vor, zusätzlich zu oder anstelle von Freiheitsstrafen Geldstrafen zu verhängen.

Artikel 7

Erschwerende Umstände

(1) Die Mitgliedstaaten stellen sicher, dass Straftaten nach Artikel 3, 4 und 5 mit einer Freiheitsstrafe von mindestens vier Jahren geahndet werden können, sofern sie unter den im Folgenden genannten Umständen begangen werden:

a) die Straftat wurde im Rahmen einer kriminellen Vereinigung gemäß Definition in der Gemeinsamen Maßnahme 98/733/JI vom 21. Dezember 1998 betreffend die Strafbarkeit der Beteiligung an einer kriminellen Vereinigung in den Mitgliedstaaten der Europäischen Union, abgesehen von dem dort vorgesehenen Strafmaß, begangen;

b) durch die Straftat wurde einer natürlichen Person direkt oder indirekt ein erheblicher wirtschaftlicher Verlust oder körperlicher Schaden zugefügt oder ein Teil der kritischen Infrastruktur des Mitgliedstaates erheblich beschädigt; oder

c) durch die Straftat wurden erhebliche Erträge erzielt.

(2) Die Mitgliedstaaten stellen sicher, dass Straftaten nach Artikel 3 und 4 mit längeren als den in Artikel 6 vorgesehenen Freiheitsstrafen geahndet werden können, wenn der Täter bereits in einem Mitgliedstaat wegen einer derartigen Straftat rechtskräftig verurteilt wurde.

Artikel 8

Besondere Umstände

Unbeschadet der Artikel 6 und 7 stellen die Mitgliedstaaten sicher, dass die in Artikel 6 und 7 genannten Strafen herabgesetzt werden können, falls der Täter nach Auffassung der zuständigen Justizbehörde nur einen geringfügigen Schaden verursacht hat.

Artikel 9

Verantwortlichkeit juristischer Personen

(1) Die Mitgliedstaaten stellen sicher, dass eine juristische Person für die in den Artikeln 3, 4 und 5 genannten Handlungen, die zu ihren Gunsten von einer Person begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person gehandelt hat und die eine Führungsposition innerhalb der juristischen Person aufgrund

a) einer Vollmacht zur Vertretung der juristischen Person oder

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

c) einer Kontrollbefugnis innerhalb der juristischen Person

innehat, verantwortlich gemacht werden kann.

(2) Neben den in Absatz 1 vorgesehenen Fällen trifft jeder Mitgliedstaaten 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 der in den Artikeln 3, 4 und 5 genannten Straftaten zugunsten der juristischen Person durch eine ihr unterstellte Person ermöglicht hat.

(3) Die Verantwortlichkeit der juristischen Person nach den Absätzen 1 und 2 schließt die strafrechtliche Verfolgung natürlicher Personen, die sich Straftaten oder Verhaltensweisen nach den Artikeln 3, 4 und 5 schuldig machen, nicht aus.

Artikel 10

Sanktionen gegen juristische Personen

(1) Die Mitgliedstaaten stellen sicher, dass gegen eine im Sinne von Artikel 9 Absatz 1 verantwortliche juristische Person wirksame, verhältnismäßige und abschreckende Sanktionen verhängt werden können, zu denen Geldbußen oder Geldstrafen sowie andere Sanktionen gehören können, beispielsweise:

a) Ausschluss von öffentlichen Zuwendungen oder Hilfen;

b) vorübergehendes oder ständiges Verbot der Ausübung einer Handelstätigkeit;

c) richterliche Aufsicht; oder

d) richterlich angeordnete Eröffnung des Liquidationsverfahrens.

(2) Die Mitgliedstaaten stellen sicher, dass gegen eine im Sinne von Artikel 9 Absatz 2 verantwortliche juristische Person wirksame, verhältnismäßige und abschreckende Sanktionen oder Maßnahmen verhängt werden können.

Artikel 11

Gerichtliche Zuständigkeit

(1) Jeder Mitgliedstaat begründet seine Zuständigkeit für die in den Artikeln 3, 4 und 5 genannten Straftaten, sofern diese

a) ganz oder teilweise in seinem Hoheitsgebiet begangen wurden oder

b) von eigenen Staatsangehörigen begangen wurden und Einzelpersonen oder Gruppen dieses Staates betreffen; oder

c) zugunsten einer juristischen Personen begangen wurden, deren Hauptsitz sich im Hoheitsgebiet dieses Mitgliedstaates befindet.

(2) Bei der Begründung der Zuständigkeit gemäß Absatz 1 Buchstabe a) stellt jeder Mitgliedstaat sicher, dass sich diese auch auf Fälle erstreckt, in denen:

a) der Täter die strafbare Handlung begeht, während er sich physisch im Hoheitsgebiet dieses Staates aufhält, unabhängig davon, ob sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, oder

b) sich die Straftat gegen ein Informationssystem in seinem Hoheitsgebiet richtet, unabhängig davon, ob der Täter die strafbare Handlung begeht, während er sich physisch im Hoheitsgebiet dieses Staates aufhält.

(3) Ein Mitgliedstaat kann beschließen, die Zuständigkeitsregelung gemäß Absatz 1 Buchstabe b) und c) nicht, nur in besonderen Fällen oder nur unter besonderen Umständen anzuwenden.

(4) Jeder Mitgliedstaat ergreift zudem die erforderlichen Maßnahmen, um seine Zuständigkeit für die in den Artikeln 3 bis 5 genannten Straftaten in den Fällen zu begründen, in denen er es ablehnt, die einer derartigen Straftat verdächtigte oder überführte Person an einen anderen Mitgliedstaat oder an ein Drittland zu übergeben oder auszuliefern.

(5) Falls eine Straftat in die Zuständigkeit von mehreren Mitgliedstaaten fällt und jedes dieser Länder auf der Grundlage desselben Sachverhalts eine rechtsgültige Anklage erheben kann, so entscheiden diese Länder gemeinsam, welches von ihnen die Anklageerhebung gegen die Täter vornimmt, um das Verfahren nach Möglichkeit auf einen Mitgliedstaat zu konzentrieren. Zu diesem Zweck können die Mitgliedstaaten auf jedwedes Gremium und jedweden Mechanismus auf EU-Ebene zurückgreifen, um die Zusammenarbeit zwischen ihren Justizbehörden und die Koordinierung ihrer Maßnahmen zu erleichtern.

(6) Die Mitgliedstaaten setzen das Generalsekretariat des Rates und die Kommission über ihren Beschluss, Absatz 3 zur Anwendung zu bringen, in Kenntnis, wobei sie gegebenenfalls die betreffenden Fälle und Umstände nennen.

Artikel 12

Informationsaustausch

(1) Zum Zwecke des Informationsaustauschs über die in den Artikeln 3, 4 und 5 genannten Straftaten im Einklang mit den Datenschutzbestimmungen richten die Mitgliedstaaten operative Kontaktstellen ein, die rund um die Uhr und sieben Tage pro Woche erreichbar sind.

(2) Jeder Mitgliedstaat setzt das Generalsekretariat des Rates und die Kommission darüber in Kenntnis, welche Kontaktstelle für den Informationsaustausch über Straftaten im Zusammenhang mit Angriffen auf Informationssysteme benannt wurde. Das Generalsekretariat leitet diese Informationen an die übrigen Mitgliedstaaten weiter.

Artikel 13

Durchführung

(1) Die Mitgliedstaaten setzen die erforderlichen Maßnahmen in Kraft, um diesem Rahmenbeschluss bis spätestens 31. Dezember 2003 nachzukommen.

(2) Sie übermitteln dem Generalsekretariat des Rates und der Kommission den Wortlaut der von ihnen angenommenen Vorschriften sowie Informationen über sonstige von ihnen zur Umsetzung dieses Rahmenbeschlusses ergriffene Maßnahmen.

(3) Auf dieser Grundlage legt die Kommission dem Europäischen Parlament und dem Rat bis spätestens 31. Dezember 2004 einen Bericht über die Umsetzung dieses Rahmenbeschlusses einschließlich etwaiger erforderlicher Legislativvorschläge vor.

(4) Der Rat prüft, inwieweit die Mitgliedstaaten die erforderlichen Maßnahmen getroffen haben, um diesem Rahmenbeschluss nachzukommen.

Artikel 14

Inkrafttreten

Dieser Rahmenbeschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Gemeinschaften* in Kraft.