KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 19.04.2002
KOM(2002) 173 endgültig

2002/0086 (CNS)

Vorschlag für einen

# RAHMENBESCHLUSS DES RATES

## über Angriffe auf Informationssysteme

(von der Kommission vorgelegt)

# BEGRÜNDUNG

## 1. EINLEITUNG

Elektronische Kommunikationsnetze und Informationssysteme sind mittlerweile ein fester Bestandteil des Alltags der EU-Bürger und zudem von grundlegender Bedeutung für den Erfolg der EU-Wirtschaft. Netze und Informationssysteme wachsen zusammen und werden immer enger miteinander verknüpft. Neben zahlreichen konkreten Vorteilen hat diese Entwicklung auch eine besorgniserregende Bedrohung in Gestalt internationaler Angriffe auf Informationssysteme mit sich gebracht. Diese Angriffe können auf verschiedene Art erfolgen, beispielsweise durch unberechtigten Zugang, die Verbreitung bösartiger Software oder Angriffe auf Dienste. Derartige Angriffe können jederzeit von jedem Ort der Welt aus auf jeden Ort der Welt verübt werden, und es muss jederzeit mit neuen Angriffsformen gerechnet werden.

Die Angriffe auf Informationssysteme bedrohen auch den Erfolg der Anstrengungen zur Schaffung einer sichereren Informationsgesellschaft und eines Raumes der Freiheit, der Sicherheit und des Rechts und machen daher gezielte Gegenmaßnahmen auf EU-Ebene erforderlich. Ein Beitrag hierzu ist dieser Vorschlag der Kommission für einen Rahmenbeschluss über die Angleichung der einzelstaatlichen Strafrechtsvorschriften gegen Angriffe auf Informationssysteme.

### 1.1. Die verschiedenen Arten des Angriffs auf Informationssysteme

Der Begriff "Informationssystem" wird in diesem Vorschlag bewusst im weitest möglichen Sinne verwendet, um dem Zusammenwachsen der elektronischen Netze und der unterschiedlichen über sie verbundenen Systeme Rechnung zu tragen. Er schließt daher im folgenden PC, elektronische Organiser, Mobiltelefone, interne und externe Netze ebenso ein wie natürlich die Netze, Server und sonstigen Infrastrukturen des Internet.

In ihrer Mitteilung "Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz"[1] hat die Kommission nach folgenden Angriffsformen unterschieden:

**(a)** **Unberechtigter Zugang zu Informationssystemen**. Darunter fällt auch der Begriff "**Hacking**". Hacking bedeutet, sich unberechtigt Zugang zu einem Computer oder einem Computernetz zu verschaffen. Hacking kann auf unterschiedliche Art und Weise erfolgen, von der einfachen Nutzung von Insider-Informationen bis hin zu "Brute-Force"-Angriffen und dem Abfangen von Passwörtern. Häufig geschieht dies in der böswilligen Absicht, Daten zu kopieren, zu verändern oder zu zerstören. Der unberechtigte Zugriff kann auch darauf abstellen, Webseiten vorsätzlich zu korrumpieren oder sich Zugang zu zugangskontrollierten Diensten zu verschaffen, ohne dafür zu bezahlen.

**(b)** **Störung von Informationssystemen.** Die Möglichkeiten, Informationssysteme durch böswillige Angriffe zu stören, sind äußerst vielfältig. Eine der bekanntesten Möglichkeiten, die im Internet angebotenen Dienste zu blockieren oder anzugreifen,

---

[1] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, "Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz", KOM(2001)298 endg. vom 6.6.2001.

ist der "Denial of Service"-Angriff (vergleichbar mit einer Blockade eines Faxgerätes durch lange, wiederholte Nachrichten). Mit "Denial of Service"-Angriffen wird versucht, Web-Server oder Anbieter von Internetdiensten (ISP) mit automatisch erzeugten Nachrichten zu überlasten. Andere Angriffsformen sind beispielsweise die Störung von Servern, die das System der Bereichsnamen (DNS) betreiben, und Angriffe auf Router. Bestimmte bekannte Webseiten (z.B. Portale) haben durch derartige Störangriffe bereits schweren Schaden erlitten. Studien kamen zu dem Ergebnis, dass durch den jüngsten Angriff dieser Art außer dem nicht wertmäßig zu fassenden Image-Schaden ein Sachschaden in Höhe von mehreren hundert Millionen Euro entstanden ist. Die Unternehmen wickeln ihre Geschäfte in immer stärkerem Maße auch über ihre Webseiten ab, und Unternehmen, die das Internet für unmittelbare Lieferungen benötigen, sind mithin besonders anfällig.

**(c)** **Bösartige Software, die Daten verändert oder zerstört.** Die bekannteste Form bösartiger Software ist der Virus, wobei als besonders schädliche Beispiele die Viren "I Love You", "Melissa" und "Kournikova" zu nennen sind. Rund 11 % aller europäischen Internet-Nutzer hatten bereits einmal einen Virus auf ihrem PC zu Hause. Daneben gibt es noch andere Arten bösartiger Software. Manche dieser Programme schädigen den PC selbst, während andere den PC nur dazu benutzen, andere vernetzte Komponenten anzugreifen. Manche Programme (häufig als "logische Bomben" bezeichnet) "schlafen" so lange, bis sie durch ein Ereignis (wie etwa ein bestimmtes Datum) aktiviert werden und dann Daten verändern oder löschen und dadurch großen Schaden anrichten. Andere, auf den ersten Blick gutartige Programme lösen bei Aufruf bösartige Angriffe aus (daher die Bezeichnung "Trojanische Pferde"). Eine weitere Variante sind (häufig als "Würmer" bezeichnete) Programme, die im Gegensatz zu einem Virus nicht andere Programme infizieren, sondern sich selbst kopieren. Die Kopien kopieren sich immer weiter und überschwemmen so letztendlich das gesamte System.

**(d)** **Überwachung des Fernmeldeverkehrs**. Eine in böser Absicht vorgenommene Überwachung des Fernmeldeverkehrs gefährdet die von den Nutzern erwartete Vertraulichkeit und Integrität. Sie wird häufig auch als "Sniffing" (Schnüffeln) bezeichnet.

**(e)** **Täuschung/Irreführung des Benutzers ("malicious misrepresentation")**. Informationssysteme bieten neue Möglichkeiten der Täuschung und Irreführung. Die Annahme der Identität einer anderen Person im Internet und deren Nutzung in böswilliger Absicht wird häufig als "Spoofing" bezeichnet.

### 1.2. Art der Gefahr

Es besteht eindeutig die Notwendigkeit, zuverlässige Informationen über das Ausmaß und die Art der Angriffe auf Informationssysteme zusammenzutragen.

Einige der schwerwiegendsten Angriffe auf Informationssysteme richten sich gegen Betreiber elektronischer Kommunikationsnetze, gegen Anbieter von Diensten oder gegen Unternehmen, die elektronischen Geschäftsverkehr betreiben. Aufgrund der zunehmenden Vernetzung der modernen Kommunikationsmedien sind aber immer mehr auch die traditionellen Bereiche wie das verarbeitende Gewerbe, der Dienstleistungssektor, Krankenhäuser und sonstige öffentliche Einrichtungen sowie sogar Regierungsstellen verstärkt betroffen. Opfer der Angriffe sind jedoch nicht nur Organisationen; auch Einzelpersonen können unmittelbar und schwer geschädigt werden. Für öffentliche Einrichtungen, Unternehmen und Einzelpersonen

gleichermaßen bedeuten diese Angriffe mitunter eine beträchtliche wirtschaftliche Belastung, und es besteht die Gefahr, dass dadurch die Informationssysteme für die Nutzer teurer und schwerer erschwinglich werden.

Die vorstehend beschriebenen Angriffe werden häufig von allein agierenden Einzelpersonen verübt und zuweilen auch von Minderjährigen, die sich der Schwere ihrer Handlungen möglicherweise gar nicht bewusst sind. Es ist zu befürchten, dass diese Angriffe immer ausgeklügelter und dreister werden, und es wächst die Besorgnis, dass organisierte Straftäter Kommunikationsnetze für Angriffe gegen Informationssysteme zu eigenen Zwecken nutzen. Organisierte, auf Hacking und die Verunstaltung von Webseiten spezialisierte Hackergruppen werden zunehmend weltweit aktiv. Als Beispiele seien die brasilianischen Silver Lords und die pakistanische Gforce genannt, die versuchen, Geld von ihren Opfern zu erpressen, indem sie ihnen spezialisierte Unterstützung anbieten, nachdem sie in ihre Informationssysteme eingedrungen sind. Die Festnahme großer Gruppen von Hackern deutet darauf hin, dass das Hacking zunehmend zu einer Erscheinungsform der organisierten Kriminalität werden könnte. So hat es in jüngster Zeit zahlreiche raffinierte und organisierte Angriffe auf geistiges Eigentum gegeben sowie Versuche, erhebliche Summen im Rahmen von Bankdienstleistungen zu stehlen[2].

Weiteren Anlass zur Sorge geben Sicherheitsverletzungen an Datenbanken von elektronischen Geschäftsverkehr betreibenden Händlern, bei denen Zugriff auf Kundendaten einschließlich Kreditkartennummern genommen wird. Hierbei besteht in immer mehr Fällen die Gefahr von Zahlungsbetrug, und in jedem Fall sind die betreffenden Bankinstitute gezwungen, Tausende von Kreditkarten zu sperren und neu auszugeben. Eine weitere Folge derartiger Angriffe sind der wertmäßig nicht zu beziffernde Imageverlust des Händlers sowie das verlorene Vertrauen des Kunden in den elektronischen Handel. Im Rahmen des Aktionsplans zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln[3] werden gegenwärtig Präventivmassnahmen (z.B. Mindestsicherheitsanforderungen) für Online-Händler, die Bezahlkarten akzeptieren, erörtert.

Der vorliegende Vorschlag ist zudem Teil des Beitrags, mit dem die Kommission der Gefahr eines Terroranschlags auf lebenswichtige Informationssysteme in der Europäischen Union begegnen will. Er ergänzt die Vorschläge der Kommission, an die Stelle der Auslieferung innerhalb der Europäischen Union einen europäischen Haftbefehl zu setzen[4] und die Rechtsvorschriften zur Terrorismusbekämpfung anzugleichen[5] (hierüber wurde auf der Tagung des Europäischen Rates in Laeken vom 14./15. Dezember 2001 politische Einigung erzielt). Insgesamt wird durch diese Rechtsinstrumente gewährleistet, dass die EU-Mitgliedstaaten über wirksame strafrechtliche Bestimmungen zur Bekämpfung des

---

2 Laut einer Erhebung der Communications Management Association (CMA) war ein Drittel aller Großunternehmen und staatlichen Einrichtungen (darunter auch Regierungsstellen) Opfer von Hacking-Angriffen. Der dabei entstandene Schaden reichte von der Infiltrierung von Firmenkonten bis zum Datenraub (Ergebnisse siehe unter http://www.cma.org).

3 Mitteilung der Kommission an den Rat, das Europäische Parlament, die Europäische Zentralbank, den Wirtschafts- und Sozialausschuss und Europol zur Vorbeugung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln, KOM(2001) 11 endg., von der Kommission am 9.2.2001 angenommen.

4 Vorschlag für einen Rahmenbeschluss des Rates über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten, KOM(2001) 522 endg., von der Kommission am 19.9.2001 angenommen.

5 Vorschlag für einen Rahmenbeschluss des Rates zur Terrorismusbekämpfung, KOM(2001) 521 endg., von der Kommission am 19.9.2001 angenommen.

Cyberterrorismus verfügen und die internationale Zusammenarbeit im Kampf gegen den Terrorismus verbessert wird.

Der vorliegende Vorschlag bezieht sich nicht nur auf Angriffe gegen Informationssysteme in den Mitgliedstaaten, sondern auch auf Handlungen im Hoheitsgebiet der Europäischen Union, die sich gegen Informationssysteme im Gebiet von Drittländern richten. Er entspringt dem Willen der Kommission, derartige Angriffe auf globaler wie auch auf EU-Ebene zu bekämpfen.

In letzter Zeit kam es bereits mehrmals vor, dass die angespannten internationalen Beziehungen eine Serie von Angriffen auf Informationssysteme ausgelöst haben, die häufig auch mit Angriffen auf Webseiten verbunden waren. Schwere Angriffe können nicht nur erhebliche finanzielle Schäden verursachen, sondern sogar Menschenleben kosten (z.B. Angriffe auf Krankenhaussysteme oder Kontrollsysteme im Luftverkehr). Die Bedeutung, die die Mitgliedstaaten diesem internationalen Kampf beimessen, wird darin deutlich, dass zahlreiche Initiativen zum Schutz kritischer Infrastrukturen Priorität genießen. So wurde im Rahmen des IST-Programms der EU (Information Society Technologies)[6] unter Mitwirkung des US-Außenministeriums eine gemeinsame Taskforce der Gemeinschaft und der Vereinigten Staaten zum Thema Schutz kritischer Infrastrukturen eingerichtet[7].

### 1.3. Bedarf an genauen Informationen und Statistiken

Über das volle Ausmaß der Computerkriminalität liegen nur wenige verlässliche Statistiken vor. Die Zahl der bisher aufgedeckten und gemeldeten Übergriffe dürfte das wahre Ausmaß des Problems eher verschleiern. Einer amerikanischen Untersuchung zufolge[8] haben im Jahre 1999 nur 32 % der Befragten, auf deren Computer im Vorjahr unbefugt Zugriff genommen wurde, diese Zugriffe den Strafverfolgungsbehörden gemeldet. Immerhin war dies bereits ein Fortschritt im Vergleich zu den Vorjahren, als lediglich 17 % der Fälle gemeldet worden waren. Die Gründe, keine Anzeige zu erstatten, waren vielfältig. Aufgrund begrenzter Vorsicht und Erfahrung der Systemverwalter und Nutzer werden viele Eindringversuche gar nicht bemerkt. Zudem melden viele Unternehmen Fälle von Computermissbrauch nicht, um kein schlechtes Bild in der Öffentlichkeit abzugeben und um ihre Anfälligkeit für weitere Angriffe nicht publik werden zu lassen. Viele Polizeidienste führen keine Statistik über die Verwendung von Computern und Kommunikationssystemen für Straftaten[9]. Den Strafverfolgungsbehörden mangelt es zudem an der entsprechenden Ausbildung, um Computerkriminalität aufzudecken, als solche zu erkennen und aufzuklären. Die Europäische Union hat sich inzwischen dieser Frage angenommen und Zahlen über Angriffe auf Informationssysteme erhoben. In einem Mitgliedstaat fanden Schätzungen zufolge im Jahre 1999 30.000 bis 40.000 Angriffe auf Informationssysteme statt, während offiziell nur

---

6 Das IST-Programm der Europäischen Kommission ist Teil des Fünften Rahmenprogramms, das von 1998 bis 2002 läuft. Weitere Informationen sind unter der Adresse http://www.cordis.lu/ist erhältlich.

7 Unter Federführung der gemeinsamen Beratungsgruppe im Rahmen des zwischen der EG und den Vereinigten Staaten geschlossenen Abkommens über die Zusammenarbeit in Wissenschaft und Technik.

8 Das Computer Security Institute (CSI) und das Federal Bureau of Investigation (FBI) veröffentlichen alljährlich im Frühjahr die Ergebnisse der von ihnen durchgeführten Erhebung über Computerkriminalität und -sicherheit (Computer Crime and Security Survey). Einzelheiten der Erhebung sind auch über die Webseiten des CSI (http://www.gocsi.com/) zugänglich.

9 Das italienische Innenministerium hat unlängst Statistiken über seine operativen Maßnahmen zur Bekämpfung der Computerkriminalität in den Jahren 1999 und 2000 veröffentlicht (http://www.mininterno.it/dip_ps/dcpsffp/index.htm). Demnach wurden im Jahr 2000 insgesamt 98 Fälle von Hacking verzeichnet; dies war mehr als das Vierfache des Vorjahres (21 Fälle).

105 Fälle verzeichnet wurden. Im Jahre 1999 wurde in sieben Mitgliedstaaten insgesamt nur in 1.844 Fällen offiziell Anzeige wegen Straftaten gegen Informationssysteme und Computerdaten erstattet. Dies ist allerdings bereits das Zweifache der im Jahre 1998 genannten Zahl, als lediglich 972 Fälle in sieben Mitgliedstaaten offiziell zu Protokoll gegeben wurden[10].

Eine unlängst durchgeführte Umfrage[11] hat ferner ergeben, dass 13 % der Unternehmen, die einem Wirtschaftsverbrechen zum Opfer fielen, angegeben haben, dass es sich bei einer dieser Straftaten auch um Computerkriminalität gehandelt habe. Aus der Umfrage geht weiter hervor, dass die Computerkriminalität zunehmend Anlass zur Sorge gibt, da 43 % der Befragten die Computerkriminalität für eine große Gefahr der Zukunft halten. Eine andere Studie gelangte zu dem Schluss, dass im Bereich der Computerkriminalität Hacker und Viren inzwischen die größte Bedrohung für Organisationen darstellen, wobei Hacker mit 45 % die größte Tätergruppe darstellen, gefolgt von ehemaligen Mitarbeitern (13 %), organisierten Kriminellen (13 %) und den derzeitigen Beschäftigten (11 %)[12]. Es kann davon ausgegangen werden, dass diese Zahlen weiter steigen, da der Einsatz von Informationssystemen und die Vernetzung immer größere Ausmaße annehmen und die Bereitschaft, Angriffe anzuzeigen, zunimmt. Gleichwohl ist es dringend erforderlich, den Mitgliedstaaten ein Werkzeug zur Aufstellung einschlägiger Statistiken an die Hand zu geben, damit die Computerkriminalität in der Europäischen Union quantitativ und qualitativ erfasst werden kann. Ausgangspunkt für eine solche Analyse ist eine gemeinsame Definition der mit Angriffen auf Informationssysteme verbundenen Straftaten auf EU-Ebene.

### 1.4. Die einschlägige Politik der Europäischen Union

Der Europäische Rat hat auf seiner Tagung in Lissabon im März 2000 die Bedeutung des Übergangs zu einer wettbewerbsfähigen, dynamischen und wissensbasierenden Wirtschaft unterstrichen und Rat und Kommission ersucht, einen Aktionsplan ("*e*Europe") aufzustellen, um diesen Umstand optimal zu nutzen[13]. Der Aktionsplan, der von Kommission und Rat erstellt und auf dem Gipfeltreffen des Europäischen Rates in Feira im Juni 2000 angenommen wurde, umfasst Maßnahmen zur Verbesserung der Sicherheit von Netzen und zur Entwicklung eines koordinierten und einheitlichen Ansatzes zur Bekämpfung der Computerkriminalität bis Ende 2002.

Im Rahmen ihres Beitrags zur Bekämpfung der Computerkriminalität hat die Kommission die Mitteilung "Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität" vorgelegt[14]. Darin wird ein ausgewogenes Konzept zur Lösung der durch Computerkriminalität bedingten Probleme vorgeschlagen, das den Standpunkten aller Beteiligten (Strafverfolgungsbehörden, Anbieter von Diensten, Netzbetreiber, andere Gruppen aus der Industrie, Verbrauchergruppen, Datenschutzbehörden, Gruppen zum Schutz der Privatsphäre usw.) uneingeschränkt Rechnung trägt. Ferner wurde in der Mitteilung eine Reihe legislativer und nichtlegislativer Initiativen vorgeschlagen.

---

10 Ratsdokument 8123/01 ENFOPOL 38, verfügbar über die Webseiten des Rats (http://db.consilium.eu.int/jai).

11 "European Economic Crime Survey 2001", PricewaterhouseCoopers (http://www.pwcglobal.com/).

12 "The Cybercrime Survey 2001", Confederation of British Industry (http://www.cbi.org.uk)

13 Schlussfolgerungen des Vorsitzes des Europäischen Rats von Lissabon (23. und 24. März 2000), abrufbar unter der Adresse http://ue.eu.int/de/Info/eurocouncil/index.htm.

14 KOM (2000) 890 endg..

Ein wichtiges Beispiel für die laufenden Maßnahmen ist das IDA-Programm, in dessen Rahmen die Mitgliedstaaten und die Kommission mit der Ausarbeitung einer gemeinsamen Sicherheitspolitik und dem Aufbau eines sicheren Netzes für den Informationsaustausch zwischen den Verwaltungen befasst sind.

Eine der Kernfragen, mit denen sich die Mitteilung befasste, war der Bedarf an wirksamen Maßnahmen zur Bekämpfung der Gefahren für die Authentizität, Integrität, Vertraulichkeit und Verfügbarkeit von Informationssystemen und Netzen. Im Bereich des Gemeinschaftsrechts ist auf diesem Gebiet bereits vieles erreicht worden. So bestehen bereits Rechtsinstrumente auf Gemeinschaftsebene, die von besonderer Bedeutung für die Sicherheit von Netzen und Informationen sind.

Dieser Rahmenbeschluss ergänzt die geltenden Gemeinschaftsvorschriften zum Schutz von Informationssystemen (u.a. Richtlinie 95/46/EG, Richtlinie 97/66/EG und Richtlinie 98/84/EG über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten). Insbesondere sehen die europäischen Telekommunikations- und Datenschutzrichtlinien (Richtlinien 95/46/EG und 97/66/EG[15]) vor, dass die Anbieter von öffentlich zugänglichen Telekommunikationsdiensten entsprechende technische und organisatorische Maßnahmen zu treffen haben, um die Sicherheit und Vertraulichkeit ihrer Dienste zu schützen, und diese Maßnahmen ein dem Risiko entsprechendes Maß an Sicherheit gewährleisten müssen.

Am besten und wirksamsten lassen sich diese Probleme auf dem Wege der Prävention und Aufklärung lösen. Daher wird in der Mitteilung die Bedeutung unterstrichen, die der Verfügbarkeit, der Entwicklung, dem Einsatz und der wirksamen Nutzung präventiver Technologien zukommt. Dabei wird hervorgehoben, dass das öffentliche Bewusstsein für die Risiken in Verbindung mit der Computerkriminalität geschärft, bewährte Praktiken für die Sicherheit im IT-Bereich gefördert, wirksame Werkzeuge und Verfahren zur Bekämpfung der Computerkriminalität entwickelt und die Weiterentwicklung von Frühwarn- und Krisenmanagementsystemen gefördert werden müssen. Das IST-Programm der EU[16] legt die Rahmenbedingungen für die Entwicklung der Kompetenzen und Technologien fest, die notwendig sind, um die neuen Herausforderungen der Computerkriminalität nachvollziehen und damit umgehen zu können.

Der Europäische Rat hat auf seiner Tagung in Stockholm am 23. und 24. März 2001 die Notwendigkeit weiterer Maßnahmen im Bereich der Sicherheit von Netzen und Informationen anerkannt und den Schluss gezogen, dass *"der Rat in Zusammenarbeit mit der Kommission eine umfassende Strategie für die Sicherheit elektronischer Netze einschließlich praktischer Durchführungsmaßnahmen entwickeln"* wird. *"Diese Strategie sollte rechtzeitig für die Tagung des Europäischen Rates in Göteborg vorliegen"*. Die Kommission ist dieser Aufforderung mit ihrer Mitteilung "Sicherheit der Netzwerke und Informationen: Vorschlag für einen europäischen Politikansatz"[17] nachgekommen. Darin werden die derzeitigen Probleme in Verbindung mit der Sicherheit der Netze untersucht und eine Strategie für einschlägige Maßnahmen entworfen. Des weiteren nahm der Rat am 6. Dezember 2001 eine Entschließung zu einem gemeinsamen Ansatz und spezifischen Maßnahmen im Bereich der Netz- und Informationssicherheit an.

---

15 ABl. L 281 vom 23.11.1995, S. 31-50 sowie ABl. L 24 vom 30.1.1998, S. 1-8.

16 Das IST-Programm der Europäischen Kommission ist Teil des Fünften Rahmenprogramms, das von 1998 bis 2002 läuft. Weitere Informationen sind unter der Adresse http://www.cordis.lu/ist erhältlich.

17 KOM(2001)298 endg. vom 6. Juni 2001

Diese Initiativen reichen allein jedoch nicht aus, um schwerwiegenden Angriffen auf Informationssysteme angemessen begegnen zu können. In beiden Mitteilungen der Kommission wird darauf hingewiesen, dass, was Angriffe auf Informationssysteme anbelangt, das materielle Strafrecht in der Europäischen Union dringend angeglichen werden muss. Dies entspricht auch den Schlussfolgerungen des Gipfeltreffens des Europäischen Rates in Tampere im Oktober 1999[18], denen zufolge die High-Tech-Kriminalität als Teil einer begrenzten Liste von Bereichen gilt, in denen man sich auf gemeinsame Definitionen, Tatbestandsmerkmale und Sanktionen verständigen muss; zudem wurde dieses Thema in der Empfehlung 7 der Strategie 2000 der Europäischen Union für den Beginn des neuen Jahrtausends zur Prävention und Bekämpfung der organisierten Kriminalität (vom Rat der Justiz- und Innenminister im März 2000 angenommen[19]) aufgegriffen. Dieser Vorschlag für einen Rahmenbeschluss ist auch Teil des Arbeitsprogramms der Kommission für das Jahr 2001[20] und des Anzeigers der Fortschritte bei der Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts, den die Kommission am 30. Oktober 2001 aktualisiert hat[21].

### 1.5. Die erforderliche Angleichung des Strafrechts

Die einschlägigen Rechtsvorschriften der Mitgliedstaaten weisen erhebliche Unterschiede und Diskrepanzen auf, die den Kampf gegen die organisierte Kriminalität und den Terrorismus sowie schwere Angriffe auf Informationssysteme durch Einzelpersonen erschweren könnten. Mit der Angleichung des materiellen Rechts im Bereich der High-Tech-Kriminalität soll gewährleistet werden, dass die einzelstaatlichen Rechtsvorschriften so umfassend sind, dass alle Formen schwerwiegender Angriffe auf Informationssysteme mit Hilfe der nach dem Strafrecht verfügbaren Techniken und Methoden aufgeklärt werden können. Die Verantwortlichen dieser Straftaten müssen ermittelt und vor Gericht gestellt werden, und die Gerichte müssen angemessene Strafen verhängen können. Auf diese Weise wird eine hohe abschreckende Wirkung auf potenzielle Angreifer auf Informationssysteme erzielt.

Die rechtlichen Unterschiede und Diskrepanzen könnten sich zudem als ein Hindernis für eine wirksame polizeiliche und justizielle Zusammenarbeit bei Angriffen auf Informationssysteme erweisen. Schwerwiegende Angriffe auf Informationssysteme sind häufig grenzüberschreitender Natur und erfordern somit eine polizeiliche und justizielle Zusammenarbeit auf internationaler Ebene. Durch die Angleichung der Rechtsvorschriften wird der Grundsatz der beiderseitigen Strafbarkeit (wonach eine Handlung in beiden Ländern einen Straftatbestand darstellen muss, bevor die gegenseitige Rechtshilfe bei strafrechtlichen Ermittlungen erfolgen kann) gewährleistet. Dadurch verbessert sich die Zusammenarbeit sowohl zwischen den EU-Mitgliedstaaten als auch zwischen diesen und Drittländern (sofern entsprechende Rechtshilfeabkommen bestehen).

Ferner ist es erforderlich, die bestehenden Instrumente auf EU-Ebene zu ergänzen. Die Bezugnahmen auf die Computerkriminalität im Rahmenbeschluss über den Europäischen Haftbefehl[22], im Anhang zum Europol-Übereinkommen[23] und im Beschluss des Rates über

---

18 Siehe http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

19 "Prävention und Bekämpfung der organisierten Kriminalität - Eine Strategie der Europäischen Union für den Beginn des neuen Jahrtausends" (ABl. C 124 vom 3.5.2000).

20 http://europa.eu.int/comm/off/work_programme/index_de.htm

21 Siehe http://europa.eu.int/comm/dgs/justice_home/pdf/scoreboard_30oct01_de.pdf

22 ABl. C ...

23 Rechtsakt des Rates vom 26. Juli 1995 über die Fertigstellung des Übereinkommens aufgrund von Artikel K.3 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts (Europol-Übereinkommen), ABl. C 316 vom 27.11.1995, S.1.

die Einrichtung von Eurojust[24] 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[25], der u.a. auch Terrorhandlungen abdeckt, die weit reichende Zerstörungen von Infrastruktureinrichtungen (wie eben Informationssysteme) verursachen und dadurch menschliches Leben gefährden oder großen wirtschaftlichen Schaden anrichten können.

### 1.6. Anwendungsbereich und Zweck des vorgeschlagenen Rahmenbeschlusses

Ziel dieses Rahmenbeschluss des Rates ist die Angleichung der Strafrechtsvorschriften in Bezug auf Angriffe auf Informationssysteme sowie die Gewährleistung einer optimalen polizeilichen und justiziellen Zusammenarbeit bei Straftaten im Zusammenhang mit Angriffen auf Informationssysteme. Der Beschluss ist ein Beitrag zu den Anstrengungen der Europäischen Union bei der Bekämpfung der organisierten Kriminalität und des Terrorismus. Er stellt nicht darauf ab, die Mitgliedstaaten zu verpflichten, geringfügige oder Bagatelldelikte unter Strafe zu stellen.

Aus Artikel 47 EU-Vertrag geht eindeutig hervor, dass dieser Rahmenbeschluss das Gemeinschaftsrecht unberührt lässt. Er berührt insbesondere nicht die Rechte und Pflichten in Bezug auf den Schutz der Privatsphäre oder auf den Datenschutz laut Definition in den einschlägigen Gemeinschaftsvorschriften (wie den Richtlinien 95/46 und 97/66). Von den Mitgliedstaaten soll nicht verlangt werden, dass sie Verstöße gegen die Bestimmungen über den Zugang zu bzw. die Offenlegung von personenbezogenen Daten, die Vertraulichkeit des Datenverkehrs, die Sicherheit der Verarbeitung personenbezogener Daten, elektronische Signaturen[26] oder Verstöße gegen das geistige Eigentum unter Strafe stellen, und der Rahmenbeschluss berührt auch nicht die Richtlinie 98/84/EG über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten[27]. Diese wichtigen Aspekte sind bereits durch das geltende Gemeinschaftsrecht geregelt. Eine den Zielen der Gemeinschaftsvorschriften entsprechende Angleichung der einzelstaatlichen Strafrechtsvorschriften für Bereiche wie den Schutz personenbezogener Daten, den Schutz geistigen Eigentums oder die Bezahlung von zugangskontrollierten Diensten ist daher nicht vor dem Hintergrund von Titel VI EU-Vertrag, sondern vielmehr auf der Grundlage des geltenden Gemeinschaftsrechts ins Auge zu fassen. Aus diesen Gründen beschränkt sich dieser Rahmenbeschluss auf die unter Punkt a) bis c) in Teil 1.1 beschriebenen Handlungen.

Legislativmaßnahmen auf EU-Ebene müssen zudem den Entwicklungen in anderen internationalen Foren Rechnung tragen. Die größten Fortschritte im Hinblick auf eine Angleichung des materiellen Strafrechts in Bezug auf Angriffe auf Informationssysteme hat bislang der Europarat erzielt. Er nahm im Februar 1997 die Arbeiten am Entwurf eines internationalen Übereinkommens zur Bekämpfung der Internet-Kriminalität auf. Das Übereinkommen ist im November 2001 formell angenommen und zur Unterzeichnung

---

[24] ABl. C ...

[25] ABl. C ...

[26] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. L 13 vom 19.1.2000).

[27] ABl. L 320 vom 28.11.1998, S. 54-57.

aufgelegt worden[28]. In dem Übereinkommen wird der Versuch unternommen, eine Reihe von strafbaren Handlungen einschließlich Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen und Daten anzugleichen. In Bezug auf derartige Straftaten verfolgt der vorliegende Rahmenbeschluss das gleiche Konzept wie das Übereinkommen des Europarates.

Bei den Gesprächen der G8 über die High-Tech-Kriminalität wurden zwei Hauptgefahren ermittelt: zum einen die Gefährdung von Computerinfrastrukturen durch den Versuch, die in Computern und Computernetzen gespeicherten Informationen bzw. die Computer und Netze selbst zu stören, zu blockieren, zu verstümmeln oder zu zerstören, sowie zum anderen der Versuch, mit Hilfe des Computers bösartige und durch den Einsatz des Computers erleichterte Handlungen wie Täuschung und Irreführung, Geldwäsche, Kinderpornografie, Verstöße gegen geistige Eigentumsrechte sowie Drogenhandel zu begehen. Dieser Vorschlag beschäftigt sich mit der ersten Gefahrenkategorie.

Eine Angleichung auf EU-Ebene sollte auch den Entwicklungen in den internationalen Foren Rechnung tragen und mit der derzeitigen Gemeinschaftspolitik in Einklang stehen. Der vorliegende Vorschlag versucht ferner, eine stärkere Angleichung innerhalb der EU herbeizuführen, als dies bisher in anderen internationalen Foren möglich war.

## 2. RECHTSGRUNDLAGE

Das Ziel des Aufbaus eines Raumes der Freiheit, der Sicherheit und des Rechts muss über die Prävention und Bekämpfung der organisierten und sonstigen Kriminalität einschließlich des Terrorismus durch eine engere Zusammenarbeit zwischen den Strafverfolgungs- und den Justizbehörden in den Mitgliedstaaten sowie eine Angleichung der einzelstaatlichen Strafrechtsvorschriften erreicht werden. Dieser Vorschlag für einen Rahmenbeschluss zielt daher auf eine Angleichung der Rechtsvorschriften der Mitgliedstaaten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen ab. Er erstreckt sich auf "Mindestvorschriften über die Tatbestandsmerkmale strafbarer Handlungen" insbesondere in den Bereichen organisierte Kriminalität und Terrorismus. Er setzt auch "die Gewährleistung der Vereinbarkeit der jeweils geltenden Vorschriften der Mitgliedstaaten untereinander" voraus, durch die die Zusammenarbeit zwischen den Justizbehörden erleichtert und beschleunigt werden soll. Die in der Präambel des Vorschlags genannte Rechtsgrundlage bilden daher die Artikel 29, 30 Absatz 1 Buchstabe a), 31 sowie 34 Absatz 2 Buchstabe b) EU-Vertrag. Der Vorschlag hat keine finanziellen Auswirkungen auf den Haushaltsplan der Europäischen Gemeinschaften.

## 3. DER RAHMENBESCHLUSS: DIE ARTIKEL

### Artikel 1 - Anwendungsbereich und Zweck des Rahmenbeschlusses

In diesem Artikel heißt es ausdrücklich, dass mit diesem Rahmenbeschluss das Strafrecht im Bereich schwerwiegender Angriffe auf Informationssysteme angeglichen und insbesondere ein Beitrag zur Bekämpfung der organisierten Kriminalität und des Terrorismus geleistet werden soll, um eine optimale justizielle Zusammenarbeit bei Straftaten in Verbindung mit Angriffen auf Informationssysteme zu gewährleisten. Auch lässt der Rahmenbeschluss das

---

[28] Der Text ist im Internet in Französisch (http://conventions.coe.int/treaty/fr/projets/cybercrime.htm) und in Englisch (http://conventions.coe.int/treaty/en/projets/cybercrime.htm) abrufbar.

Gemeinschaftsrecht in Übereinstimmung mit Artikel 47 EU-Vertrag unberührt. Dies gilt insbesondere für die in den Richtlinien 95/46 und 97/66 vorgesehenen Rechte und Pflichten in Bezug auf den Schutz der Privatsphäre und den Datenschutz. Es ist nicht beabsichtigt, dass die Mitgliedstaaten Verstöße gegen Vorschriften über den Zugang zu bzw. die Offenlegung von personenbezogenen Daten, die Vertraulichkeit des Datenverkehrs, die Sicherheit der Verarbeitung personenbezogener Daten, elektronische Signaturen[29] oder Verstöße gegen das geistige Eigentum unter Strafe stellen sollen, und der Rahmenbeschluss berührt auch nicht die Richtlinie 98/84/EG über den rechtlichen Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten[30].

Die Mitgliedstaaten sollen in diesem Rahmenbeschluss nicht dazu verpflichtet werden, geringfügige oder Bagatelldelikte unter Strafe zu stellen. In den Artikeln 3 und 4 werden die Kriterien für die Erfüllung des Straftatbestands festgelegt. Für sie gelten die im Entwurf des Übereinkommens über Computerkriminalität des Europarats genannten Ausnahme- und Vorbehaltsmöglichkeiten.

Dieser Rahmenbeschluss bezieht sich ausschließlich auf Straftaten, die vorsätzlich begangen werden. Der Begriff "vorsätzlich" wird in den Artikeln 3, 4 und 5 ausdrücklich verwendet. Er ist gemäß den üblichen strafrechtlichen Grundsätzen der Mitgliedstaaten in Bezug auf den Begriff "Vorsatz" auszulegen. Folglich sieht der Rahmenbeschluss auch nicht vor, dass Handlungen unter Strafe gestellt werden sollen, die grob fahrlässig oder leichtfertig, aber eben ohne Vorsatz begangen werden. Dabei reicht bereits das Vorliegen des allgemeinen Vorsatzes des widerrechtlichen Zugriffs auf bzw. Eingriffs in Informationssysteme aus, und es ist nicht erforderlich, nachzuweisen, dass sich dieser Vorsatz auf ein spezielles Informationssystem bezog.

**Artikel 2 - Begriffsbestimmungen**

Der vorgeschlagene Rahmenbeschluss des Rates enthält folgende Begriffsbestimmungen:

(a) "*Elektronisches Kommunikationsnetz*": Diese Definition entspricht der Definition in der Richtlinie des Europäischen Parlaments und des Rates über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste vom 14. Februar 2002[31].

(b) "*Computer*": Diese Definition beruht auf Artikel 1 des Entwurfs des Übereinkommens des Europarates über Computerkriminalität. Die Definition erstreckt sich beispielsweise auch auf Einzelplatz-PC, persönliche digitale Organiser, digitale Set-top Boxen, Videorekorder und Mobiltelefone (sofern diese über Datenverarbeitungsfunktionen verfügen, z.B. WAP und dritte Generation), für die die Definition elektronischer Kommunikationsnetze alleine nicht umfassend genug wäre.

(c) "*Computerdaten*": Diese Definition beruht auf der ISO[32]-Definition des Begriffs "Daten". Daten in gegenständlicher Form (beispielsweise als Buch) sollen nicht unter

---

29 Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. L 13 vom 19.1.2000).

30 ABl. L 320 vom 28.11.1998, S. 54-57.

31 http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/03672d1.pdf

32 Der Internationale Normenausschuss (ISO) ist ein weltweit tätiger Verband nationaler Normungsgremien aus rund 100 Ländern.

diese Definition fallen, wohl aber Bücher, die in Form von Computerdaten (z.B. elektronisch als Textverarbeitungsdatei) gespeichert werden oder elektronisch eingelesen und in Computerdaten umgewandelt wurden. Daher wird in der Definition ausdrücklich darauf hingewiesen, dass die betreffenden Computerdaten "erzeugt oder in eine Form gebracht werden" müssen, die für die Verarbeitung in einem Informationssystem oder zur Bewirkung einer Funktion in einem Informationssystem geeignet ist.

(d) "*Informationssystem*": Die Definition von Informationssystemen stammt ursprünglich aus der diesbezüglichen Definition in den Leitlinien der OECD für die Sicherheit von Informationssystemen aus dem Jahre 1992 sowie aus den vorangegangenen Definitionen für elektronische Kommunikationsnetze, Computer und Computerdaten. Der Begriff wurde auch früher schon in gemeinschaftlichen Rechtsakten verwendet, etwa im Beschluss des Rates vom 31. März 1992 "auf dem Gebiet der Sicherheit von Informationssystemen" und in der Empfehlung des Rates vom 7. April 1995 "über gemeinsame Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik". Er soll in technischer Hinsicht neutral sein und das Konzept miteinander verbundener Netze und Systeme, die Daten enthalten, genau widerspiegeln. Der Begriff erstreckt sich auf die Hardware und die Software des Systems, jedoch nicht auf den Inhalt der Information. Auch eigenständig operierende Systeme fallen darunter. Die Kommission hält es für wünschenswert, den durch das Strafrecht gewährten Schutz auch auf Einzelplatz-Computer zu erweitern und ihn nicht nur auf vernetzte Systeme zu beschränken.

(e) "*Juristische Person*": Dabei handelt es sich um eine übliche, früheren Rahmenbeschlüssen des Rates entnommene Definition.

(f) "*Befugte Personen*": Dieser Begriff bezeichnet Personen, die vertraglich oder kraft des 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 im Einklang mit diesem Recht bzw. mit dieser Erlaubnis handeln. Hierunter fallen auch Personen, die aufgrund einer rechtmäßigen Einwilligung einer Person handeln, die diese Genehmigung ausdrücklich erteilt hat. Besonders wichtig ist, dass folgende Kategorien von Personen und rechtlich zulässigen Tätigkeiten (im Rahmen der Rechte, Erlaubnisse und Zuständigkeiten der betreffenden Person sowie nach dem Gemeinschaftsrecht über Datenschutz und Vertraulichkeit des Datenverkehrs) bei der Umsetzung dieses Rahmenbeschlusses in nationales Recht nicht unter Strafe gestellt werden:

— Handlungen gewöhnlicher privater oder geschäftlicher Nutzer einschließlich der Verwendung von Verschlüsselungen zum Schutz ihrer Nachrichten und Daten;

— "reverse engineering" im Rahmen der Richtlinie 91/250 des Rates vom 14. Mai 1991 über den Rechtsschutz von Computerprogrammen[33];

— Handlungen von Verantwortlichen, Aufsichtspersonen sowie Netz- oder Systembetreibern;

---

33 ABl. L 122 vom 17.5.1991, S. 42-46.

— Handlungen unternehmensinterner oder extern ernannter Zugangsberechtigter, die die Erlaubnis besitzen, die Sicherheit eines Systems zu testen;

— rechtlich zulässige wissenschaftliche Forschung.

(g) "*Unrechtmäßig*": Dies ist ein recht allgemeiner Begriff, der es den Mitgliedstaaten erlaubt, den Tatbestand mehr oder weniger weit zu fassen. Um jedoch die Umsetzung des Rahmenbeschlusses des Rates in nationales Recht zu fördern, ist die Kommission der Auffassung, dass ausdrücklich angegeben werden muss, dass bestimmte Aktivitäten den Tatbestand nicht erfüllen. So ist es nicht möglich und vermutlich auch nicht erstrebenswert, eine umfassende, ausschließliche Liste von Ausnahmen auf EU-Ebene zu erstellen. Der Begriff "unrechtmäßig" beruht jedoch auf den vorangegangenen Definitionen, wonach Handlungen befugter Personen ausgeschlossen sind. Ausgeschlossen sind ferner Handlungen, die nach nationalem Recht rechtmäßig sind, einschließlich der üblichen Verteidigung vor Gericht und anderer, nach nationalem Recht anerkannter Befugnisse.

**Artikel 3 - Rechtswidriger Zugang zu Informationssystemen**

Dieser Straftatbestand umfasst den rechtswidrigen Zugang zu Informationssystemen einschließlich des "Hacking". Den Mitgliedstaaten ist freigestellt, bei der Umsetzung des Rahmenbeschlusses in nationales Recht geringfügige oder Bagatelldelikte aus dem Straftatbestand auszunehmen.

Der von den Mitgliedstaaten einzuführende Straftatbestand muss sich lediglich darauf erstrecken, dass das betreffende Delikt

(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.

Obwohl die Kommission bereits seit langem darauf hinweist, wie wichtig wirksame technische Maßnahmen zum Schutz von Informationssystemen sind, schützt sich bedauerlicherweise die Mehrheit der Nutzer noch immer nicht ausreichend (oder überhaupt nicht) mit technischen Mitteln vor etwaigen Angriffen. Zur Abschreckung von Angriffen auf diese Nutzer ist es erforderlich, den unbefugten Zugang zu ihren Systemen auch für den Fall zu regeln, dass kein entsprechender technischer Schutz vorhanden ist. Unter der Voraussetzung, daß der Angriff mit der Absicht erfolgt, einen Schaden oder einen wirtschaftlichen Vorteil zu bewirken, sieht die Definition dieser Straftat daher nicht das Erfordernis vor, dass zu ihrer Begehung Sicherheitsmaßnahmen überwunden werden müssen.

**Artikel 4 - Rechtswidriger Eingriff in Informationssysteme**

Unter diesen Straftatbestand fallen folgende mit Vorsatz begangene unrechtmäßige Handlungen:

(a) die schwere, unrechtmäßig herbeigeführte Behinderung oder Störung des Betriebs eines Informationssystems durch Eingabe, Übermittlung, Beschädigung, Löschung, Verstümmelung, Veränderung oder Unterdrückung von Computerdaten. Die

Erwähnung der Eingabe und der Ermittlung erfolgt vor allem im Hinblick auf das Problem der "Denial of Service"-Angriffe, bei denen vorsätzlich der Versuch unternommen wird, ein Informationssystem zu überlasten. Der Begriff "Störung" ließe sich zwar aus dem Begriff "Behinderung" ableiten, wird jedoch der Klarheit halber ausdrücklich in der Definition des Tatbestands genannt. Die anderen Tatbestandsmerkmale (Beschädigung, Löschung, Verstümmelung, Veränderung oder Unterdrückung von Computerdaten) beziehen sich insbesondere auf Viren- und sonstige Angriffe, die den Betrieb des Informationssystems als solchen behindern oder stören sollen;

(b) die unrechtmäßige Löschung, Verstümmelung, Veränderung, Unterdrückung oder Blockierung von Computerdaten eines Informationssystems, sofern dies in der Absicht erfolgt, einer natürlichen oder einer juristischen Person Schaden zuzufügen. Hierunter fallen Virenangriffe auf den Inhalt (bzw. die Computerdaten) eines Informationssystems sowie die Korrumpierung von Webseiten.

In Absatz (a) wird die Bezeichnung "schwere Behinderung oder Störung" als ein Tatbestandsmerkmal verwendet, um die Auswirkungen eines solchen Angriffs zu beschreiben. Die Bedeutung der Bezeichnung "schwere Behinderung" wird nicht definiert, da eine Behinderung unterschiedliche Formen annehmen und ihr Ausmaß je nach Art des Angriffs und den technischen Kapazitäten des angegriffenen Informationssystems unterschiedlich sein kann. Jeder Mitgliedstaat legt für sich fest, welche Kriterien erfüllt sein müssen, damit eine "schwere Behinderung" eines Informationssystems vorliegt. Allerdings sollten geringfügige Störungen oder Beeinträchtigungen des Betriebs nicht als schwerwiegend eingestuft werden.

Wie bereits ausgeführt, können die Mitgliedstaaten bei der Umsetzung des Rahmenbeschlusses in nationales Recht geringfügige oder Bagatelldelikte aus dem Straftatbestand ausnehmen.

**Artikel 5 - Anstiftung, Beihilfe und Versuch**

Artikel 5 Absatz 1 verpflichtet die Mitgliedstaaten, dafür Sorge zu tragen, dass die Anstiftung oder Beihilfe zur Begehung der in Artikel 3 und 4 beschriebenen Straftaten gegen Informationssysteme unter Strafe gestellt werden.

Artikel 5 Absatz 2 bezieht sich konkret auf den Versuch. Er verpflichtet die Mitgliedstaaten, dafür Sorge zu tragen, dass der Versuch, eine der in Artikel 3 und 4 beschriebenen Straftaten gegen Informationssysteme zu begehen, unter Strafe gestellt wird.

**Artikel 6 – Strafen**

Absatz 1 verpflichtet die Mitgliedstaaten, die erforderlichen Maßnahmen zu treffen, damit die in Artikel 3 bis 5 definierten Straftaten durch wirksame, verhältnismäßige und abschreckende Strafe geahndet werden können[34].

Aufgrund dieses Absatzes sind die Mitgliedstaaten verpflichtet, Strafen festzusetzen, die der Schwere der Straftat entsprechen; darunter fallen auch Freiheitsstrafen im Höchstmaß von

[34] Dieser Satz stammt aus dem Urteil, das der Europäische Gerichtshof am 21. September 1989 in der Rechtssache 68/88 [1989] (Slg. 2965) fällte.

mindestens einem Jahr in schweren Fällen. Fälle, in denen durch die betreffende Handlung kein Schaden oder wirtschaftlicher Vorteil bewirkt wurde, gelten nicht als schwere Fälle.

Mit dem Höchststrafmaß von mindestens einem Jahr Gefängnis in schweren Fällen fallen diese Straftaten in den Anwendungsbereich des Rahmenbeschlusses des Rates über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten sowie von weiteren Rechtsinstrumenten wie dem Rahmenbeschluss des Rates vom 26. Juni 2001[35] über Geldwäsche sowie Ermittlung, Einfrieren, Beschlagnahme und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten.

In Übereinstimmung mit der Eigenschaft von Rahmenbeschlüssen, dass diese für die Mitgliedstaaten zwar hinsichtlich der Zielvorgabe verbindlich sind, ihnen jedoch die Wahl der Form und der Mittel überlassen, verfügen die Mitgliedstaaten - innerhalb der im Rahmenbeschluss vorgegeben Grenzen und insbesondere in Bezug auf die erschwerenden Umstände nach Artikel 7 - über einen gewissen Spielraum bei der Anpassung ihrer Rechtsvorschriften an diese Bestimmungen und insbesondere bei der Festlegung der Strafen. So bleibt es den Mitgliedstaaten vorbehalten, die Kriterien, die bei der Bestimmung der Schwere einer Straftat zugrunde gelegt werden, nach ihrem innerstaatlichen Recht festzulegen.

Die Ahndung wiederum muss nicht unbedingt in Form einer Freiheitsstrafe erfolgen: Nach Absatz 2 haben die Mitgliedstaaten die Möglichkeit, ihren Traditionen und Rechtsordnungen entsprechend zusätzlich zu oder anstelle von Freiheitsstrafen Geldstrafen vorzusehen.

**Artikel 7 - Erschwerende Umstände**

Dieser Artikel sieht vor, dass die Mitgliedstaaten unter bestimmten Umständen die in Artikel 6 definierten Strafen verschärfen können. Die Kommission weist darauf hin, dass die in diesem Artikel vorgenommene Auflistung erschwerender Umstände etwaige sonstige, nach den Rechtsvorschriften der Mitgliedstaaten als erschwerend geltende Umstände unberührt lässt. Die Auflistung berücksichtigt die in den nationalen Rechtsvorschriften der Mitgliedstaaten beschriebenen und in früheren Vorschlägen der Kommission für Rahmenbeschlüsse festgelegten erschwerenden Umstände.

Ist eine der nachstehend genannten, in Absatz 1 aufgeführten Voraussetzungen erfüllt, beträgt das Höchstmaß der Freiheitsstrafe mindestens vier Jahre:

(a) die Straftat wurde im Rahmen einer kriminellen Vereinigung gemäß Definition in der Gemeinsamen Maßnahme 98/733 JI 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 körperlichen Schaden zugefügt oder ein Teil der kritischen Infrastruktur des Mitgliedstaates erheblich beschädigt; oder

---

[35] ABl. L 182 vom 5.7.2001, S.1.
ABl. C 316 vom 27.11.1995.
ABl. L 105 vom 27.4.1996.
ABl. L 191 vom 7.7.1998.
ABl. L 324 vom 21.12.2000.

(c) durch die Straftat wurden erhebliche Erträge erzielt.

Die Mitgliedstaaten müssen zudem sicherstellen, dass Straftaten nach Artikel 3, 4 und 5 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**

Dieser Artikel bezieht sich auf Umstände, bei deren Vorliegen ein Mitgliedstaat die in Artikel 6 und 7 genannten Strafen herabsetzen kann, wenn der Täter nach Auffassung der zuständigen Justizbehörde nur geringfügigen Schaden verursacht hat.

**Artikel 9 - Verantwortlichkeit juristischer Personen**

Im Einklang mit dem Ansatz, der mit mehreren auf EU-Ebene zur Bekämpfung der verschiedenen Arten von Kriminalität eingeführten Rechtsinstrumenten verfolgt wird, müssen auch die Situationen erfasst werden, in denen juristische Personen an Angriffen auf Informationssysteme beteiligt sind. Daher sieht Artikel 9 vor, dass sich juristische Personen für in den Artikeln 3, 4 und 5 beschriebene Straftaten zu verantworten haben, die zu ihren Gunsten von einer Person begangen wurde, die eine Führungsposition innehat und die entweder allein oder als Teil eines Organs der juristischen Person gehandelt hat. Der Begriff "Verantwortlichkeit" ist so auszulegen, dass er sowohl die zivil- als auch die strafrechtliche Haftung einschließt.

Gemäß dem üblichen Verfahren bestimmt Absatz 2 außerdem, dass eine juristische Person auch dann verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle seitens einer dafür zuständigen Person die Begehung einer Straftat zu Gunsten der juristischen Person ermöglicht hat. Absatz 3 besagt, dass ein Verfahren gegen eine juristische Person ein gleichzeitiges Verfahren gegen eine natürliche Person nicht ausschließt.

**Artikel 10 - Sanktionen gegen juristische Personen**

In Artikel 10 wird aufgezeigt, welche Sanktionen gegen juristische Personen, die für die in den Artikeln 3, 4 und 5 beschriebenen Straftaten verantwortlich gemacht werden, verhängt werden können. Der Artikel sieht wirksame, verhältnismäßige und abschreckende Strafen vor, bei denen es sich mindestens um Geldbußen oder Geldstrafen handeln muss. Darüber hinaus werden weitere Strafen aufgeführt, die üblicherweise für juristische Personen in Betracht kommen.

**Artikel 11 - Gerichtliche Zuständigkeit**

Aufgrund des internationalen Charakters von Straftaten im Zusammenhang mit Angriffen auf Informationssysteme setzt ein wirksames rechtliches Vorgehen Verfahrensvorschriften für die gerichtliche Zuständigkeit und die Auslieferung voraus, die so eindeutig und auf EU-Ebene so weitreichend sein müssen, dass die Straftäter sich der Strafverfolgung nicht entziehen können.

In Absatz 1 werden Kriterien zur Begründung der gerichtlichen Zuständigkeit für die Ermittlung und strafrechtliche Verfolgung der in diesem Rahmenbeschluss genannten Straftaten aufgeführt. Ein Mitgliedstaat begründet seine Zuständigkeit, wenn eine der drei folgenden Situationen vorliegt:

(a) Die Straftat wurde ganz oder teilweise in seinem Hoheitsgebiet begangen, wobei die Rechtsstellung oder die Staatsangehörigkeit der beteiligten natürlichen Person unerheblich ist (Territorialitätsprinzip);

(b) der Straftäter ist Staatsangehöriger dieses Mitgliedstaates (Täterprinzip), und Einzelpersonen oder Gruppen dieses Staates sind von der Tat betroffen. Mitgliedstaaten, die keine Auslieferungsregelungen treffen, sind für die Verfolgung eigenen Staatsangehöriger, die im Ausland Straftaten begangen haben, verantwortlich;

(c) die Straftat wurde zu Gunsten einer juristischen Person begangen, die ihren Sitz im Hoheitsgebiet des betreffenden Mitgliedstaats hat.

Mit Absatz 2 soll gewährleistet werden, dass jeder Mitgliedstaat bei der Begründung seiner Zuständigkeit für Straftaten aufgrund des Territorialitätsprinzips nach Absatz 1 Buchstabe a) dafür Sorge trägt, dass er auch für Fälle zuständig ist, 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 - Beispiel: eine Person verschafft sich vom Hoheitsgebiet des Mitgliedstaates aus unberechtigten Zugang (durch Hacking) zu einem Informationssystem in einem Drittland; 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 - Beispiel: eine Person verschafft sich vom Hoheitsgebiet eines Drittlandes aus unberechtigten Zugang (durch Hacking) zu einem Informationssystem im Hoheitsgebiet des Mitgliedstaates.

Da das Prinzip der extraterritorialen Zuständigkeit aufgrund der Rechtstradition nicht in allen Mitgliedstaaten für alle Arten von Straftaten anerkannt wird, bietet Absatz 3 diesen Mitgliedstaaten die Möglichkeit, ihre gerichtliche Zuständigkeit gemäß Absatz 1 in Situationen, die unter Absatz 1 Buchstabe b) und c) fallen, nicht anzuwenden.

Absatz 4 sieht vor, daß jeder Mitgliedstaat zudem die erforderlichen Maßnahmen ergreift, 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.

Absatz 5 bezieht sich auf Fälle, die in die Zuständigkeit von mehreren Mitgliedstaaten fallen. Er stellt darauf ab, daß die Mitgliedstaaten umfassend zusammenarbeiten, um Gerichtsverfahren 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. Dies würde auch Eurojust und das Europäische justizielle Netz einschließen.

Absatz 6 besagt, dass die Mitgliedstaaten das Generalsekretariat des Rates und der Kommission über ihre Entscheidung, Absatz 3 zur Anwendung zu bringen, unterrichten müssen.

**Artikel 12 – Informationsaustausch**

Artikel 12 soll den Informationsaustausch erleichtern, indem vorgesehen wird, dass operative Kontaktstellen einzurichten sind. Für eine effiziente polizeiliche Zusammenarbeit ist dies von großer Bedeutung. So wurde auf der Tagung des Rates der Justiz- und Innenminister am 19. März 1998 sowie unlängst bei der Annahme einer Empfehlung des Rates über Kontaktstellen mit einem rund um die Uhr erreichbaren Dauerdienst zur Bekämpfung der Hightech-Kriminalität[36] insbesondere anerkannt, dass alle Mitgliedstaaten sich dem Kontaktstellennetz der G8 anschließen sollten.

**Artikel 13 - Durchführung**

Artikel 13 betrifft die Durchführung dieses Rahmenbeschlusses und die Folgemaßnahmen.

Die Mitgliedstaten müssen die erforderlichen Maßnahmen treffen, um diesem Rahmenbeschluss bis spätestens 31. Dezember 2003 nachzukommen.

Die Mitgliedstaaten müssen dem Generalsekretariat des Rates und der Kommission zum selben Termin die Vorschriften übermitteln, mit denen sie ihre Verpflichtungen aus diesem Rahmenbeschluss in nationales Recht umsetzen. Anhand dieser Angaben und eines schriftlichen Berichts der Kommission prüft der Rat binnen eines Jahres, inwieweit die Mitgliedstaaten ihren Verpflichtungen aus dem Rahmenbeschluss nachgekommen sind.

**Artikel 14 – Inkrafttreten**

Artikel 14 besagt, dass der Rahmenbeschluss am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Gemeinschaften* in Kraft tritt.

---

[36] ABl. C 187 vom 3.7.2001, S. 5.

2002/0086 (CNS)

Vorschlag für einen

# RAHMENBESCHLUSS DES RATES

## über Angriffe auf Informationssysteme

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[1],

nach Stellungnahme des Europäischen Parlaments[2],

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"[3] 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[4] 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

---

1 ABl. C ..., S. ...

2 ABl. C ..., S. ...

3 KOM (2001) 298.

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

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[5], 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[6] und das Europäische Parlament in seiner Entschließung vom 19. Mai 2000[7] 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"[8] 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.

(8) Die Bezugnahmen auf die Computerkriminalität im Rahmenbeschluss über den Europäischen Haftbefehl[9], 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[10], 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

---

5 ABl. C 19 vom 23.1.1999.
6 KOM (2001) 278 endg.
7 A5-0127/2000.
8 KOM (2000) 890.
9 ABl. C ...
10 ABl. C ...

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[11].

(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.

---

[11] ABl. L 351 vom 29.12.1998, S. 1.

(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.

*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. 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. 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 körperlichen 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.

Geschehen zu Brüssel am

Im Namen des Rates
Der Präsident