Voorstel voor een kaderbesluit van de Raad over aanvallen op informatiesystemen

(2002/C 203 E/16)

COM(2002) 173 def. — 2002/0086(CNS)

(Door de Commissie ingediend op 19 april 2002)

DE RAAD VAN DE EUROPESE UNIE,

Gelet op het Verdrag betreffende de Europese Unie, en met name op artikel 29, artikel 30, lid 1, onder a), artikel 31 en artikel 34, lid 2, onder b),

Gezien het voorstel van de Commissie,

Gezien het advies van het Europees Parlement,

Overwegende hetgeen volgt:

(1) Er zijn gegevens die wijzen op aanvallen op informatiesystemen, in het bijzonder als gevolg van de dreiging van de georganiseerde criminaliteit, en de bezorgdheid over mogelijke terroristische aanvallen op informatiesystemen die deel uitmaken van de kritische infrastructuur van de lidstaten neemt toe. Dit vormt een bedreiging voor de totstandbrenging van een veiligere informatiemaatschappij en een ruimte van vrijheid, veiligheid en rechtvaardigheid, en derhalve is een reactie op het niveau van de Europese Unie noodzakelijk.

(2) Teneinde doeltreffend op deze bedreigingen te kunnen reageren, is een allesomvattende aanpak van de netwerk- en informatieveiligheid vereist, zoals is onderstreept in het Actieplan eEurope, in de mededeling van de Commissie „Netwerk- en informatieveiligheid: voorstel voor een Europese beleidsaanpak" ([1]) en in de Resolutie van de Raad van 6 december 2001 betreffende een gemeenschappelijke aanpak en specifieke acties inzake netwerk- en informatiebeveiliging.

(3) De noodzaak om meer bekendheid te geven aan de problemen in verband met informatieveiligheid en praktische bijstand te verlenen, is ook onderstreept in de resolutie van het Europees Parlement van 5 september 2001 ([2]).

([1]) COM(2001) 298.

([2]) (2001/2098(INI)).

(4) Een aantal grote lacunes en verschillen in de wetgeving van de lidstaten op dit gebied vormen een belemmering voor de bestrijding van georganiseerde criminaliteit en staan een doeltreffende politiële en justitiële samenwerking op het gebied van aanvallen op informatiesystemen in de weg. Het transnationale en grensoverschrijdende karakter van moderne elektronische communicatienetwerken houdt in dat aanvallen op informatiesystemen steeds vaker internationaal van aard zijn, waardoor wordt onderstreept dat er dringend behoefte bestaat aan verdere onderlinge afstemming van het strafrecht op dit gebied.

(5) In het actieplan van de Raad en de Commissie over hoe de bepalingen van het Verdrag van Amsterdam inzake de totstandbrenging van een ruimte van vrijheid, veiligheid en rechtvaardigheid het best kunnen worden uitgevoerd ([3]), in de conclusies van de Europese Raad van Tampere van 15 en 16 oktober 1999, in de conclusies van de Europese Raad van Santa Maria da Feira van 19 en 20 juni 2000, in het scorebord van de Commissie ([4]) en in de resolutie van het Europees Parlement van 19 mei 2000 ([5]) zijn wetgevende maatregelen ter bestrijding van hightech-criminaliteit, waaronder gemeenschappelijke definities, strafbaarstellingen en straffen, aangegeven of wordt op dergelijke maatregelen aangedrongen.

(6) De door internationale organisaties verrichte werkzaamheden, in het bijzonder die van de Raad van Europa met het oog op de onderlinge afstemming van het strafrecht en die van de G8 met het oog op transnationale samenwerking op het gebied van hightech-criminaliteit moeten worden aangevuld met een gemeenschappelijke aanpak in de Europese Unie op dit gebied. De oproep daartoe is nader uitgewerkt in de mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's „De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden" ([6]).

(7) Er moet worden gezorgd voor een betere onderlinge afstemming van het strafrecht op het gebied van aanvallen op informatiesystemen teneinde een optimale politiële en justitiële samenwerking te garanderen op het gebied van strafbare feiten waarvan sprake is bij aanvallen op informatiesystemen en teneinde bij te dragen aan de bestrijding van de georganiseerde criminaliteit en terrorisme.

([3]) PB C 19 van 23.1.1999.

([4]) COM (2001) 278 def.

([5]) A5-0127/2000.

([6]) COM(2000) 890.

(8) Het kaderbesluit van de Raad inzake het Europees arrestatiebevel, de bijlage bij de Europol-Overeenkomst en het besluit van de Raad betreffende de oprichting van Eurojust bevatten verwijzingen naar computercriminaliteit, die nader moet worden omschreven. Met het oog op dergelijke instrumenten moet computercriminaliteit worden verstaan in die zin dat deze ook aanvallen op informatiesystemen omvat zoals deze zijn gedefinieerd in dit kaderbesluit, dat zal zorgen voor een veel verdergaande onderlinge afstemming van de bestanddelen van dergelijke strafbare feiten. Dit kaderbesluit vult ook het kaderbesluit inzake de bestrijding van terrorisme aan, dat betrekking heeft op terroristische handelingen waardoor grootschalige vernielingen aan een infrastructurele voorziening, inclusief een informatiesysteem, worden aangebracht, het leven van mensen in gevaar kan worden gebracht of grote economische schade kan worden veroorzaakt.

(9) Alle lidstaten hebben het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens geratificeerd. De persoonsgegevens die worden verwerkt in het kader van de tenuitvoerlegging van dit kaderbesluit, worden beschermd overeenkomstig de beginselen van genoemd Verdrag.

(10) Gemeenschappelijke definities op dit gebied, in het bijzonder van informatiesystemen en computergegevens, zijn van belang om in de lidstaten bij de toepassing van dit kaderbesluit een coherente aanpak te garanderen.

(11) Teneinde tot een gemeenschappelijke aanpak van de bestanddelen van strafbare feiten te komen, moet voor een gemeenschappelijke definitie van onrechtmatige toegang tot een informatiesysteem en van onrechtmatige verstoring van een informatiesysteem worden gezorgd.

(12) Er moet worden voorkomen dat met name gedragingen te zwaar worden bestraft en dat handelingen van houders van rechten en bevoegde personen — zoals rechtmatige particuliere of zakelijke gebruikers, beheerders, controleurs en exploitanten van netwerken en systemen, personen die rechtmatig wetenschappelijk onderzoek verrichten en bevoegde personen die een systeem testen, ongeacht of het om een persoon binnen de onderneming gaat of dat daartoe een externe persoon wordt aangewezen die wordt gemachtigd de beveiliging van een systeem te testen — strafbaar worden gesteld.

(13) De lidstaten zorgen ervoor dat aanvallen op informatiesystemen strafbaar worden gesteld met doeltreffende, evenredige en afschrikkende straffen, die in ernstige gevallen ook vrijheidsstraffen kunnen omvatten.

(14) Voor gevallen waarin bepaalde, met een aanval op een informatiesysteem samengaande omstandigheden ertoe leiden dat deze een nog grotere bedreiging voor de samenleving vormt, moet in zwaardere straffen worden voorzien. In dergelijke gevallen moeten de aan de daders opgelegde straffen volstaan om aanvallen op informatiesystemen te bestrijden binnen de strekking van andere instrumenten die reeds werden goedgekeurd met het oog op de bestrijding van de georganiseerde misdaad, zoals Gemeenschappelijk optreden 98/733/JBZ van 21 december 1998 door de Raad aangenomen op grond van artikel K.3 van het Verdrag betreffende de Europese Unie inzake de strafbaarstelling van deelneming aan een criminele organisatie in de lidstaten van de Europese Unie ([1]).

(15) Er moeten maatregelen worden genomen om het mogelijk te maken dat rechtspersonen aansprakelijk worden gesteld voor strafbare feiten in de zin van dit kaderbesluit die te hunnen voordele zijn gepleegd, en om er voor te zorgen dat elke lidstaat in situaties waarin de dader fysiek op zijn grondgebied aanwezig is of waarin het informatiesysteem zich op zijn grondgebied bevindt, bevoegd is voor ten aanzien van informatiesystemen gepleegde strafbare feiten.

(16) Er moeten ook maatregelen worden genomen met het oog op de samenwerking tussen de lidstaten teneinde een doeltreffend optreden tegen aanvallen op informatiesystemen mogelijk te maken. Er moeten operationele meldpunten worden ingesteld voor de uitwisseling van informatie.

(17) Omdat de doelstellingen om aanvallen op informatiesystemen in alle lidstaten te bestraffen met doeltreffende, evenredige en afschrikkende straffen en om de justitiële samenwerking te verbeteren en te bevorderen door mogelijke belemmeringen weg te nemen, niet in voldoende mate door de lidstaten afzonderlijk kunnen worden verwezenlijkt omdat de regels gemeenschappelijk en met elkaar verenigbaar moeten zijn, en deze doelstellingen dus beter op het niveau van de Unie kunnen worden verwezenlijkt, kan de Unie maatregelen nemen, overeenkomstig het in artikel 2 van het Verdrag betreffende de EU en artikel 5 van het EG-Verdrag omschreven subsidiariteitsbeginsel. Overeenkomstig het eveneens in artikel 5 van het EG-Verdrag omschreven evenredigheidsbeginsel gaat dit kaderbesluit niet verder dan wat nodig is om deze doelstellingen te verwezenlijken.

(18) Dit kaderbesluit laat de bevoegdheden van de Europese Gemeenschap onverlet.

(19) In dit kaderbesluit worden de grondrechten in acht genomen en de beginselen nageleefd die in het bijzonder zijn vastgelegd in het Handvest van de grondrechten van de Europese Unie, met name in de hoofdstukken II en VI,

HEEFT HET VOLGENDE KADERBESLUIT VASTGESTELD:

Artikel 1

Werkingssfeer en doelstelling van het kaderbesluit

Dit kaderbesluit heeft ten doel de samenwerking tussen de justitiële en andere bevoegde autoriteiten van de lidstaten, zoals de politie en andere gespecialiseerde rechtshandhavingsinstanties, te verbeteren door middel van de onderlinge afstemming van de strafrechtelijke regels van de lidstaten inzake aanvallen op informatiesystemen.

([1]) PB L 351 van 29.12.1998, blz. 1.

Artikel 2

Definities

In de zin van dit kaderbesluit gelden de volgende definities:

a) „Elektronisch communicatienetwerk": de transmissiesystemen en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele terrestrische netwerken, netten voor radio- en televisieomroep en kabeltelevisienetten, ongeacht de aard van de overgebrachte informatie.

b) „Computer": elk apparaat of groep van onderling verbonden of met elkaar verband houdende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerkt.

c) „Computergegevens": elke weergave van feiten, gegevens of begrippen die is gemaakt of omgezet in een vorm die geschikt is voor verwerking in een informatiesysteem, met inbegrip van programma's die een informatiesysteem een bepaalde functie kunnen laten uitvoeren.

d) „Informatiesysteem": computers en elektronische communicatienetwerken, alsmede de computergegevens die daarmee worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

e) „Rechtspersoon": ieder lichaam dat deze hoedanigheid krachtens het toepasselijke recht bezit, met uitzondering van staten of andere overheidslichamen in de uitoefening van hun openbaar gezag en van publiekrechtelijke internationale organisaties.

f) „Bevoegde persoon": elke natuurlijke of rechtspersoon die contractueel of wettelijk het recht heeft, of de rechtmatige toestemming, om een informatiesysteem te gebruiken, te beheren, te controleren, te testen, er rechtmatig wetenschappelijk onderzoek mee te doen of op een andere manier te exploiteren, en die in overeenstemming met dat recht of die toestemming handelt.

g) „Onrechtmatig" betekent dat gedragingen door bevoegde personen of andere gedragingen die in het nationale recht als rechtmatig worden erkend, zijn uitgesloten.

Artikel 3

Onrechtmatige toegang tot informatiesystemen

De lidstaten zorgen ervoor dat de opzettelijke, onrechtmatige toegang tot een informatiesysteem of enig onderdeel daarvan, strafbaar wordt gesteld indien het feit is gepleegd:

i) tegen een deel van een informatiesysteem waarvoor specifieke beveiligingsmaatregelen gelden; of

ii) met het oogmerk een natuurlijke of een rechtspersoon schade te berokkenen; of

iii) met het oogmerk economisch voordeel tot gevolg te hebben.

Artikel 4

Onrechtmatige verstoring van informatiesystemen

De lidstaten zorgen ervoor dat de volgende opzettelijke, onrechtmatige gedragingen strafbaar worden gesteld:

a) het ernstig hinderen of onderbreken van de werking van een informatiesysteem door de invoer, de transmissie, het beschadigen, wissen, verminken, wijzigen, onderdrukken of ontoegankelijk maken van computergegevens;

b) het wissen, verminken, wijzigen, onderdrukken of ontoegankelijk maken van computergegevens in een informatiesysteem met het oogmerk om een natuurlijke of een rechtspersoon schade te berokkenen.

Artikel 5

Instigatie, hulp, aanstoking en poging

1. De lidstaten zorgen ervoor dat de opzettelijke instigatie of aanstoking tot of hulp bij de feiten in de zin van de artikelen 3 en 4 strafbaar wordt gesteld.

2. De lidstaten zorgen ervoor dat pogingen om de feiten in de zin van de artikelen 3 en 4 te plegen, strafbaar worden gesteld.

Artikel 6

Straffen

1. De lidstaten zorgen ervoor dat de strafbare feiten in de zin van de artikelen 3, 4 en 5 strafbaar worden gesteld met doeltreffende, evenredige en afschrikkende straffen, waaronder maximumgevangenisstraffen die in ernstige gevallen ten minste een jaar moeten bedragen. Het begrip „ernstige gevallen" moet aldus worden opgevat dat gedragingen die geen schade of economisch voordeel ten gevolge hebben gehad daar niet onder vallen.

2. De lidstaten zorgen ervoor dat naast vrijheidsstraffen bijkomende of alternatieve straffen in de vorm van boetes kunnen worden opgelegd.

Artikel 7

Verzwarende omstandigheden

1. De lidstaten zorgen ervoor dat op de strafbare feiten in de zin van de artikelen 3, 4 en 5 een maximumgevangenisstraf staat van niet minder dan vier jaar wanneer deze in de volgende omstandigheden zijn gepleegd:

a) indien het strafbare feit werd gepleegd in het kader van een criminele organisatie in de zin van Gemeenschappelijk optreden 98/733/JBZ van 21 december 1998 inzake de strafbaarstelling van deelneming aan een criminele organisatie in de lidstaten van de Europese Unie, afgezien van het daarin aangegeven strafniveau;

b) indien door het het strafbare feit rechtstreeks of onrechtstreeks aanzienlijke economische schade of lichamelijk letsel werd toegebracht of aanzienlijke schade aan een deel van de kritische infrastructuur van de lidstaat werd veroorzaakt;

c) indien door het strafbare feit aanzienlijke opbrengsten werden verkregen.

2. De lidstaten zorgen ervoor dat op de strafbare feiten in de zin van de artikelen 3, 4 en 5 zwaardere vrijheidsstraffen staan dan die waarin artikel 6 voorziet, indien tegen de dader in een lidstaat voor een dergelijk strafbaar feit een eindvonnis is uitgesproken.

Artikel 8

Bijzondere omstandigheden

Onverminderd de artikelen 6 en 7, zorgen de lidstaten ervoor dat de in de artikelen 6 en 7 bedoelde straffen kunnen worden verlicht indien de dader naar de mening van de bevoegde justitiële autoriteit slechts onbeduidende schade heeft veroorzaakt.

Artikel 9

Aansprakelijkheid van rechtspersonen

1. De lidstaten zorgen ervoor dat rechtspersonen aansprakelijke kunnen worden gesteld voor gedragingen in de zin van de artikelen 3, 4 en 5, waaraan zich te hunnen voordele personen schuldig maken die hetzij individueel, hetzij als lid van een orgaan van de rechtspersoon handelen en die in die rechtspersoon een leidende functie bekleden op grond van:

a) de bevoegdheid om de rechtspersoon te vertegenwoordigen; of

b) de bevoegdheid om namens de rechtspersoon beslissingen te nemen; of

c) de bevoegdheid om binnen de rechtspersoon toezicht uit te oefenen.

2. Afgezien van de in lid 1 genoemde gevallen, zorgen de lidstaten ervoor dat de rechtspersoon aansprakelijk kan worden gesteld wanneer, bij gebreke van toezicht of controle door een in lid 1 bedoelde persoon, strafbare feiten in de zin van de artikelen 3, 4 en 5 konden worden gepleegd ten voordele van die rechtspersoon door een onder het gezag van die rechtspersoon staande persoon.

3. De aansprakelijkheid van een rechtspersoon krachtens de leden 1 en 2 sluit strafvervolging van natuurlijke personen die strafbare feiten plegen of zich schuldig maken aan gedragingen in de zin van de artikelen 3, 4 en 5 niet uit.

Artikel 10

Straffen tegen rechtspersonen

1. De lidstaten zorgen ervoor dat een rechtspersoon die volgens artikel 9, lid 1, aansprakelijk is, straffen kunnen worden opgelegd die doeltreffend, evenredig en afschrikkend zijn. Deze straffen omvatten al dan niet strafrechtelijke geldboetes en kunnen andere maatregelen omvatten zoals:

a) uitsluiting van uitkeringen of steun van de overheid;

b) tijdelijk of permanent verbod op het uitoefenen van commerciële activiteiten;

c) plaatsing onder toezicht van de rechter; of

d) een gerechtelijk bevel tot liquidatie.

2. De lidstaten zorgen ervoor dat tegen een rechtspersoon die volgens artikel 9, lid 2, aansprakelijk is, straffen kunnen worden vastgesteld of maatregelen kunnen worden getroffen die doeltreffend, evenredig en afschrikkend zijn.

Artikel 11

Rechtsmacht

1. Elke lidstaat vestigt zijn rechtsmacht ten aanzien van de strafbare feiten als bedoeld in de zin van de artikelen 3, 4 en 5 indien deze:

a) geheel of gedeeltelijk op zijn grondgebied zijn gepleegd; of

b) door een van zijn onderdanen zijn gepleegd en de handeling is gericht tegen personen of groepen uit die staat; of

c) zijn gepleegd ten voordele van een rechtspersoon die zijn hoofdkantoor op het grondgebied van die lidstaat heeft.

2. Bij het vestigen van de rechtsmacht overeenkomstig lid 1, onder a), zorgt elke lidstaat ervoor dat zijn rechtsmacht zich uitstrekt tot gevallen waarin:

a) de dader het strafbare feit pleegt terwijl hij zich fysiek op het grondgebied van die lidstaat bevindt, ongeacht of het strafbare feit is gericht tegen een informatiesysteem op het eigen grondgebied; of

b) het strafbare feit is gericht tegen een informatiesysteem op het eigen grondgebied, ongeacht of de dader het strafbare feit pleegt terwijl hij zich fysiek op het grondgebied van de betrokken lidstaat bevindt.

3. Elke lidstaat kan besluiten de in lid 1, onder b) en c), beschreven regels inzake de rechtsmacht niet of slechts in specifieke gevallen of omstandigheden toe te passen.

4. Elke lidstaat neemt de nodige maatregelen om zijn rechtsmacht ook te vestigen voor de strafbare feiten in de zin van de artikelen 3, 4 en 5 in gevallen waarin hij weigert een persoon die van een dergelijk strafbaar feit wordt verdacht of daaraan schuldig is bevonden aan een andere lidstaat of een derde land over te dragen of uit te leveren.

5. Indien een strafbaar feit onder de rechtsmacht van meer dan een lidstaat valt en indien elk van de betrokken lidstaten geldig vervolging kan instellen op grond van hetzelfde feit, werken de betrokken lidstaten samen om te beslissen wie van hen de daders zal vervolgen, teneinde de procedure zo mogelijk in een enkele lidstaat te centraliseren. Daartoe kunnen de lidstaten een beroep doen op elk orgaan of mechanisme dat in de Europese Unie is ingesteld om de samenwerking tussen hun rechterlijke instanties en de coördinatie van hun actie te vergemakkelijken.

6. De lidstaten stellen het Secretariaat-generaal van de Raad en de Commissie op de hoogte wanneer zij besluiten lid 3 toe te passen, zo nodig onder vermelding van de specifieke gevallen of omstandigheden waarin het besluit van toepassing is.

Artikel 12

Uitwisseling van informatie

1. Met het oog op de uitwisseling van informatie in verband met strafbare feiten in de zin van de artikelen 3, 4 en 5, stellen de lidstaten, met inachtneming van de regels inzake gegevensbescherming, operationele meldpunten in die 24 uur per dag en zeven dagen per week operationeel zijn.

2. Elke lidstaat stelt het Secretariaat-generaal van de Raad en de Commissie in kennis van het meldpunt dat is aangewezen met het oog op de uitwisseling van informatie over strafbare feiten waarvan sprake is bij aanvallen op informatiesystemen. Het Secretariaat-generaal brengt deze informatie ter kennis van de andere lidstaten.

Artikel 13

Tenuitvoerlegging

1. De lidstaten treffen de noodzakelijke maatregelen om uiterlijk op 31 december 2003 aan dit kaderbesluit te voldoen.

2. Zij stellen het Secretariaat-generaal van de Raad en de Commissie in kennis van de tekst van de bepalingen die zij goedkeuren, alsmede van eventuele andere maatregelen die zij nemen om aan dit kaderbesluit te voldoen.

3. Op basis daarvan dient de Commissie uiterlijk op 31 december 2004 bij het Europees Parlement en de Raad een verslag in over de werking van dit kaderbesluit, zo nodig vergezeld van wetgevingsvoorstellen.

4. De Raad beoordeelt in hoeverre de lidstaten aan dit kaderbesluit voldoen.

Artikel 14

Inwerkingtreding

Dit kaderbesluit treedt in werking op de twintigste dag na de bekendmaking ervan in het *Publicatieblad van de Europese Gemeenschappen*.