(Besluiten aangenomen krachtens titel VI van het Verdrag betreffende de Europese Unie)

KADERBESLUIT 2005/222/JBZ VAN DE RAAD

van 24 februari 2005

over aanvallen op informatiesystemen

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, lid 1, onder e), en artikel 34, lid 2, onder b),

Gezien het voorstel van de Commissie,

Gezien het advies van het Europees Parlement [1],

Overwegende hetgeen volgt:

(1) Dit kaderbesluit heeft ten doel de samenwerking tussen 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 bepalingen van de lidstaten inzake aanvallen op informatiesystemen.

(2) 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 veiliger informatiemaatschappij en een ruimte van vrijheid, veiligheid en rechtvaardigheid en derhalve is een reactie op het niveau van de Europese Unie noodzakelijk.

(3) Teneinde doeltreffend op deze bedreigingen te kunnen reageren, is een integrale aanpak van de netwerk- en informatieveiligheid vereist, zoals is onderstreept in het actieplan e-Europa, in de mededeling van de Commissie „Netwerk- en informatieveiligheid: voorstel voor een Europese beleidsaanpak" en in de resolutie van de Raad van 28 januari 2002 betreffende een gemeenschappelijke aanpak en specifieke acties inzake netwerk- en informatiebeveiliging [2].

(4) 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.

(5) Een aantal grote lacunes en verschillen in de wetgeving van de lidstaten op dit gebied kunnen een belemmering vormen voor de bestrijding van georganiseerde criminaliteit en terrorisme en kunnen een doeltreffende politiële en justitiële samenwerking op het gebied van aanvallen op informatiesystemen bemoeilijken. Het transnationale grensloze karakter van moderne informatiesystemen houdt in dat aanvallen op deze systemen vaak grensoverschrijdend van aard zijn, waardoor wordt onderstreept dat er dringend behoefte bestaat aan verdere onderlinge afstemming van het strafrecht op dit gebied.

(6) 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 en in de resolutie van het Europees Parlement van 19 mei 2000 zijn wetgevingsmaatregelen ter bestrijding van hightech-criminaliteit, waaronder gemeenschappelijke definities, strafbaarstellingen en straffen, aangegeven of wordt op dergelijke maatregelen aangedrongen.

(7) 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 Europees 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".

(8) 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.

[1] PB C 300 E van 11.12.2003, blz. 26.
[2] PB C 43 van 16.2.2002, blz. 2.
[3] PB C 19, 23.1.1999, blz. 1.

(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 uitvoering van dit kaderbesluit, moeten 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, onrechtmatige systeemverstoring en onrechtmatige gegevensverstoring worden gezorgd.

(12) In het belang van de bestrijding van cybercriminaliteit dient elke lidstaat te zorgen voor doeltreffende justitiële samenwerking met betrekking tot strafbare feiten op grond van gedragingen zoals bedoeld in de artikelen 2, 3, 4 en 5.

(13) Er moet worden voorkomen dat, met name in onbeduidende zaken, te zware straffen worden opgelegd en dat handelingen van houders van rechten en bevoegde personen strafbaar worden gesteld.

(14) De lidstaten zorgen ervoor dat aanvallen op informatiesystemen strafbaar zijn met doeltreffende, evenredige en afschrikkende straffen.

(15) Het is passend in zwaardere straffen te voorzien voor aanvallen op een informatiesysteem die gepleegd zijn in het kader van een criminele organisatie in de zin van Gemeenschappelijk Optreden 98/733/JBZ van de Raad van 21 december 1998 inzake de strafbaarstelling van deelneming aan een criminele organisatie in de lidstaten van de Europese Unie [1]. Het is ook mogelijk in zwaardere straffen te voorzien indien zulke aanvallen ernstige schade hebben berokkend of essentiële belangen hebben geschaad.

(16) Er moeten ook maatregelen worden genomen met het oog op samenwerking tussen de lidstaten teneinde een doeltreffend optreden tegen aanvallen op informatiesystemen mogelijk te maken. De lidstaten moeten derhalve voor de uitwisseling van informatie gebruikmaken van het bestaande net van operationele meldpunten zoals bedoeld in de aanbeveling van de Raad van 25 juni 2001 betreffende meldpunten die 24 uur per dag operationeel zijn voor de bestrijding van hightech-criminaliteit [2].

(17) Aangezien de doelstellingen van dit kaderbesluit 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 moeilijkheden weg te nemen, niet in voldoende mate door de lidstaten kunnen worden verwezenlijkt, omdat de regels gemeenschappelijk en met elkaar verenigbaar moeten zijn, en deze doelstellingen dus beter op het niveau van de Europese Unie kunnen worden verwezenlijkt, kan de Unie maatregelen nemen, in overeenstemming met het in artikel 5 van het Verdrag tot oprichting van de Europese Gemeenschap omschreven subsidiariteitsbeginsel. Overeenkomstig het in laatstgenoemd artikel omschreven evenredigheidsbeginsel gaat dit kaderbesluit niet verder dan wat nodig is om deze doelstellingen te verwezenlijken.

(18) In dit kaderbesluit worden de grondrechten in acht genomen en de beginselen nageleefd die in artikel 6 van het Verdrag betreffende de Europese Unie worden erkend en in het Handvest van de grondrechten van de Europese Unie zijn vastgelegd, met name in de hoofdstukken II en VI,

HEEFT HET VOLGENDE KADERBESLUIT VASTGESTELD:

Artikel 1

Definities

In dit kaderbesluit wordt verstaan onder:

a) „informatiesysteem": 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, alsmede de computergegevens die daarmee worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan;

b) „computergegevens": elke weergave van feiten, gegevens of begrippen 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;

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

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

[2] PB C 187 van 3.7.2001, blz. 5.

d) „onrechtmatig": toegang of verstoring, niet toegestaan door de eigenaar of een andere houder van rechten op het systeem of een deel daarvan, of niet toegestaan krachtens de nationale wetgeving.

Artikel 2

Onrechtmatige toegang tot informatiesystemen

1. Iedere lidstaat treft de nodige maatregelen om opzettelijke, onrechtmatige toegang tot een informatiesysteem of enig onderdeel daarvan strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.

2. Iedere lidstaat kan beslissen dat de in lid 1 bedoelde gedragingen alleen strafbaar worden gesteld indien het feit wordt gepleegd door een inbreuk op de beveiligingsmaatregelen.

Artikel 3

Onrechtmatige systeemverstoring

Iedere lidstaat treft de nodige maatregelen om het opzettelijk ernstig hinderen of het onderbreken van de werking van een informatiesysteem, door de invoer, de transmissie, het beschadigen, wissen, verminken, wijzigen, onderdrukken of ontoegankelijk maken van computergegevens, indien dat op onrechtmatige wijze geschiedt, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.

Artikel 4

Onrechtmatige gegevensverstoring

Iedere lidstaat treft de nodige maatregelen om het opzettelijk wissen, beschadigen, verminken, wijzigen, onderdrukken of ontoegankelijk maken van computergegevens in een informatiesysteem, indien dat op onrechtmatige wijze geschiedt, strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.

Artikel 5

Uitlokking, medeplichtigheid, poging

1. Iedere lidstaat zorgt ervoor dat uitlokking van of medeplichtigheid aan een van de in de artikelen 2, 3 en 4 genoemde feiten strafbaar wordt gesteld.

2. Iedere lidstaat zorgt ervoor dat poging tot het plegen van een van de in de artikelen 2, 3 en 4 genoemde feiten strafbaar wordt gesteld.

3. Iedere lidstaat kan besluiten om voor de in artikel 2 genoemde feiten lid 2 niet toe te passen.

Artikel 6

Straffen

1. Iedere lidstaat treft de nodige maatregelen om op de in de artikelen 2, 3, 4 en 5 genoemde gedragingen doeltreffende, evenredige en afschrikkende straffen te stellen.

2. Iedere lidstaat treft de nodige maatregelen opdat de gedragingen, genoemd in de artikelen 3 en 4, strafbaar worden gesteld met een maximum van ten minste één tot drie jaar gevangenisstraf.

Artikel 7

Verzwarende omstandigheden

1. Iedere lidstaat treft de nodige maatregelen opdat de gedragingen, genoemd in artikel 2, lid 2, en in de artikelen 3 en 4, strafbaar worden gesteld met een maximum van ten minste twee tot vijf jaar gevangenisstraf, indien begaan in het kader van een criminele organisatie in de zin van Gemeenschappelijk Optreden 98/733/JBZ, afgezien van de daarin aangegeven strafmaat.

2. Een lidstaat mag de in lid 1 genoemde maatregelen ook treffen als de betrokken gedragingen ernstige schade hebben berokkend of essentiële belangen hebben geschaad.

Artikel 8

Aansprakelijkheid van rechtspersonen

1. Iedere lidstaat treft de nodige maatregelen opdat rechtspersonen aansprakelijk kunnen worden gesteld voor de in de artikelen 2, 3, 4 en 5 genoemde gedragingen, 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 2, 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 als daders, uitlokkers of medeplichtigen betrokken zijn bij de in de artikelen 2, 3, 4 en 5 genoemde gedragingen, niet uit.

Artikel 9

Straffen tegen rechtspersonen

1. Iedere lidstaat treft de nodige maatregelen opdat aan een rechtspersoon die volgens artikel 8, 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 rechterlijk bevel tot ontbinding.

2. Iedere lidstaat treft de nodige maatregelen opdat tegen een rechtspersoon die volgens artikel 8, lid 2, aansprakelijk is, straffen kunnen worden vastgesteld of maatregelen kunnen worden getroffen die doeltreffend, evenredig en afschrikkend zijn.

Artikel 10

Rechtsmacht

1. Elke lidstaat vestigt zijn rechtsmacht ten aanzien van gedragingen in de zin van de artikelen 2, 3, 4 en 5, indien deze:

a) geheel of gedeeltelijk op zijn grondgebied zijn begaan, of

b) door een van zijn onderdanen zijn begaan, of

c) zijn begaan 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. Een lidstaat die zijn eigen onderdanen krachtens zijn wetgeving momenteel niet uitlevert of overlevert, treft de nodige maatregelen om zijn rechtsmacht te vestigen over de in de artikelen 2, 3, 4 en 5 genoemde gedragingen, en vervolgt die gedragingen, indien van toepassing, wanneer een van zijn onderdanen zich daaraan buiten zijn grondgebied schuldig heeft gemaakt.

4. 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. Daarbij mag achtereenvolgens rekening worden gehouden met de volgende criteria:

— de lidstaat op het grondgebied waarvan de handelingen zijn gepleegd, overeenkomstig lid 1, onder a), en lid 2;

— de lidstaat waarvan de dader een onderdaan is;

— de lidstaat waar de dader is aangetroffen.

5. Een lidstaat kan besluiten de in lid 1, onder b) en c), beschreven rechtsmachtsregels niet, of slechts in specifieke gevallen of omstandigheden, toe te passen.

6. De lidstaten stellen het secretariaat-generaal van de Raad en de Commissie op de hoogte wanneer zij besluiten lid 5 toe te passen, zo nodig onder vermelding van de specifieke gevallen of omstandigheden waarin het besluit van toepassing is.

Artikel 11

Uitwisseling van informatie

1. Met het oog op de uitwisseling van informatie in verband met strafbare feiten in de zin van de artikelen 2, 3, 4 en 5, maken de lidstaten, met inachtneming van de regels inzake gegevensbescherming, gebruik van het bestaande netwerk van operationele meldpunten 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 12

Tenuitvoerlegging

1. De lidstaten treffen de nodige maatregelen om uiterlijk op 16 maart 2007 aan de bepalingen van dit kaderbesluit te voldoen.

2. Uiterlijk op 16 maart 2007 zenden de lidstaten het secretariaat-generaal van de Raad en de Commissie de tekst toe van de bepalingen waarmee de uit hoofde van dit kaderbesluit op hen rustende verplichtingen in hun nationale wetgeving zijn omgezet. Uiterlijk op 16 september 2007 beoordeelt de Raad, op basis van een op grond van de informatie opgesteld rapport en een schriftelijk rapport van de Commissie, in hoeverre de lidstaten hebben voldaan aan de bepalingen van dit kaderbesluit.

Artikel 13

Inwerkingtreding

Dit kaderbesluit treedt in werking op de dag van zijn bekendmaking in het *Publicatieblad van de Europese Unie*.

Gedaan te Brussel, 24 februari 2005.

Voor de Raad
De voorzitter
N. SCHMIT