EUROPESE COMMISSIE

Brussel, 30.9.2010
COM(2010) 517 definitief

2010/0273 (COD)

Voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ van de Raad

SEC(2010) 1122 final}
SEC(2010) 1123 final}

TOELICHTING

1. MOTIVERING EN DOEL VAN HET VOORSTEL

Het doel van dit voorstel is Kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen[1] te vervangen. Dat kaderbesluit had – zoals vermeld in zijn overwegingen – 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 op het gebied van aanvallen op informatiesystemen. Het kaderbesluit zorgde voor EU-wetgeving inzake strafbare feiten als onrechtmatige toegang tot informatiesystemen, onrechtmatige systeemverstoring en onrechtmatige gegevensverstoring, alsmede voor specifieke regels betreffende de aansprakelijkheid van rechtspersonen, rechtsmacht en informatie-uitwisseling. De lidstaten dienden de maatregelen te nemen die noodzakelijk waren om uiterlijk op 16 maart 2007 aan de bepalingen van het kaderbesluit te voldoen.

Op 14 juli 2008 publiceerde de Commissie een verslag over de tenuitvoerlegging van het kaderbesluit[2]. In de conclusies van het verslag werd vastgesteld dat er in de meeste lidstaten belangrijke vooruitgang was geboekt en dat het uitvoeringsniveau betrekkelijk goed was, hoewel de tenuitvoerlegging in een aantal lidstaten nog niet volledig was afgerond. Het verslag bevatte daarnaast de volgende constatering: "Sinds het vaststellen van het kaderbesluit hebben recente aanvallen in heel Europa allerlei nieuwe bedreigingen aan het licht gebracht, met name het zich voordoen van omvangrijke gelijktijdige aanvallen op informatiesystemen en een toenemend crimineel gebruik van zogeheten botnets." Deze aanvallen waren niet het belangrijkste aandachtspunt toen het kaderbesluit werd aangenomen. Naar aanleiding van deze ontwikkelingen zal de Commissie nagaan met welke acties beter op dit gevaar kan worden ingespeeld (zie volgende punt voor een uitleg van het verschijnsel botnet).

Het belang van verdere maatregelen om de strijd tegen cybercriminaliteit op te voeren werd onderstreept in het Haags programma van 2004 betreffende de versterking van vrijheid, veiligheid en recht in de Europese Unie en in het programma van Stockholm van 2009 en het bijbehorende actieplan[3]. Bovendien werd in de onlangs gepresenteerde digitale agenda voor Europa[4], het eerste kerninitiatief in het kader van de Europa 2020-strategie, vastgesteld dat de groei van nieuwe vormen van criminaliteit, en met name van cybercriminaliteit, op Europees niveau moet worden gekeerd. Bij de acties op het gebied van vertrouwen en beveiliging staan maatregelen ter bestrijding van cyberaanvallen op informatiesystemen centraal.

Op internationaal niveau wordt het op 23 november 2001 ondertekende Verdrag inzake cybercriminaliteit van de Raad van Europa (hierna "Verdrag inzake cybercriminaliteit" genoemd) beschouwd als de tot dusver meest volledige internationale rechtsnorm, aangezien het voorziet in een alomvattend en samenhangend kader dat de diverse aspecten van cybercriminaliteit bestrijkt[5]. Het Verdrag is door alle 27 lidstaten ondertekend, maar tot

---

1 PB L 69 van 16.3.2005, blz. 68.

2 Verslag van de Commissie aan de Raad op basis van artikel 12 van het kaderbesluit van de Raad van 24 februari 2005 over aanvallen op informatiesystemen, COM(2008) 448.

3 PB C 198 van 12.8.2005, PB C 115 van 4.5.2010 en COM(2010) 171 van 20.4.2010.

4 Mededeling COM(2010) 245 van de Commissie van 19.5.2010.

5 Verdrag inzake cybercriminaliteit van de Raad van Europa, Boedapest, 23.11.2001, CETS nr. 185.

dusver door slechts 15 lidstaten geratificeerd[6]. Het Verdrag is op 1 juli 2004 in werking getreden. De EU is geen partij bij het Verdrag. Gelet op het belang van dit instrument, moedigt de Commissie de overige EU-lidstaten uitdrukkelijk aan om het Verdrag zo spoedig mogelijk te ratificeren.

- **Algemene context**

Er zijn tal van factoren waardoor cybercriminaliteit een kans krijgt. Tekortkomingen in de rechtshandhaving dragen ertoe bij dat het verschijnsel om zich heen kan grijpen. Het probleem is des te groter daar sommige soorten delicten de landsgrenzen overschrijden. Cybercriminaliteit wordt dikwijls onvoldoende gemeld, deels omdat bepaalde strafbare feiten onopgemerkt blijven en deels omdat de slachtoffers (economische actoren en ondernemingen) strafbare feiten niet melden uit angst voor een slechte naam en omdat zij er beducht voor zijn dat hun bedrijfsvooruitzichten eronder zullen lijden wanneer hun kwetsbare punten algemeen bekend worden.

Daarnaast kunnen discrepanties tussen de nationale strafrechtelijke bepalingen en procedures leiden tot verschillen bij onderzoek en vervolging, waardoor deze strafbare feiten op uiteenlopende manieren worden aangepakt. Ontwikkelingen in de informatietechnologie hebben deze problemen nog groter gemaakt, doordat het voor de daders gemakkelijker is geworden om instrumenten (kwaadaardige software en botnets) te vervaardigen en te verspreiden, terwijl ze zelf anoniem blijven en de strafrechtelijke bevoegdheid over verschillende rechtsgebieden is verspreid. Aangezien het moeilijk is om vervolging in te stellen, kan de georganiseerde misdaad forse winsten maken met geringe risico's.

Dit voorstel houdt rekening met de nieuwe methoden om cyberdelicten te plegen, zoals het gebruik van "botnets". Onder deze term wordt een netwerk verstaan van computers die zijn besmet met kwaadaardige software (een computervirus). Een dergelijk netwerk van besmette computers ("zombies") kan worden ingezet voor specifieke acties, zoals aanvallen op informatiesystemen (cyberaanvallen). Deze zombies kunnen door een andere computer worden bestuurd – dikwijls zonder dat de gebruikers van de besmette computers hier erg in hebben. De besturingscomputer wordt ook wel aangeduid als het "command-and-control centre". De personen die dit centrum besturen, behoren tot de daders, aangezien zij de besmette computers gebruiken voor aanvallen op informatiesystemen. Het is bijzonder moeilijk om de daders op te sporen, doordat de computers die deel uitmaken van het botnet en de aanval uitvoeren, zich op een andere locatie kunnen bevinden dan de dader zelf.

Aanvallen die door een botnet worden uitgevoerd zijn vaak grootschalig. Als grootschalig gelden aanvallen die worden uitgevoerd met behulp van instrumenten die zich bedienen van grote aantallen informatiesystemen (computers), en aanvallen die aanzienlijke schade veroorzaken, bv. in termen van ontregelde systeemdiensten, financiële kosten, verlies van persoonsgegevens, enz. De schade veroorzaakt door grootschalige aanvallen heeft grote gevolgen voor het functioneren van het doelwit en/of tast zijn werkomgeving aan. In dit kader geldt als een "groot botnet" een netwerk dat ernstige schade kan veroorzaken. Het is moeilijk om botnets te definiëren naar omvang, maar het is bekend dat de grootste botnets voor naar

[6] Zie voor een overzicht betreffende de ratificatie van het Verdrag (CETS nr. 185): http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

schatting tussen de 40 000 en 100 000 verbindingen (dat wil zeggen: besmette computers) per etmaal zorgen[7].

- **Bestaande bepalingen op het door het voorstel bestreken gebied**

Op EU-niveau moest het kaderbesluit zorgen voor een minimale onderlinge aanpassing van de wetgeving van de lidstaten om een aantal vormen van cybercriminaliteit strafbaar te stellen, met inbegrip van onrechtmatige toegang tot informatiesystemen, onrechtmatige systeemverstoring, onrechtmatige gegevensverstoring, alsook uitlokking van, medeplichtigheid aan en poging tot dergelijke feiten.

Hoewel de bepalingen van het kaderbesluit over het algemeen door de lidstaten ten uitvoer zijn gelegd, schiet het instrument op bepaalde punten tekort door de toename van de feiten (cyberaanvallen), zowel in omvang als in aantal. Het kaderbesluit zorgt alleen voor onderlinge afstemming van de wetgeving inzake een beperkt aantal strafbare feiten, maar biedt geen volledige aanpak van de sociale risico's van grootschalige aanvallen. Ook wordt er onvoldoende rekening gehouden met de ernst van de delicten en de daaraan verbonden sancties.

Andere lopende of geplande EU-initiatieven en –programma's richten zich ook op het oplossen van problemen in verband met cyberaanvallen of daarmee samenhangende kwesties, zoals netwerkbeveiliging en de veiligheid van internetgebruikers. Het gaat onder meer om maatregelen die worden ondersteund door de programma's "Preventie en de bestrijding van criminaliteit"[8], "Strafrecht"[9], "Veiliger internet"[10] en het initiatief "Bescherming van kritieke informatie-infrastructuur"[11]. Naast het genoemde kaderbesluit is er nog een belangrijk rechtsinstrument van kracht, namelijk Kaderbesluit 2004/68/JBZ ter bestrijding van seksuele uitbuiting van kinderen en kinderpornografie.

Het besmetten van computers met het oog op integratie in botnets is al verboden op grond van EU-regelgeving inzake privacy en gegevensbescherming[12]. Met name administratieve instanties werken al samen in het kader van het Europese verbindingsnetwerk van organen voor spambestrijding (Contact Network of Spam Authorities, CNSA). Op grond van voornoemde regelgeving moeten de lidstaten het verbieden om zonder toestemming van de betrokken gebruikers of een wettelijke machtiging berichten te onderscheppen die zijn verzonden via openbare communicatienetwerken en openbaar beschikbare elektronische communicatiediensten.

Dit voorstel voldoet aan deze regelgeving. De lidstaten dienen te streven naar betere samenwerking tussen de administratieve en wetshandhavingsinstanties bij zaken waarop zowel administratieve als strafrechtelijke sancties van toepassing zijn.

---

7 Het aantal verbindingen per etmaal is de gebruikelijke eenheid om de omvang van botnets in uit te drukken.

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

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

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

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

12 Richtlijn betreffende privacy en elektronische communicatie (PB L 201 van 31.7.2002), gewijzigd bij Richtlijn 2009/136/EG (PB L 337 van 18.12.2009).

- **Samenhang met andere beleidsgebieden en doelstellingen van de Unie**

De doelstellingen zijn in overeenstemming met het EU-beleid op het gebied van de bestrijding van de georganiseerde criminaliteit, vergroting van de veerkracht van netwerken, bescherming van de vitale infrastructuur en gegevensbescherming. De doelstellingen stroken tevens met het programma voor een veiliger internet, dat werd opgezet om een veiliger gebruik van internet en van nieuwe onlinetechnologieën te bevorderen en om illegale inhoud te bestrijden.

Aan dit voorstel is grondig onderzoek voorafgegaan om te waarborgen dat de bepalingen ervan volledig in overeenstemming zijn met de grondrechten, in het bijzonder de bescherming van persoonsgegevens, de vrijheid van meningsuiting en van informatie, het recht op een eerlijk proces, het beginsel van het vermoeden van onschuld, de rechten van de verdediging, alsmede het legaliteitsbeginsel en het evenredigheidsbeginsel inzake delicten en straffen.

2. RAADPLEGING VAN BELANGHEBBENDE PARTIJEN EN EFFECTBEOORDELING

- **Raadpleging van belanghebbenden**

Tal van deskundigen op dit gebied zijn geraadpleegd tijdens meerdere bijeenkomsten over diverse aspecten van de bestrijding van cybercriminaliteit, zoals de justitiële follow-up (vervolging) van strafbare feiten. Het ging met name om vertegenwoordigers van de overheden van de lidstaten, de particuliere sector, gespecialiseerde rechters en aanklagers, internationale organisaties, Europese agentschappen en groepen van deskundigen. Een aantal deskundigen en organisaties heeft nadien standpunten ingediend en informatie verstrekt.

De belangrijkste punten die uit de raadpleging naar voren zijn gekomen, zijn:

– de noodzaak van EU-optreden op dit gebied;

– de noodzaak om handelingen strafbaar te stellen die niet in het huidige kaderbesluit zijn opgenomen, met name nieuwe soorten cyberaanvallen (botnets);

– de noodzaak om hinderpalen voor onderzoek en vervolging in grensoverschrijdende zaken uit de weg te ruimen.

Met de informatie die bij de raadpleging naar voren is gebracht, is in de effectbeoordeling rekening gehouden.

Bijeenbrengen en benutten van deskundigheid

Externe knowhow is verworven tijdens verscheidene bijeenkomsten met belanghebbenden.

Effectbeoordeling

Diverse beleidsopties zijn overwogen als middel om het beoogde doel te bereiken.

- Beleidsoptie 1: Status quo/geen nieuwe EU-maatregelen

Deze optie houdt in dat de EU geen verdere maatregelen treft om deze vorm van cybercriminaliteit, namelijk aanvallen op informatiesystemen, te bestrijden. Lopende

maatregelen, zoals met name de programma's voor betere bescherming van de vitale informatiestructuur en betere publiek-private samenwerking tegen cybercriminaliteit, zouden moeten worden voortgezet.

- Beleidsoptie 2: Ontwikkeling van een programma om aanvallen op informatiesystemen krachtiger tegen te gaan met niet-wetgevende maatregelen

Naast het programma ter bescherming van de vitale informatie-infrastructuur zouden niet-wetgevende maatregelen met name grensoverschrijdende wetshandhaving en publiek-private samenwerking bevorderen. Deze "soft law"-instrumenten zouden meer gecoördineerde EU-maatregelen moeten bevorderen door onder meer een versterking van het bestaande 24/7-netwerk van meldpunten voor rechtshandhavingsinstanties, de oprichting van een EU-netwerk van publiek-private meldpunten voor deskundigen op het gebied van cybercriminaliteit en rechtshandhavingsinstanties, de formulering van een standaard-EU-dienstenovereenkomst voor samenwerking op het gebied van rechtshandhaving met particuliere partijen, en ondersteuning van de organisatie van voor rechtshandhavingsinstanties bestemde opleidingsprogramma's op het gebied van onderzoek naar cybercriminaliteit.

- Beleidsoptie 3: Gerichte herziening van de regels van het kaderbesluit (nieuwe richtlijn ter vervanging van het huidige kaderbesluit) om het risico van grootschalige aanvallen op informatiesystemen (botnets) aan te pakken en om, indien de dader zijn ware identiteit verhult en de rechtmatige bezitter van een identiteit schade berokkent, de doeltreffendheid van de meldpunten voor rechtshandhaving van de lidstaten te verbeteren en te zorgen voor statistische gegevens over cyberaanvallen.

Deze optie houdt de invoering in van specifieke gerichte (d.w.z. beperkte) wetgeving ter voorkoming van grootschalige aanvallen op informatiesystemen. Een dergelijke verscherpte wetgeving zou vergezeld gaan van niet-wetgevende maatregelen ter verbetering van de operationele grensoverschrijdende samenwerking tegen zulke aanvallen, hetgeen de tenuitvoerlegging van de wetgevende maatregelen zou vereenvoudigen. Deze maatregelen zouden de paraatheid, veiligheid en veerkracht van de vitale informatie-infrastructuur moeten vergroten en moeten leiden tot uitwisseling van beste praktijken.

- Beleidsoptie 4: Invoering van alomvattende EU-wetgeving tegen cybercriminaliteit

Deze optie houdt nieuwe alomvattende EU-wetgeving in. Naast de "soft law"-maatregelen van beleidsoptie 2 en de herziening van beleidsoptie 3 zouden ook andere juridische problemen in verband met internetgebruik worden aangepakt. Dergelijke maatregelen zouden niet alleen betrekking hebben op aanvallen op informatiesystemen, maar ook op zaken als financiële cybercriminaliteit, illegale internetinhoud en het verzamelen/bewaren/doorgeven van elektronisch bewijsmateriaal; ook zouden zij meer gedetailleerde rechtsmachtsregels meebrengen. De wetgeving zou naast het Verdrag inzake cybercriminaliteit van de Raad van Europa bestaan en worden begeleid door de hierboven genoemde niet-wetgevende maatregelen.

- Beleidsoptie 5: Herziening van het Verdrag inzake cybercriminaliteit van de Raad van Europa

Deze optie houdt een grondige heronderhandeling van het huidige Verdrag in. Dit veronderstelt een langdurig proces en is niet te rijmen met de termijnen voor actie die in de effectbeoordeling worden voorgesteld. Er lijkt geen internationale bereidheid te zijn om

opnieuw te onderhandelen over het Verdrag. Een herziening van het Verdrag kan derhalve niet als een haalbare optie worden aangemerkt, aangezien zij buiten de vereiste termijn zou vallen.

Voorkeursoptie: Combinatie van niet-wetgevende maatregelen (optie 2) en een gerichte herziening van het kaderbesluit (optie 3)

Op grond van de analyse van de economische en sociale gevolgen en van de implicaties op het gebied van de grondrechten komen de opties 2 en 3 naar voren als de beste aanpak van het probleem, die aan de doelstellingen van het voorstel beantwoordt.

Ter voorbereiding van dit voorstel heeft de Commissie een effectbeoordeling uitgevoerd.

3. JURIDISCHE ELEMENTEN VAN HET VOORSTEL

- **Samenvatting van de voorgestelde maatregel**

De richtlijn strekt weliswaar tot intrekking van Kaderbesluit 2005/222/JBZ, maar neemt de bestaande bepalingen daarvan over en breidt deze uit met de navolgende nieuwe elementen.

– Met betrekking tot het materiële strafrecht in het algemeen:

A. stelt de richtlijn de productie, verkoop, aanschaf voor gebruik, invoer, verspreiding of het op andere wijze beschikbaar maken van instrumenten voor het plegen van de strafbare feiten strafbaar;

B. bevat de richtlijn de volgende verzwarende omstandigheden:

- de grootschaligheid van de aanvallen: botnets of vergelijkbare instrumenten zouden worden aangepakt door een nieuwe verzwarende omstandigheid in te voeren, in de zin dat het opzetten van een botnet of een vergelijkbaar instrument bij het plegen van de in het huidige kaderbesluit opgesomde strafbare feiten als een verzwarende factor zou gelden,

- het plegen van dergelijke aanvallen door de ware identiteit van de dader te verhullen en de rechtmatige bezitter van de identiteit schade te berokkenen. Dergelijke regels zouden moeten voldoen aan het legaliteitsbeginsel en het evenredigheidsbeginsel inzake delicten en straffen, en in overeenstemming moeten zijn met de bestaande wetgeving inzake de bescherming van persoonsgegevens[13];

C. stelt de richtlijn "onrechtmatige onderschepping" strafbaar;

[13] Zoals Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12.7.2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn voor de gegevensbescherming voor elektronische communicatie), PB L 201 van 31.7.2002, blz. 37 (die momenteel wordt herzien) en de algemene gegevensbeschermingsrichtlijn 95/46/EG.

D. voert de richtlijn maatregelen in ter verbetering van de Europese strafrechtelijke samenwerking door de bestaande structuur van 24/7-meldpunten[14] te versterken:

- er wordt voorgesteld dat binnen een bepaalde termijn (vastgesteld in artikel 14 van de richtlijn) gehoor moet worden gegeven aan een verzoek om bijstand van de operationele meldpunten. Het Verdrag inzake cybercriminaliteit kent een dergelijke bindende bepaling niet. Deze maatregel moet ervoor zorgen dat de meldpunten binnen een vastgestelde termijn verklaren of zij gehoor kunnen geven aan het verzoek om bijstand en wanneer het verzoekende meldpunt een oplossing tegemoet kan zien. De eigenlijke inhoud van de oplossingen wordt niet vermeld;

E. voorziet de richtlijn in de behoefte aan statistische gegevens over cybercriminaliteit door lidstaten ertoe te verplichten voor een passend systeem te zorgen, waarmee statistische gegevens over de in het huidige kaderbesluit bedoelde strafbare feiten en het toegevoegde nieuwe feit "onrechtmatige onderschepping" kunnen worden geregistreerd, aangemaakt en verstrekt.

De richtlijn bevat in de definities van strafbare feiten in de artikelen 3, 4 en 5 (onrechtmatige toegang tot informatiesystemen, onrechtmatige systeemverstoring en onrechtmatige gegevensverstoring) een bepaling op grond waarvan alleen "gevallen die niet onbeduidend zijn" bij de omzetting van de richtlijn in nationaal recht strafbaar hoeven te worden gesteld. Deze speelruimte moet lidstaten in de gelegenheid stellen om te voorzien in een uitzondering voor gevallen die in abstracto onder de basisdefinitie zouden vallen, maar niet gelden als schadelijk voor het beschermde rechtsbelang, in het bijzonder wanneer het bijvoorbeeld gaat om jongeren die hun deskundigheid op het gebied van informatietechnologie proberen te tonen. Deze mogelijkheid om de strafbaarstelling te beperken dient echter niet te leiden tot de invoering van aanvullende bestanddelen van strafbare feiten die verder gaan dan hetgeen reeds in de richtlijn is opgenomen, aangezien dit een situatie zou scheppen waarin uitsluitend feiten waarbij sprake is van verzwarende omstandigheden, strafbaar worden gesteld. Bij de omzetting dienen de lidstaten er zich met name van te onthouden de basisdelicten uit te breiden met aanvullende bestanddelen, zoals bv. de specifieke opzet om op criminele wijze illegale opbrengsten te genereren of de aanwezigheid van een specifiek effect, zoals het veroorzaken van aanzienlijke schade.

- **Rechtsgrondslag**

Artikel 83, lid 1, van het Verdrag betreffende de werking van de Europese Unie[15].

- **Subsidiariteitsbeginsel**

Op de maatregelen van de Europese Unie is het subsidiariteitsbeginsel van toepassing. De doelstellingen van het voorstel kunnen om de navolgende redenen niet voldoende door de lidstaten worden verwezenlijkt:

cybercriminaliteit en in het bijzonder aanvallen op informatiesystemen hebben een forse grensoverschrijdende dimensie, die het duidelijkst blijkt uit grootschalige aanvallen, aangezien de gekoppelde elementen waarmee de aanval wordt uitgevoerd zich dikwijls op verschillende locaties en in meerdere landen bevinden. Dit vereist EU-optreden, met name om

[14] Ingevoerd bij het Verdrag en Kaderbesluit 2005/222/JBZ over aanvallen op informatiesystemen.
[15] PB C 83 van 30.3.2010, blz. 49.

het hoofd te bieden aan de huidige tendens om binnen en buiten Europa grootschalige aanvallen uit te voeren. Ook in de conclusies van de Raad van november 2008[16] is gepleit voor actie op EU-niveau en een herziening van Kaderbesluit 2005/222/JBZ, aangezien de doelstelling om burgers doeltreffend te beschermen tegen cybercriminaliteit niet toereikend kan worden verwezenlijkt door de lidstaten alleen.

De doelstellingen van het voorstel zullen beter worden verwezenlijkt door een optreden van de EU, en wel om de navolgende redenen:

het voorstel zal het materiële strafrecht van de lidstaten en de procedureregels verder onderling afstemmen, hetgeen positieve gevolgen zal hebben voor de bestrijding van deze strafbare feiten. Ten eerste kan zo worden voorkomen dat daders naar lidstaten trekken waar de wetgeving inzake cyberaanvallen soepeler is. Ten tweede maken gezamenlijke definities het mogelijk om informatie uit te wisselen en relevante gegevens te verzamelen en vergelijken. Ten derde worden de preventieve maatregelen in de EU er doeltreffender van en zal ook de internationale samenwerking er door worden versterkt.

Het voorstel is dan ook in overeenstemming met het subsidiariteitsbeginsel.

- **Evenredigheidsbeginsel**

Het voorstel is om de navolgende reden in overeenstemming met het evenredigheidsbeginsel.

Deze richtlijn beperkt zich tot het voor de verwezenlijking van deze doelstellingen op Europees niveau vereiste minimum en reikt niet verder dan wat daarvoor nodig is, rekening houdend met de vereiste nauwkeurigheid van de strafwetgeving.

- **Keuze van het instrument**

Voorgesteld instrument: richtlijn.

Andere instrumenten zouden om de navolgende reden ongeschikt zijn:

de rechtsgrondslag vereist een richtlijn;

niet-wetgevende maatregelen en zelfregulering zouden de situatie weliswaar verbeteren op sommige gebieden waarop tenuitvoerlegging van cruciaal belang is, maar op andere terreinen waar nieuwe wetgeving onmisbaar is, zouden dergelijke maatregelen niet veel uithalen.

4. GEVOLGEN VOOR DE BEGROTING

Het voorstel heeft geringe gevolgen voor de begroting van de Unie. Meer dan 90% van de geraamde kosten van 5 913 000 EUR zou ten laste van de lidstaten komen en er kan EU-financiering worden aangevraagd om de kosten te beperken.

---

[16] "Gemeenschappelijke werkstrategie en concrete maatregelen tegen cybercriminaliteit", 2987e zitting van de Raad Justitie en Binnenlandse Zaken, 27 en 28 november 2008.

5. AANVULLENDE INFORMATIE

- **Intrekking van bestaande wetgeving**

De goedkeuring van het voorstel heeft de intrekking van bestaande wetgeving tot gevolg.

- **Territoriale werkingssfeer**

Deze richtlijn is overeenkomstig de Verdragen gericht tot de lidstaten.

2010/0273 (COD)

Voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ van de Raad

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name

artikel 83, lid 1,

Gezien het voorstel van de Europese Commissie[17],

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité,

Gezien het advies van het Comité van de Regio's,

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Deze richtlijn heeft ten doel de strafrechtelijke bepalingen van de lidstaten inzake aanvallen op informatiesystemen onderling af te stemmen en de samenwerking tussen justitiële en andere bevoegde autoriteiten, zoals de politie en andere gespecialiseerde rechtshandhavingsinstanties van de lidstaten, te verbeteren.

(2) Aanvallen op informatiesystemen, in het bijzonder in het kader van de georganiseerde criminaliteit, vormen een groeiende bedreiging en de bezorgdheid over mogelijke terroristische of politiek gemotiveerde aanvallen op informatiesystemen die deel uitmaken van de vitale infrastructuur van de lidstaten en de Unie neemt toe. Dit brengt de totstandbrenging van een veiliger informatiemaatschappij en een ruimte van vrijheid, veiligheid en recht in gevaar en maakt derhalve een reactie op het niveau van de Europese Unie noodzakelijk.

(3) Er zijn aanwijzingen dat grootschalige aanvallen op de informatiesystemen die van vitaal belang zijn voor staten of voor specifieke onderdelen van de publieke of particuliere sector steeds gevaarlijker en frequenter worden. Deze tendens gaat gepaard met de ontwikkeling van telkens geavanceerder instrumenten die door criminelen kunnen worden gebruikt om diverse soorten cyberaanvallen uit te voeren.

[17] PB C […] van […], blz.. […].

(4) Gemeenschappelijke definities op dit gebied, en in het bijzonder van informatiesystemen en computergegevens, zijn van belang om te garanderen dat de richtlijn in de lidstaten coherent wordt toegepast.

(5) Teneinde tot een gemeenschappelijke aanpak van de bestanddelen van strafbare feiten te komen, moet een gemeenschappelijke definitie van de strafbare feiten onrechtmatige toegang tot een informatiesysteem, onrechtmatige systeemverstoring en onrechtmatige gegevensverstoring worden ingevoerd.

(6) De lidstaten dienen aanvallen op informatiesystemen strafbaar te stellen. De straffen dienen doeltreffend, evenredig en afschrikkend te zijn.

(7) Het is passend om te voorzien in zwaardere straffen voor een aanval op een informatiesysteem die gepleegd wordt door een criminele organisatie in de zin van Kaderbesluit 2008/841/JBZ van de Raad van 24 oktober 2008 ter bestrijding van georganiseerde criminaliteit[18], voor een grootschalige aanval en voor een strafbaar feit dat wordt gepleegd door de ware identiteit van de dader te verhullen en de rechtmatige bezitter van de identiteit schade te berokkenen. Het is ook passend in zwaardere straffen te voorzien voor gevallen waarin zulke aanvallen ernstige schade hebben veroorzaakt of essentiële belangen hebben geschaad.

(8) De conclusies van de Raad van 27 en 28 november 2008 hielden in dat er binnen de lidstaten en de Commissie een nieuwe strategie dient te worden ontwikkeld, waarbij rekening wordt gehouden met de inhoud van het uit 2001 daterende Verdrag inzake cybercriminaliteit van de Raad van Europa. Dat Verdrag is het wettelijke referentiekader voor de bestrijding van cybercriminaliteit, waaronder aanvallen op informatiesystemen. Deze richtlijn bouwt voort op dat Verdrag.

(9) Gelet op de verschillende manieren waarop aanvallen kunnen worden uitgevoerd, en gelet op de snelle ontwikkelingen op het gebied van hardware en software, wordt er in deze richtlijn verwezen naar "instrumenten" die kunnen worden gebruikt voor het plegen van de in deze richtlijn opgesomde strafbare feiten. Onder instrumenten wordt bijvoorbeeld kwaadaardige software verstaan, zoals botnets, waarmee cyberaanvallen worden gepleegd.

(10) Deze richtlijn beoogt niet de strafbaarstelling van feiten die gepleegd worden zonder criminele opzet, zoals het officieel testen of beveiligen van informatiesystemen.

(11) Deze richtlijn vergroot het belang van netwerken, zoals dat van de G8 of het netwerk van meldpunten van de Raad van Europa, die vierentwintig uur per dag en zeven dagen per week voor informatie-uitwisseling bereikbaar zijn om te waarborgen dat er onmiddellijk bijstand kan worden verleend voor onderzoeken of procedures inzake strafbare feiten op het gebied van informatiesystemen en gegevens, of voor het vergaren van elektronisch bewijs voor een strafbaar feit. Gelet op de snelheid waarmee grootschalige aanvallen kunnen worden uitgevoerd, dienen alle lidstaten onverwijld te kunnen reageren op dringende bijstandsverzoeken van dit netwerk van meldpunten. Dergelijke bijstand dient onder meer te bestaan uit het vereenvoudigen of rechtstreeks uitvoeren van maatregelen als het verlenen van technisch advies, het bewaren van

[18] PB L 300 van 11.11.2008, blz. 42.

gegevens, het verzamelen van bewijs, het verstrekken van juridische informatie en het lokaliseren van verdachten.

(12) Er dienen gegevens te worden verzameld over strafbare feiten in de zin van deze richtlijn, zodat er een vollediger beeld ontstaat van het probleem op het niveau van de Unie en er doeltreffender antwoorden kunnen worden geformuleerd. Met behulp van deze gegevens kunnen gespecialiseerde agentschappen als Europol en het Europees Agentschap voor netwerk- en informatiebeveiliging de omvang van cybercriminaliteit en de netwerk- en informatiebeveiliging in Europa bovendien beter beoordelen.

(13) Grote lacunes en verschillen in de wetgeving van de lidstaten op het gebied van aanvallen op informatiesystemen kunnen een belemmering vormen voor de bestrijding van georganiseerde criminaliteit en terrorisme en kunnen doeltreffende politiële en justitiële samenwerking op dit gebied bemoeilijken. Het transnationale grensloze karakter van moderne informatiesystemen houdt in dat aanvallen op deze systemen een grensoverschrijdende dimensie hebben, wat tot gevolg heeft dat er dringend behoefte bestaat aan verdere onderlinge afstemming van het strafrecht op dit gebied. Bovendien dient de coördinatie van de vervolging van aanvallen op informatiesystemen te worden vergemakkelijkt door de vaststelling van Kaderbesluit 2009/948/JBZ van de Raad over het voorkomen en beslechten van geschillen over de uitoefening van rechtsmacht bij strafprocedures.

(14) Aangezien de doelstellingen van deze richtlijn 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 betreffende de Europese Unie omschreven subsidiariteitsbeginsel. Deze richtlijn gaat niet verder dan wat nodig is om voornoemde doelstellingen te verwezenlijken.

(15) De persoonsgegevens die worden verwerkt in het kader van de uitvoering van deze richtlijn dienen te worden beschermd overeenkomstig de regels van Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 inzake de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken[19] (met betrekking tot de verwerkingswerkzaamheden die binnen het toepassingsgebied daarvan vallen) en Verordening nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens[20].

(16) Deze richtlijn eerbiedigt de grondrechten en is in overeenstemming met de beginselen die met name bij het Handvest van de grondrechten van de Europese Unie zijn erkend, waaronder de bescherming van persoonsgegevens, de vrijheid van meningsuiting en van informatie, het recht op een eerlijk proces en het beginsel van het vermoeden van

---

19 PB L 350 van 30.12.2008, blz. 60.

20 PB L 8 van 12.1.2001, blz. 1.

onschuld, alsmede het legaliteitsbeginsel en het evenredigheidsbeginsel inzake delicten en straffen. Deze richtlijn beoogt in het bijzonder de onverkorte eerbiediging van deze rechten en beginselen te waarborgen en moet dienovereenkomstig worden uitgevoerd.

(17) [Overeenkomstig de artikelen 1 tot en met 4 van het Protocol betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, dat gehecht is aan het Verdrag betreffende de werking van de Europese Unie, hebben het Verenigd Koninkrijk en Ierland kennis gegeven van hun wens om aan de goedkeuring en toepassing van deze richtlijn deel te nemen] OF [Onverminderd artikel 4 van het Protocol betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, zullen het Verenigd Koninkrijk en Ierland niet deelnemen aan de goedkeuring van deze richtlijn en zullen zij niet gebonden zijn door, noch onderworpen aan de toepassing van deze richtlijn].

(18) Overeenkomstig artikel 1 en artikel 2 van het Protocol betreffende de positie van Denemarken, dat gehecht is aan het Verdrag betreffende de werking van de Europese Unie, neemt Denemarken niet deel aan de goedkeuring van deze richtlijn en is het dus niet gebonden door, noch onderworpen aan de toepassing van deze richtlijn,

HEBBEN DE VOLGENDE RICHTLIJN VASTGESTELD:

Artikel 1
Onderwerp

Deze richtlijn definieert strafbare feiten op het gebied van aanvallen op informatiesystemen en stelt minimumregels inzake sancties voor dergelijke strafbare feiten vast. Ook beoogt zij gemeenschappelijke bepalingen in te voeren om dergelijke aanvallen te voorkomen en de Europese strafrechtelijke samenwerking op dit gebied te verbeteren.

Artikel 2
Definities

In deze richtlijn wordt verstaan onder:

a) "informatiesysteem": apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken, 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 vervullen;

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;

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

Artikel 3

Onrechtmatige toegang tot informatiesystemen

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.

Artikel 4

Onrechtmatige systeemverstoring

De lidstaten treffen 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 5

Onrechtmatige gegevensverstoring

De lidstaten treffen 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 6

Onrechtmatige onderschepping

De lidstaten treffen de nodige maatregelen om het opzettelijk met technische middelen onderscheppen van niet-openbare transmissies van computergegevens naar, vanuit of binnen een computersysteem, met inbegrip van elektromagnetische emissies uit een computersysteem dat zulke computergegevens draagt, indien onrechtmatig begaan, strafbaar te stellen.

Artikel 7

Instrumenten voor het plegen van strafbare feiten

De lidstaten treffen de nodige maatregelen om de productie, de verkoop, de aanschaf voor gebruik, de invoer, het bezit, de verspreiding of het op andere wijze beschikbaar maken van de volgende zaken, indien opzettelijk en onrechtmatig gedaan, met het oog op het plegen van een van de in de artikelen 3 tot en met 6 bedoelde feiten, strafbaar te stellen:

a) een instrument, zoals een computerprogramma, dat hoofdzakelijk ontworpen of aangepast is voor het plegen van de in de artikelen 3 tot en met 6 bedoelde strafbare feiten;

b) een computerwachtwoord, toegangscode of soortgelijke gegevens die toegang bieden tot een informatiesysteem of een deel daarvan.

Artikel 8

Uitlokking, deelneming, medeplichtigheid en poging

1. De lidstaten zorgen ervoor dat uitlokking van, alsmede deelneming en medeplichtigheid aan een van de in de artikelen 3 tot en met 7 genoemde feiten strafbaar wordt gesteld.

2. De lidstaten zorgen ervoor dat poging tot het plegen van een van de in de artikelen 3 tot en met 6 genoemde feiten strafbaar wordt gesteld.

Artikel 9

Sancties

1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 3 tot en met 8 bedoelde feiten strafbaar worden gesteld met doeltreffende, evenredige en afschrikkende strafrechtelijke sancties.

2. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 3 tot en met 7 bedoelde feiten strafbaar worden gesteld met een maximale gevangenisstraf van ten minste twee jaar.

Artikel 10

Verzwarende omstandigheden

1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 3 tot en met 7 bedoelde feiten strafbaar worden gesteld met een maximale gevangenisstraf van ten minste vijf jaar wanneer deze worden gepleegd in het kader van een criminele organisatie zoals gedefinieerd in Kaderbesluit 2008/841/JBZ.

2. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 3 tot en met 6 bedoelde feiten strafbaar worden gesteld met een maximale gevangenisstraf van ten minste vijf jaar, wanneer deze worden gepleegd met behulp van een instrument dat bestemd is voor het uitvoeren van aanvallen die een groot aantal informatiesystemen treffen of aanzienlijke schade veroorzaken, zoals ontregelde systeemdiensten, financiële kosten of verlies van persoonsgegevens.

3. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 3 tot en met 6 bedoelde feiten strafbaar worden gesteld met een maximale gevangenisstraf van ten minste vijf jaar, wanneer deze worden gepleegd door de ware identiteit van de dader te verhullen en de rechtmatige bezitter van de identiteit schade te berokkenen.

Artikel 11

Aansprakelijkheid van rechtspersonen

1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat rechtspersonen aansprakelijk kunnen worden gesteld voor de in de artikelen 3 tot en met 8 genoemde strafbare feiten wanneer die feiten tot hun voordeel zijn gepleegd door personen die hetzij individueel, hetzij als lid van een orgaan van de rechtspersoon optreden en die in de 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. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat rechtspersonen aansprakelijk kunnen worden gesteld indien het gebrek aan toezicht of controle door een in lid 1 bedoelde persoon het voor een persoon die onder het gezag van de rechtspersoon staat, mogelijk heeft gemaakt ten voordele van die rechtspersoon een van de in de artikelen 3 tot en met 8 bedoelde strafbare feiten te plegen.

3. De aansprakelijkheid van rechtspersonen krachtens de leden 1 en 2 sluit strafvervolging van natuurlijke personen die een in de artikelen 3 tot en met 8 bedoeld strafbaar feit plegen of eraan medeplichtig zijn, niet uit.

Artikel 12

Sancties tegen rechtspersonen

1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat tegen een rechtspersoon die uit hoofde van artikel 11, lid 1, aansprakelijk is gesteld, doeltreffende, evenredige en afschrikkende sancties kunnen worden vastgesteld, waaronder strafrechtelijke of niet-strafrechtelijke geldboetes en eventueel andere sancties, zoals:

   a) uitsluiting van door de overheid verleende voordelen of steun;

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

   c) plaatsing onder toezicht van de rechter;

   d) gerechtelijke ontbinding;

   e) tijdelijke of permanente sluiting van vestigingen die zijn gebruikt voor het plegen van het strafbare feit.

2. De lidstaten treffen de nodige maatregelen opdat tegen een rechtspersoon die volgens artikel 11, lid 2, aansprakelijk is, sancties kunnen worden vastgesteld of maatregelen kunnen worden getroffen die doeltreffend, evenredig en afschrikkend zijn.

Artikel 13
Rechtsmacht

1. Iedere lidstaat vestigt zijn rechtsmacht ten aanzien van de in de artikelen 3 tot en met 8 genoemde strafbare feiten indien deze:

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

   b) zijn gepleegd door een van zijn onderdanen of door een persoon die gewoonlijk op zijn grondgebied verblijft, of

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

2. Bij het vestigen van zijn rechtsmacht overeenkomstig lid 1, onder a), zorgt elke lidstaat ervoor dat deze 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 dat grondgebied, of

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

Artikel 14
Informatie-uitwisseling

1. Voor informatie-uitwisseling over strafbare feiten in de zin van de artikelen 3 tot en met 8 maken de lidstaten, met inachtneming van de regels inzake gegevensbescherming, gebruik van het bestaande netwerk van operationele meldpunten die vierentwintig uur per dag en zeven dagen per week bereikbaar zijn. De lidstaten zorgen er tevens voor dat zij over procedures beschikken waarmee zij binnen maximaal acht uur kunnen reageren op dringende verzoeken. In een dergelijke reactie wordt ten minste vermeld of en hoe het verzoek om bijstand wordt ingewilligd en wanneer.

2. De lidstaten stellen de Commissie in kennis van het meldpunt dat is aangewezen voor de informatie-uitwisseling over in de artikelen 3 tot en met 8 bedoelde strafbare feiten. De Commissie geeft deze informatie door aan de overige lidstaten.

Artikel 15
Toetsing en statistieken

1. De lidstaten zorgen voor een systeem voor het registreren, aanmaken en verstrekken van statistische gegevens over de in de artikelen 3 tot en met 8 bedoelde strafbare feiten.

2. De in lid 1 bedoelde statistieken vermelden ten minste het aantal in de artikelen 3 tot en met 8 bedoelde strafbare feiten die aan de lidstaten zijn gemeld en de follow-up

die aan deze meldingen is gegeven, alsmede – op jaarbasis – het aantal onderzochte meldingen, het aantal personen dat is vervolgd en het aantal personen dat is veroordeeld in verband met de in de artikelen 3 tot en met 8 bedoelde strafbare feiten.

3. De lidstaten verstrekken de overeenkomstig dit artikel verzamelde gegevens aan de Commissie. De lidstaten zorgen er tevens voor dat een geconsolideerd overzicht van hun statistische verslagen wordt gepubliceerd.

Artikel 16
Intrekking van Kaderbesluit 2005/222/JBZ

Kaderbesluit 2005/222/JBZ wordt hierbij ingetrokken, onverminderd de verplichtingen voor de lidstaten met betrekking tot de termijnen voor omzetting in de nationale wetgeving.

Verwijzingen naar het ingetrokken kaderbesluit gelden als verwijzingen naar deze richtlijn.

Artikel 17
Omzetting

1. De lidstaten doen de nodige wettelijke en bestuursrechtelijke bepalingen in werking treden om uiterlijk op [twee jaar na goedkeuring] aan deze richtlijn te voldoen. Zij delen de Commissie de tekst van die bepalingen onverwijld mede, alsmede een tabel ter weergave van het verband tussen die bepalingen en deze richtlijn. Wanneer de lidstaten deze bepalingen aannemen wordt in die bepalingen naar de onderhavige richtlijn verwezen of wordt hiernaar verwezen bij de officiële bekendmaking van die bepalingen. De regels voor deze verwijzing worden vastgesteld door de lidstaten.

2. De lidstaten delen de Commissie de tekst van de belangrijkste bepalingen van intern recht mede die zij op het onder deze richtlijn vallende gebied vaststellen.

Artikel 18
Verslaglegging

1. Uiterlijk op [VIER JAAR VANAF DE GOEDKEURING] en vervolgens om de drie jaar dient de Commissie bij het Europees Parlement en de Raad een verslag in over de tenuitvoerlegging van deze richtlijn, met de eventueel noodzakelijke voorstellen.

2. De lidstaten doen de Commissie alle informatie toekomen die zij nodig heeft voor het opstellen van het in lid 1 bedoelde verslag. De informatie omvat een uitvoerige beschrijving van de wetgevende en niet-wetgevende maatregelen die ter uitvoerlegging van deze richtlijn zijn vastgesteld.

Artikel 19
Inwerkingtreding

Deze richtlijn treedt in werking op de twintigste dag volgende op die van haar bekendmaking in het *Publicatieblad van de Europese Unie*.

Artikel 20
Adressaten

Deze richtlijn is overeenkomstig de Verdragen gericht tot de lidstaten.

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*