EUROPEES PARLEMENT 2009 - 2014

Zittingsdocument

A7-0224/2013

18.6.2013

***I
VERSLAG

over het 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
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Commissie burgerlijke vrijheden, justitie en binnenlandse zaken

Rapporteur: Monika Hohlmeier

Verklaring van de gebruikte tekens

*	Raadplegingsprocedure
***	Goedkeuringsprocedure
***I	Gewone wetgevingsprocedure (eerste lezing)
***II	Gewone wetgevingsprocedure (tweede lezing)
***III	Gewone wetgevingsprocedure (derde lezing)

(De aangeduide procedure is gebaseerd op de in de ontwerptekst voorgestelde rechtsgrond.)

Amendementen op een ontwerptekst

Door het Parlement aangebrachte wijzigingen op de ontwerptekst worden in ***vet cursief*** aangegeven. De markering in *mager cursief* is een aanwijzing voor de technische diensten en betreft passages in de ontwerptekst waarvoor een correctie wordt voorgesteld met het oog op de uiteindelijke tekst (bijvoorbeeld aperte fouten of weglatingen in een taalversie). Dergelijke correcties moeten worden goedgekeurd door de betrokken technische diensten.

In de koptekst van een amendement op een bestaande tekst, waarvoor in de ontwerptekst wijzigingen worden voorgesteld, wordt op respectievelijk de derde en vierde regel verwezen naar de bestaande tekst en naar de bepaling in kwestie. Tekstdelen die worden overgenomen uit een bepaling van een bestaande tekst die in de ontwerptekst niet is gewijzigd, maar door het Parlement wordt geamendeerd, worden in **vet** gemarkeerd. Een eventuele schrapping van dergelijke tekstdelen wordt als volgt aangegeven: **[...]**.

INHOUD

Blz.

ONTWERPWETGEVINGSRESOLUTIE VAN HET EUROPEES PARLEMENT 5

ADVIES VAN DE COMMISSIE BUITENLANDSE ZAKEN 39

ADVIES VAN DE COMMISSIE INDUSTRIE, ONDERZOEK EN ENERGIE 51

PROCEDURE 68

ONTWERPWETGEVINGSRESOLUTIE VAN HET EUROPEES PARLEMENT

over het 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
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

(Gewone wetgevingsprocedure: eerste lezing)

Het Europees Parlement,

– gezien het voorstel van de Commissie aan het Europees Parlement en de Raad (COM(2010)0517),

– gezien artikel 294, lid 2, en artikel 83, lid 1, van het Verdrag betreffende de werking van de Europese Unie, op grond waarvan het voorstel door de Commissie bij het Parlement is ingediend (C7-0293/2010),

– gezien artikel 294, lid 3, van het Verdrag betreffende de werking van de Europese Unie,

– gezien het advies van het Europees Economisch en Sociaal Comité van 4 mei 2011[1],

– gezien de schriftelijke toezegging van de vertegenwoordiger van de Raad van xxx om het standpunt van het Europees Parlement goed te keuren, overeenkomstig artikel 294, lid 4, van het Verdrag betreffende de werking van de Europese Unie,

– gezien artikel 55 van zijn Reglement,

– gezien het verslag van de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken en de adviezen van de Commissie buitenlandse zaken en de Commissie industrie, onderzoek en energie (A7-0224/2013),

1. stelt onderstaand standpunt in eerste lezing vast;

2. verzoekt om hernieuwde voorlegging indien de Commissie voornemens is ingrijpende wijzigingen in haar voorstel aan te brengen of dit door een nieuwe tekst te vervangen;

3. verzoekt zijn Voorzitter het standpunt van het Parlement te doen toekomen aan de Raad en aan de Commissie alsmede aan de nationale parlementen.

Amendement 129
Voorstel voor een richtlijn
–

[1] PB C 218 van 23.7.2011, blz. 130.

AMENDEMENTEN VAN HET EUROPEES PARLEMENT*

op het voorstel van de Commissie

Voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

over aanvallen op informatiesystemen en *ter vervanging*
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,[1]

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

Gezien het advies van het Europees Economisch en Sociaal Comité***[2]***,

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

Handelend volgens de gewone wetgevingsprocedure,

* Amendementen: nieuwe of vervangende tekst staat in vet en cursief, schrappingen zijn met het symbool ▌ aangegeven.

1 PB C […] van […], blz. […].

2 PB C […] van […], blz. […].

Overwegende hetgeen volgt:

(1) Deze richtlijn heeft ten doel ***de strafwetgeving*** van de lidstaten inzake aanvallen op informatiesystemen onderling af te stemmen ***door minimumvoorschriften vast te stellen voor de definitie van strafbare feiten en sancties op dit gebied***, ***en*** de samenwerking tussen ▌ de bevoegde autoriteiten, waaronder de politie en andere gespecialiseerde rechtshandhavingsinstanties van de lidstaten, ***alsook de bevoegde gespecialiseerde agentschappen van de Unie, zoals Eurojust, Europol en zijn Europees cybercriminaliteitscentrum, en het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa),*** te verbeteren.

(1 bis) Informatiesystemen zijn een essentieel onderdeel van de politieke, maatschappelijke en economische interactie in de Unie. De samenleving is sterk en in toenemende mate afhankelijk van dit soort systemen. De goede werking en de veiligheid van deze systemen in de Unie is cruciaal voor de ontwikkeling van de interne markt en van een concurrerende en innovatieve economie. Het waarborgen van passende beschermingsniveaus voor informatiesystemen dient deel uit te maken van een effectief alomvattend kader van preventieve maatregelen, in combinatie met strafrechtelijke reacties op cybercriminaliteit.

(2) Aanvallen op informatiesystemen, ***in het bijzonder in het kader van*** de georganiseerde criminaliteit, vormen een groeiende bedreiging, ***zowel in de Unie als in de rest van de wereld***, en de bezorgdheid over mogelijke terroristische of politiek gemotiveerde aanvallen op informatiesystemen die deel uitmaken van de kritieke 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 en ***betere internationale samenwerking en coördinatie*** noodzakelijk.

(2 bis) Ontwrichting of vernietiging van bepaalde kritieke infrastructuren in de Unie zou aanzienlijke grensoverschrijdende gevolgen hebben. Uit de behoefte aan een grotere capaciteit tot bescherming van de kritieke infrastructuur in de Unie blijkt dat de maatregelen tegen cyberaanvallen moeten worden aangevuld met zware strafrechtelijke sancties die in verhouding staan tot de ernst van deze aanvallen. Onder "kritieke infrastructuur" kan worden verstaan een voorziening, systeem of een deel daarvan op het grondgebied van een lidstaat dat van essentieel belang is voor bijvoorbeeld het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn van de bevolking, zoals energiecentrales, vervoersnetwerken of overheidsnetwerken, en waarvan de ontwrichting of vernietiging in een lidstaat aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken.

(3) Er zijn aanwijzingen dat grootschalige aanvallen op de informatiesystemen die ***vaak*** van vitaal belang ***kunnen zijn*** voor staten of voor specifieke functies van de publieke of particuliere sector steeds gevaarlijker en frequenter worden. Deze tendens gaat gepaard met de ontwikkeling van steeds geavanceerder ***methoden***, ***zoals het creëren en gebruiken van zogenaamde "botnets", waarbij de strafbare handeling in opeenvolgende fasen plaatsvindt en iedere fase afzonderlijk ernstig gevaar voor openbare belangen kan opleveren. In dit verband is de richtlijn er onder meer op gericht strafrechtelijke sancties in te voeren voor de fase waar de "botnet" wordt gecreëerd, namelijk wanneer controle op afstand over een aanzienlijk aantal computers tot stand wordt gebracht door deze door middel van gerichte cyberaanvallen te besmetten met kwaadaardige software. In een latere fase kan het netwerk van besmette computers, dat de "botnet" vormt, zonder medeweten van de gebruikers ervan worden ingezet om een grootschalige cyberaanval uit te voeren, die gewoonlijk het vermogen heeft om ernstige schade te veroorzaken als bedoeld in deze richtlijn. De lidstaten kunnen bepalen wat overeenkomstig hun nationaal recht en hun nationale praktijk onder ernstige schade wordt verstaan; het kan daarbij onder meer gaan om ontregelde systeemdiensten van groot openbaar belang, aanzienlijke financiële kosten of verlies van persoonsgegeven of gevoelige informatie.***

(3 bis) Grootschalige aanvallen kunnen ernstige economische schade veroorzaken doordat informatiesystemen uitvallen en de communicatie wordt onderbroken en doordat er commercieel belangrijke vertrouwelijke of andere gegevens verloren gaan of worden gewijzigd. Er dient met name op te worden gelet dat innovatieve kmo's bewuster worden gemaakt van bedreigingen en zwakke punten in dat verband, vanwege hun grotere afhankelijkheid van de goede werking en beschikbaarheid van informatiesystemen en hun vaak beperkte middelen voor informatiebeveiliging.

(4) Gemeenschappelijke definities op dit gebied 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 gemeenschappelijk begrip van de strafbare feiten "onrechtmatige toegang tot een informatiesysteem", "onrechtmatige systeemverstoring", "onrechtmatige gegevensverstoring" en "onrechtmatige onderschepping" worden ingevoerd.

(5 bis) Onderschepping omvat, maar is niet noodzakelijkerwijs beperkt tot, luisteren naar, monitoren van of houden van toezicht op de inhoud van communicaties, en het ofwel rechtstreeks, door middel van toegang tot en gebruik van de informatiesystemen, ofwel indirect, door middel van het gebruik van elektronische afluister- of aftapapparatuur, verkrijgen van de inhoud van gegevens.

(6) De lidstaten dienen aanvallen op informatiesystemen strafbaar te stellen. De straffen dienen doeltreffend, evenredig en afschrikkend te zijn ***en dienen gevangenisstraffen en/of geldboeten te omvatten.***

(6 bis) De richtlijn voorziet in elk geval in strafrechtelijke sancties voor gevallen die niet onbeduidend zijn. De lidstaten kunnen volgens hun nationaal recht en hun nationale praktijk bepalen welke gevallen onbeduidende gevallen zijn. Het geval kan bijvoorbeeld als onbeduidend worden beschouwd, wanneer de door het strafbare feit aangerichte schade en/of het risico dat het oplevert voor openbare of particuliere belangen, zoals de integriteit van een computersysteem of van computergegevens, of de integriteit, de rechten en andere belangen van een persoon, te verwaarlozen zijn of van dien aard zijn dat het opleggen van een strafrechtelijke sanctie binnen de door de wet bepaalde minima en maxima of het strafrechtelijk aansprakelijk stellen voor deze feiten niet noodzakelijk is.

(6 ter) Het onderkennen en rapporteren van bedreigingen en risico's die uitgaan van cyberaanvallen, alsook van zwakke punten van informatiesystemen in dat verband, is een belangrijk element om cyberaanvallen daadwerkelijk te voorkomen en te bestrijden en de beveiliging van informatiesystemen te verbeteren. Door het rapporteren van beveiligingslacunes te stimuleren kan op dit gebied nog meer effect worden gesorteerd. De lidstaten moeten mogelijkheden trachten aan te reiken voor de wettige opsporing en rapportering van beveiligingslacunes.

(7) Het is dienstig te voorzien in zwaardere straffen voor aanvallen op een informatiesysteem die gepleegd worden door een criminele organisatie in de zin van Kaderbesluit 2008/841/JBZ van de Raad van 24 oktober 2008 ter bestrijding van georganiseerde criminaliteit[1] , ***of*** voor grootschalige aanvallen, ***die een groot aantal informatiesystemen treffen of ernstige schade veroorzaken, met inbegrip van aanvallen die tot doel hebben een "botnet" te creëren of die worden uitgevoerd door middel van een "botnet", en aldus ernstige schade veroorzaken.*** Het is tevens dienstig te voorzien in zwaardere straffen voor aanvallen ***op een kritieke infrastructuur.***

(7 bis) Het nemen van doeltreffende maatregelen tegen identiteitsdiefstal en andere identiteitsgerelateerde strafbare feiten is een ander belangrijk onderdeel van een geïntegreerde aanpak van cybercriminaliteit. De behoefte aan een EU-optreden met betrekking tot dit soort crimineel gedrag kan eveneens worden nagegaan in het kader van het onderzoek naar de noodzaak van een alomvattend horizontaal EU-instrument.

(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 daarop voort. ***Het zo spoedig mogelijk afronden van het proces van ratificering van het verdrag door alle lidstaten moet derhalve als een prioriteit worden beschouwd.***

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

(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 die voor het creëren*** van botnets, waarmee cyberaanvallen worden gepleegd. ***Zelfs als een instrument geschikt of zelfs zeer geschikt is voor het plegen van bovengenoemde strafbare feiten, kan het toch voor legitieme doeleinden zijn vervaardigd. Aangezien strafbaarstelling moet worden voorkomen wanneer dergelijke instrumenten worden vervaardigd en in de handel worden gebracht voor legitieme doeleinden, zoals het testen van de betrouwbaarheid van informatietechnologieproducten of de beveiliging van informatiesystemen, moet er, naast het algemene oogmerk, ook sprake zijn van een direct oogmerk om deze instrumenten te gebruiken voor het plegen van een van de in de richtlijn vermelde strafbare feiten.***

I

(10 bis) ***Deze richtlijn beoogt niet de strafbaarstelling van feiten wanneer deze volgens de objectieve criteria voor misdrijven als vermeld in deze richtlijn zijn gepleegd, maar er geen sprake van crimineel opzet is, bijvoorbeeld wanneer een persoon zich er niet bewust van was dat de toegang niet was toegestaan, of in het geval van het gemachtigd testen of beschermen van informatiesystemen, bijvoorbeeld wanneer een persoon door een bedrijf of een verkoper is aangewezen om de sterkte van zijn beveiligingssysteem te testen. In de context van deze richtlijn mogen contractuele verplichtingen of overeenkomsten om de toegang tot informatiesystemen door middel van gebruikersbeleid of functievoorwaarden te beperken, alsook arbeidsconflicten met betrekking tot de toegang tot en het gebruik van informatiesystemen van de werkgever voor privégebruik, geen strafrechtelijke gevolgen hebben indien de toegang onder die omstandigheden ongeoorloofd wordt geacht en derhalve de enige grondslag voor een strafprocedure zou vormen. Deze richtlijn doet niet af aan het wettelijk gewaarborgd recht van toegang tot informatie zoals dat is vastgelegd in nationale en uniale wetgeving, maar dat recht mag tegelijkertijd niet worden ingeroepen om onrechtmatige en willekeurige toegang tot informatie te rechtvaardigen.***

(10 ter) ***Het plegen van cyberaanvallen kan door verschillende omstandigheden in de hand worden gewerkt, zoals wanneer de dader uit hoofde van zijn functie toegang heeft tot de beveiligingsmechanismen van de getroffen informatiesystemen. In het kader van het nationaal recht moet in strafprocedures naar behoren rekening worden gehouden met dergelijke omstandigheden.***

(10 quater) De lidstaten moeten in hun nationaal recht verzwarende omstandigheden opnemen overeenkomstig de in hun rechtsstelsels vastgestelde regels die hierop van toepassing zijn. Zij dienen ervoor te zorgen dat rechters deze verzwarende omstandigheden bij de veroordeling van daders kunnen laten meewegen. Het behoort tot de beoordelingsvrijheid van de rechter deze omstandigheden samen met de andere feitelijke elementen van de zaak te beoordelen.

(10 quienquies) Deze richtlijn betreft niet de voorwaarden waaraan voldaan dient te worden voor de uitoefening van rechtsmacht met betrekking tot een van de in de artikelen 3 tot en met 8 genoemde strafbare feiten, zoals een aangifte die door het slachtoffer is gedaan op de plaats waar de feiten zijn gepleegd, een aanklacht die is geformuleerd door de staat van de plaats waar de feiten zijn gepleegd of het feit dat de dader niet vervolgd is op de plaats waar de feiten zijn gepleegd.

(10 sexies) Staten en overheidslichamen moeten in het kader van deze richtlijn de eerbiediging van de mensenrechten en de fundamentele vrijheden onverkort blijven waarborgen, overeenkomstig bestaande internationale verplichtingen.

(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 bereikbaar zijn. ***Dergelijke meldpunten moeten daadwerkelijk bijstand kunnen verlenen en aldus bijvoorbeeld zorgen voor een vlottere uitwisseling van beschikbare relevante gegevens of een vlottere verstrekking van technisch advies of juridische informatie*** ten behoeve van onderzoeken of procedures inzake strafbare feiten ***op het gebied van*** informatiesystemen ***en daarmee samenhangende gegevens, die de verzoekende lidstaat aanbelangen. Met het oog op een goede werking van de netwerken moet elk meldpunt over de capaciteit beschikken om snel met het meldpunt van een andere lidstaat te communiceren, mede dankzij de ondersteuning van opgeleid en uitgerust personeel.*** Gelet op de snelheid waarmee grootschalige ***cyber***aanvallen kunnen worden uitgevoerd, dienen alle lidstaten onverwijld te kunnen reageren op dringende bijstandsverzoeken van dit netwerk van meldpunten. ***In zulke gevallen kan het dienstig zijn dat in het verzoek tot het verstrekken van gegevens een telefonisch te bereiken contactpersoon wordt vermeld, teneinde te waarborgen dat het verzoek spoedig door de aangezochte staat kan worden behandeld en dat binnen 8 uur feedback wordt gegeven.***

(11 bis) Om aanvallen op informatiesystemen te voorkomen en te bestrijden, is het van groot belang dat de overheidsinstanties samenwerken met de particuliere sector en de maatschappelijke organisaties. De samenwerking tussen dienstverleners, producenten, wetshandhavingsinstanties en justitiële autoriteiten moet worden gestimuleerd en verbeterd, met volledige inachtneming van de rechtsstaat. De samenwerking kan bijvoorbeeld steun door dienstverleners omvatten om mogelijk bewijsmateriaal te helpen bewaren, om elementen aan te leveren die kunnen helpen bij de identificatie van daders, en om, in laatste instantie, informatiesystemen of -functies die zijn besmet of voor illegale doeleinden zijn gebruikt, overeenkomstig de nationale wetgeving en praktijk volledig of gedeeltelijk buiten werking te stellen. De lidstaten moeten tevens de oprichting overwegen van netwerken voor samenwerking en partnerschappen met dienstverleners en producenten voor de uitwisseling van informatie in verband met strafbare feiten die onder het toepassingsgebied van deze richtlijn vallen.

I

(12 bis) ***Er moeten vergelijkbare gegevens over in deze richtlijn bedoelde strafbare feiten worden verzameld. Relevante gegevens moeten ter beschikking worden gesteld van de bevoegde gespecialiseerde agentschappen, zoals Europol en het Europees Agentschap voor netwerk- en informatiebeveiliging, naar gelang van hun taken en informatiebehoeften, opdat er een vollediger beeld ontstaat van de problematiek van cybercriminaliteit en netwerk- en informatiebeveiliging op het niveau van de Unie en er doeltreffender antwoorden kunnen worden geformuleerd. De lidstaten moeten aan Europol en zijn Europees centrum inzake cybercriminaliteit gegevens over de modus operandi van de daders verstrekken met het oog op dreigingsevaluatie en strategische analyses van cybercriminaliteit in overeenstemming met Besluit 2009/371/JBZ van de Raad. Het verstrekken van informatie kan een beter inzicht bevorderen in huidige en toekomstige dreigingen, en aldus bijdragen tot een meer passende en gerichte besluitvorming over het bestrijden en voorkomen van aanvallen op informatiesystemen.***

(12 ter) ***De Commissie moet op grond van deze richtlijn een verslag over de toepassing van de richtlijn presenteren en eventueel de nodige wetgevingsvoorstellen indienen die kunnen leiden tot een verruiming van de werkingssfeer ervan, rekening houdend met ontwikkelingen op het gebied van cybercriminaliteit. Deze ontwikkelingen kunnen technologische ontwikkelingen zijn, die bijvoorbeeld een effectievere handhaving op het gebied van aanvallen op informatiesystemen mogelijk maken, de voorkoming ervan vergemakkelijken of de gevolgen ervan tot een minimum beperken. Daartoe dient de Commissie rekening te houden met de beschikbare analyses en verslagen van betrokken actoren, meer bepaald Europol en Enisa.***

(12 quater) Om cybercriminaliteit op een effectieve manier te bestrijden, is het eveneens van belang de weerstandscapaciteit van informatiesystemen te verhogen door deze beter te beschermen tegen cyberaanvallen en de juiste maatregelen te nemen om dit te doen. De lidstaten moeten de nodige maatregelen treffen om kritieke infrastructuur te beschermen tegen cyberaanvallen, en in het kader daarvan moeten zij de bescherming van hun informatiesystemen en daarmee samenhangende gegevens overwegen. Het waarborgen van een passend niveau van bescherming en beveiliging van informatiesystemen door rechtspersonen, bijvoorbeeld in het kader van het verstrekken van openbaar beschikbare elektronische communicatiediensten overeenkomstig bestaande EU-wetgeving inzake de persoonlijke levenssfeer en elektronische communicatie en gegevensbescherming, is een wezenlijk bestanddeel van een alomvattende aanpak voor de doeltreffende bestrijding van cybercriminaliteit. Er moet worden gezorgd voor passende niveaus van bescherming tegen op een redelijke manier te identificeren dreigingen en kwetsbaarheden, overeenkomstig de allernieuwste technieken voor specifieke sectoren en specifieke gegevensverwerkingssituaties. De kosten en lasten van dergelijke bescherming dienen evenredig te zijn met de waarschijnlijke schade die een cyberaanval voor de betrokkenen veroorzaakt. De lidstaten worden ertoe aangemoedigd om in het kader van hun nationaal recht te voorzien in aansprakelijkheidsmaatregelen ingeval een rechtspersoon duidelijk geen passend niveau van bescherming tegen cyberaanvallen heeft ingesteld.

(13) Grote lacunes en verschillen in de wetgeving ***en de strafrechtelijke procedures*** 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 ***passende tenuitvoerlegging en toepassing*** van Kaderbesluit 2009/948/JBZ van de Raad over het voorkomen en beslechten van geschillen over de uitoefening van rechtsmacht bij strafprocedures. ***De lidstaten moeten in samenwerking met de Europese Unie tevens streven naar een betere internationale samenwerking op het gebied van de beveiliging van informatiesystemen, computernetwerken en computergegevens. In elke internationale overeenkomst waar gegevensuitwisseling mee gemoeid is, moet passende aandacht worden besteed aan de beveiliging van het verzenden en het opslaan van gegevens.***

(13 bis) Een verbeterde samenwerking tussen de bevoegde rechtshandhavingsinstanties en justitiële autoriteiten in de hele Unie is van wezenlijk belang voor de effectieve bestrijding van cybercriminaliteit. In dit verband moet er meer werk worden gemaakt van een passende opleiding voor de betrokken instanties, met als doel een beter begrip te kweken van cybercriminaliteit en de gevolgen daarvan, en samenwerking en uitwisseling van beste praktijken te bevorderen, bijvoorbeeld via de bevoegde gespecialiseerde EU-agentschappen. Die opleiding moet onder meer de verschillende nationale rechtsstelsels, de mogelijke juridische en technische moeilijkheden bij strafrechtelijke onderzoeken of de bevoegdheidsverdeling tussen de betrokken nationale autoriteiten beter onder de aandacht brengen.

(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.

I

(15 bis) De bescherming van persoonsgegevens is een grondrecht overeenkomstig artikel 16, lid 1, VWEU en artikel 8 van het Handvest van de grondrechten. Derhalve moet elke verwerking van persoonsgegevens in het kader van de uitvoering van deze richtlijn volledig voldoen aan de op grond van de Verdragen aangenomen EU-wetgeving inzake gegevensbescherming.

(16) Deze richtlijn eerbiedigt de fundamentele ***vrijheden en*** grondrechten en is in overeenstemming is met de beginselen die met name bij het Handvest van de grondrechten van de Europese Unie ***en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden*** zijn erkend, waaronder de bescherming van persoonsgegevens, ***de eerbiediging van de persoonlijke levenssfeer,*** de vrijheid van meningsuiting en van informatie, het recht op een eerlijk proces, het beginsel van het vermoeden van onschuld en de rechten van de verdediging, 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 artikel 3*** 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 ▌.

(18) Overeenkomstig de artikelen 1 en 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 aanneming van deze richtlijn die derhalve niet bindend is voor, noch van toepassing is in Denemarken.

(19) Deze richtlijn strekt tot wijziging en uitbreiding van de bepalingen van Kaderbesluit 2005/222/JBZ. Aangezien de aan te brengen wijzigingen talrijk en ingrijpend zijn, dient het kaderbesluit ter wille van de duidelijkheid integraal te worden vervangen voor de lidstaten die aan de aanneming van deze richtlijn deelnemen.

HEBBEN DE VOLGENDE RICHTLIJN VASTGESTELD:

Artikel 1

Onderwerp

I

Deze richtlijn stelt minimumvoorschriften vast voor de definitie van strafbare feiten en sancties op het gebied van aanvallen op informatiesystemen. Zij strekt er tevens toe de preventie van deze strafbare feiten te vergemakkelijken en de samenwerking tussen de justitiële en de andere bevoegde autoriteiten 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, verstoring, onderschepping of enige andere in deze richtlijn genoemde gedraging*** die niet is toegestaan door de eigenaar of een andere houder van rechten op het systeem of op een deel daarvan, of niet is toegestaan krachtens de nationale wetgeving.

Artikel 3

Onrechtmatige toegang tot informatiesystemen

De lidstaten treffen de nodige maatregelen om onrechtmatige toegang tot een informatiesysteem of tot een deel ervan, ***wanneer deze opzettelijk is geschied***, strafbaar te stellen ***wanneer het strafbaar feit is gepleegd door het overtreden van een beveiligingsmaatregel,*** althans voor gevallen die niet onbeduidend zijn.

Artikel 4

Onrechtmatige systeemverstoring

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

Artikel 7

Instrumenten voor het plegen van strafbare feiten

1. De lidstaten treffen de nodige ***maatregelen*** om de productie, de verkoop, de aanschaf voor gebruik, de invoer, ▌ de verspreiding of het op andere wijze beschikbaar maken van de volgende zaken, indien dat opzettelijk en op onrechtmatige wijze geschiedt, ***met het oogmerk deze te gebruiken*** voor het plegen van een van de in de artikelen 3 tot en met ***6*** bedoelde feiten, strafbaar te stellen, ***althans voor gevallen die niet onbeduidend zijn***:

a) ▌ 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**, hulp **en** medeplichtigheid en poging*

1. De lidstaten zorgen ervoor dat ***uitlokking*** van, alsmede hulp 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 4 en 5*** genoemde ***feiten*** strafbaar wordt gesteld.

Artikel 9

Sancties

1. De lidstaten treffen 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 treffen 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, althans voor gevallen die niet onbeduidend zijn.***

3. ***De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 4 en 5 bedoelde feiten, wanneer deze opzettelijk worden gepleegd, strafbaar worden gesteld met een maximale gevangenisstraf van ten minste drie jaar, wanneer een groot aantal informatiesystemen getroffen zijn door het gebruik van een in artikel 7, lid 1, bedoeld instrument, dat hoofdzakelijk voor dit doel is ontworpen of aangepast.***

4. ***De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 4 en 5 bedoelde feiten strafbaar worden gesteld met een maximale gevangenisstraf van ten minste vijf jaar wanneer het strafbare feit***

a) ***is gepleegd in het kader van een criminele organisatie zoals omschreven in Kaderbesluit 2008/814/JBZ van de Raad, ongeacht de daarin aangegeven strafmaat, of***

b) ***ernstige schade heeft teweeggebracht, of***

c) ***is gepleegd tegen een informatiesysteem dat deel uitmaakt van de kritieke infrastructuur.***

5. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat wanneer de in de artikelen 4 en 5 bedoelde strafbare feiten worden gepleegd door de persoonsgegevens van een andere persoon te misbruiken met het oogmerk het vertrouwen van een derde partij te winnen, waardoor de rechtmatige bezitter van een identiteit schade wordt berokkend, dit overeenkomstig de betrokken bepalingen van het nationaal recht kan worden beschouwd als verzwarende omstandigheden, tenzij deze omstandigheden reeds worden bestreken door een ander feit dat overeenkomstig het nationaal recht strafbaar is.

I

Artikel 11

Aansprakelijkheid van rechtspersonen

1. De lidstaten treffen 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 treffen 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, ***uitlokken*** of eraan medeplichtig zijn, niet uit.

Artikel 12

Sancties tegen rechtspersonen

1. De lidstaten treffen 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

(a bis) door een van zijn onderdanen zijn gepleegd, in elk geval voor zover het feit een strafbaar feit is op de plaats waar het is gepleegd.

I

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.

3. ***Elke lidstaat stelt de Commissie in kennis van zijn besluit om ook zijn rechtsmacht te vestigen over een strafbaar feit in de zin van de artikelen 3 en 8 dat buiten zijn grondgebied is gepleegd, bijvoorbeeld indien het strafbare feit is gepleegd:***

a) ***door iemand die gewoonlijk op zijn grondgebied verblijft; of***

b) ***ten voordele van een rechtspersoon die gevestigd is op het grondgebied van die lidstaat.***

Artikel 14

Uitwisseling van informatie

1. Voor informatie-uitwisseling over strafbare feiten in de zin van de artikelen 3 tot en met 8 ***zorgen de lidstaten ervoor dat zij beschikken over een operationeel nationaal meldpunt en gebruik***maken 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 ***in geval van dringende verzoeken binnen maximaal acht uur ten minste kunnen aangeven of het verzoek om bijstand zal worden ingewilligd, alsmede de vorm en het tijdstip waarop dit naar verwachting zal gebeuren.***

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 ***en aan de bevoegde gespecialiseerde EU-agentschappen en -organen.***

3. De lidstaten treffen de nodige maatregelen om ervoor te zorgen dat passende rapportagekanalen ter beschikking worden gesteld om het rapporteren zonder onnodige vertraging van de in de artikelen 3 tot en 6 genoemde strafbare feiten aan de bevoegde nationale autoriteiten te vergemakkelijken.

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 7*** bedoelde strafbare feiten.

2. De in lid 1 bedoelde statistieken vermelden ten minste de ***beschikbare gegevens over*** het aantal in de artikelen 3 tot en met ***7*** bedoelde strafbare feiten die ***door*** de lidstaten ***zijn geregistreerd*** en ▌ het aantal personen dat is ***vervolgd en veroordeeld*** in verband met de in de artikelen 3 ***tot en met 7*** bedoelde strafbare feiten.

3. De lidstaten verstrekken de overeenkomstig dit artikel verzamelde gegevens aan de Commissie. ***De Commissie zorgt ervoor*** dat een geconsolideerd overzicht van hun statistische verslagen wordt gepubliceerd ***en aan de bevoegde gespecialiseerde EU-agentschappen en organen wordt toegezonden.***

Artikel 16

Vervanging *van Kaderbesluit 2005/222/JBZ*

Kaderbesluit 2005/222/JBZ wordt hierbij ***vervangen voor de lidstaten die aan de aanneming van deze richtlijn deelnemen***, onverminderd de verplichtingen van de lidstaten wat betreft de ***termijn*** voor de omzetting ***van het kaderbesluit*** in nationaal recht.

Voor lidstaten die aan de aanneming van deze richtlijn deelnemen, worden verwijzingen naar Kaderbesluit ***2005/222/JBZ*** gelezen 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 aanneming] aan deze richtlijn te voldoen ▌.

▌

3. De lidstaten delen aan de Commissie de tekst mede van alle bepalingen waarmee zij hun verplichtingen uit hoofde van deze richtlijn in hun nationaal recht omzetten.

4. Wanneer de lidstaten deze bepalingen aannemen, wordt in de bepalingen zelf of bij de officiële bekendmaking daarvan naar deze richtlijn verwezen. De regels voor deze verwijzing worden vastgesteld door de lidstaten.

Artikel 18

Verslaglegging

▌

De Commissie dient uiterlijk op [VIER JAAR NA AANNEMING] bij het Europees Parlement en de Raad een verslag in waarin wordt beoordeeld in hoeverre de lidstaten de nodige maatregelen hebben genomen om aan deze richtlijn te voldoen, indien nodig vergezeld van wetgevingsvoorstellen. In dit verband houdt de Commissie tevens rekening met de technische en juridische ontwikkelingen op het vlak van cybercriminaliteit, met name met betrekking tot het toepassingsgebied van deze richtlijn.

▌

Artikel 19

Inwerkingtreding

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

Artikel 20

Adressaten

Deze richtlijn is overeenkomstig de Verdragen gericht tot de lidstaten.

28.11.2011

ADVIES VAN DE COMMISSIE BUITENLANDSE ZAKEN

aan de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken

over het 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 (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Rapporteur voor advies: Kristiina Ojuland

BEKNOPTE MOTIVERING

De rapporteur voor advies is vast overtuigd van de noodzaak van een betere uitwisseling van informatie over cyberveiligheid tussen de lidstaten tegen de achtergrond van een groeiende bezorgdheid over mogelijke cyberaanvallen. De kwestie van cyberveiligheid moet echt dringend worden aangepakt op EU-niveau en door middel van gecoördineerde acties van de lidstaten.

Het advies onderstreept de rol van de Commissie om de bevordering en coördinatie van de bestaande initiatieven te vergemakkelijken.

De Commissie buitenlandse zaken en de Subcommissie veiligheid en defensie hechten veel belang aan de dringende noodzaak om op te treden en de coördinatie van de reacties, initiatieven en programma's op EU-niveau te versterken. Er dient steun te worden verleend aan de ontwikkeling van capaciteit en nauwere samenwerking om het niveau van informatieveiligheid te verhogen.

De rapporteur voor advies steunt het idee om een EU-coördinator voor cyberveiligheid aan te stellen om de integratie en coördinatie van verschillende Europese activiteiten en initiatieven op EU-niveau en tussen de EU-instellingen te vergemakkelijken.

AMENDEMENTEN

De Commissie buitenlandse zaken verzoekt de ten principale bevoegde Commissie burgerlijke vrijheden, justitie en binnenlandse zaken onderstaande amendementen in haar verslag op te nemen:

Amendement 1

Voorstel voor een richtlijn
Overweging 1

Door de Commissie voorgestelde tekst	*Amendement*
(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.	(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 ***en de Unie***, te verbeteren***. Deze doelstelling past binnen de algemene strategie van de EU om georganiseerde criminaliteit te bestrijden, informatienetwerken doeltreffender te beveiligen en de bescherming van vitale informatie-infrastructuur en van gegevens te waarborgen.***

Amendement 2

Voorstel voor een richtlijn
Overweging 1 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(1 bis) Informatiesystemen zijn cruciaal voor de politieke, sociale en economische interactie in de Unie. De samenleving is in toenemende mate afhankelijk van informatiesystemen. Deze systemen houden naast grote voordelen echter ook een aantal risico's in voor onze veiligheid, omwille van hun complexe structuur en hun kwetsbaarheid ten aanzien van allerlei vormen van cybercriminaliteit. De veiligheid van informatiesystemen vormt dan ook een voortdurend zorgpunt en dit noopt de lidstaten en de Unie tot doeltreffende maatregelen.

Amendement 3

Voorstel voor een richtlijn
Overweging 2

Door de Commissie voorgestelde tekst	*Amendement*
(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.	(2) Aanvallen op informatiesystemen vormen een groeiende bedreiging. ***Zij kunnen uitgaan van terroristische organisaties of van de georganiseerde misdaad en kunnen worden uitgevoerd door staten of individuele personen.*** 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. ***Het grensoverschrijdende karakter van sommige aanvallen en het feit dat de daders relatief weinig risico lopen en met een beperkte investering een hoog rendement kunnen halen en veel schade kunnen aanrichten, verhoogt de kans op dergelijke aanvallen aanzienlijk.*** Dit brengt de totstandbrenging van een veiliger informatiemaatschappij en een ruimte van vrijheid, veiligheid en recht in gevaar en maakt derhalve een reactie ***niet alleen*** op het niveau van de Europese Unie ***maar ook van de internationale gemeenschap*** noodzakelijk.

Amendement 4

Voorstel voor een richtlijn
Overweging 3

Door de Commissie voorgestelde tekst	*Amendement*
(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	(3) Er zijn aanwijzingen dat grootschalige aanvallen op de informatiesystemen die van vitaal belang zijn voor ***lidstaten, voor de Unie*** of voor specifieke onderdelen van de publieke of particuliere sector ***alsook op het niveau van de Unie,*** steeds gevaarlijker en frequenter worden. Deze tendens gaat gepaard met de ***snelle*** ontwikkeling van ***computertechnologie en bijgevolg van*** telkens geavanceerder instrumenten die

voeren.	door criminelen kunnen worden gebruikt om diverse soorten cyberaanvallen uit te voeren***, waarvan sommige zo krachtig zijn dat ze economische en sociale schade kunnen aanrichten***.

Amendement 5

Voorstel voor een richtlijn
Overweging 4 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(4 bis) Het algemene niveau van de dreiging die van aanvallen tegen informatiesystemen uitgaat, moet op een grondige, betrouwbare en onafhankelijke manier worden onderzocht. De instellingen van de Unie moeten hun niveau van informatiebeveiliging in het licht daarvan aanpassen.

Amendement 6

Voorstel voor een richtlijn
Overweging 4 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(4 ter) Er is coördinatie op het niveau van de Unie nodig om de integratie van de verschillende initiatieven, programma's en activiteiten te bevorderen.

Amendement 7

Voorstel voor een richtlijn
Overweging 6

Door de Commissie voorgestelde tekst	*Amendement*
(6) De lidstaten dienen aanvallen op informatiesystemen strafbaar te stellen. De straffen dienen doeltreffend, evenredig en afschrikkend te zijn.	(6) De lidstaten dienen aanvallen op informatiesystemen strafbaar te stellen***, als onderdeel van een ruimere nationale strategie die dit soort aanvallen moet beletten en bestrijden.*** De straffen dienen

doeltreffend, evenredig en afschrikkend te zijn. ***Gezien het grensoverschrijdende karakter van de dreiging moeten de lidstaten hun sancties en straffen harmoniseren en zodoende de onderlinge verschillen inzake hun behandeling van inbreuken in de gehele Unie wegwerken.***

Amendement 8

Voorstel voor een richtlijn
Overweging 8 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(8 bis) De Raad en de Commissie moeten de lidstaten die het Verdrag inzake cybercriminaliteit van de Raad van Europa nog niet hebben geratificeerd, ertoe aansporen dit zo snel mogelijk te doen.

Amendement 9

Voorstel voor een richtlijn
Overweging 11 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(11 bis) Om cyberaanvallen te voorkomen en te bestrijden, is samenwerking van de autoriteiten met de particuliere sector en het maatschappelijk middenveld van groot belang. Een voortdurende dialoog met deze actoren is nodig, aangezien zij op grote schaal gebruik maken van computersystemen en de betrouwbaarheid en doelmatigheid van de systemen enkel kan gegarandeerd worden bij een gedeelde verantwoordelijkheid. Het komt erop aan alle belanghebbenden bewust te maken van het probleem om op die manier een cultuur van informatiebeveiliging te creëren.

Amendement 10

Voorstel voor een richtlijn
Overweging 11 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(11 ter) Recente initiatieven en projecten in verband met cyberverdediging, bijvoorbeeld in het kader van het Europees Defensieagentschap (EDA), moeten worden aangemoedigd om de cyberverdedigingscapaciteit van de lidstaten te steunen. Er moet worden overwogen nauwer samen te werken met het EDA en het Cooperative Cyber Defence Centre of Excellence van de NAVO, vooral op het gebied van capaciteitsopbouw en opleiding.

Amendement 11

Voorstel voor een richtlijn
Overweging 12

Door de Commissie voorgestelde tekst	*Amendement*
(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.	(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. ***De lidstaten moeten met steun van de Commissie en het Europees Agentschap voor netwerk- en informatiebeveiliging op grotere schaal informatie over cyberaanvallen uitwisselen.*** Met behulp van deze gegevens kunnen gespecialiseerde agentschappen als Europol en het Europees Agentschap voor netwerk- en informatiebeveiliging de omvang ***en de impact*** van cybercriminaliteit en de netwerk- en informatiebeveiliging in Europa bovendien beter beoordelen. ***Hoe meer bekend is over de huidige en toekomstige gevaren van cyberaanvallen, hoe gemakkelijker het***

	wordt om ze op een doeltreffende manier te beletten en te bestrijden, of om de aangerichte schade te beperken.

Amendement 12

Voorstel voor een richtlijn
Overweging 12 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(12 bis) De informatie-uitwisseling en publiek-private partnerschappen (PPP) spelen een belangrijke rol bij het verbeteren van de cyberveiligheid. De Commissie moet dan ook onderzoeken of het haalbaar is een kader of instrumenten te verschaffen om publiek-private partnerschappen met elkaar te laten samenwerken op nationaal niveau en het niveau van de Unie, om kwaliteitsnormen voor informatie vast te stellen met het oog op interoperabiliteit, en om te garanderen dat de grondrechten, de scheiding der machten en de democratische controle geëerbiedigd worden.

Amendement 13

Voorstel voor een richtlijn
Overweging 13

Door de Commissie voorgestelde tekst	*Amendement*
(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	(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.	behoefte bestaat aan verdere onderlinge afstemming ***op het niveau van de Unie*** van het strafrecht op dit gebied. ***De Unie moet ook streven naar meer internationale samenwerking op het gebied van informatienetwerkbeveiliging door nauw samen te werken met andere organisaties met een relevant mandaat, zoals de Verenigde Naties, de NAVO, de Raad van Europa of de OVSE, en door hier andere internationale actoren bij te betrekken.*** 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.

Amendement 14

Voorstel voor een richtlijn
Overweging 16

Door de Commissie voorgestelde tekst	*Amendement*
(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 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.	(16) Deze richtlijn ***en alle praktische toepassingen ervan eerbiedigen*** de grondrechten***, in het bijzonder het recht op privacy,*** en ***zijn*** 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 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. ***Deze richtlijn raakt niet aan de vrije en open aard van het internet.***

Amendement 15

Voorstel voor een richtlijn
Overweging 16 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(16 bis) De Raad en de Commissie moeten bij onderhandelingen en in de loop van de samenwerking met derde landen aandringen op minimumvoorschriften voor het voorkomen en bestrijden van cybercriminaliteit en cyberaanvallen, alsook op minimumnormen voor de beveiliging van informatiesystemen.

Amendement 16

Voorstel voor een richtlijn
Overweging 16 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(16 ter) De Commissie moet nagaan wat de mogelijkheden zijn om derde landen te helpen en bij te staan bij de ontwikkeling van hun capaciteit inzake cyberveiligheid en cyberverdediging.

Amendement 17

Voorstel voor een richtlijn
Artikel 14 – lid 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	2 bis. De Commissie helpt de lidstaten bij het bevorderen van de veerkracht en de stabiliteit van het internet en neemt ook andere initiatieven met het oog op meer informatieveiligheid.

Amendement 18

Voorstel voor een richtlijn
Artikel 14 – lid 2 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	2 ter. De Raad geeft toelichting bij de rol van het Politiek en Veiligheidscomité en van zijn andere organen in de context van de aanpak van mogelijke cyberaanvallen.

Amendement 19

Voorstel voor een richtlijn
Artikel 14 – lid 2 quater (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	2 quater. De lidstaten zorgen voor een betere uitwisseling van informatie inzake cyberveiligheid. De lidstaten streven met de steun van de Commissie naar interacties met derde landen, met name die landen van waaruit het vaakst cyberaanvallen komen.

Amendement 20

Voorstel voor een richtlijn
Artikel 15 – lid 3

Door de Commissie voorgestelde tekst	*Amendement*
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.	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 ***aan het Europees Parlement wordt verstrekt en*** wordt gepubliceerd.

Amendement 21

Voorstel voor een richtlijn
Artikel 15 – lid 3 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	3 bis. Er moet een EU-coördinator voor cyberveiligheid worden aangesteld om de integratie en coördinatie van de initiatieven, programma's en activiteiten van de instellingen van de Unie te bevorderen.

PROCEDURE

Titel	Aanvallen op informatiesystemen en intrekking van Kaderbesluit 2005/222/JBZ van de Raad
Document- en procedurenummers	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Commissie ten principale Datum bekendmaking	LIBE 7.10.2010
Medeadviserende commissie(s) Datum bekendmaking	AFET 7.4.2011
Rapporteur(s) Datum benoeming	Kristiina Ojuland 29.3.2011
Datum goedkeuring	22.11.2011
Uitslag eindstemming	+: 38 –: 8 0: 0
Bij de eindstemming aanwezige leden	Sir Robert Atkins, Frieda Brepoels, Elmar Brok, Marietta Giannakou, Andrzej Grzyb, Takis Hadjigeorgiou, Anna Ibrisagic, Othmar Karas, Ioannis Kasoulides, Tunne Kelam, Evgeni Kirilov, Andrey Kovatchev, Eduard Kukan, Krzysztof Lisek, Sabine Lösing, Ulrike Lunacek, Barry Madlener, Francisco José Millán Mon, Annemie Neyts-Uyttebroeck, Raimon Obiols, Justas Vincas Paleckis, Ioan Mircea Paşcu, Cristian Dan Preda, Libor Rouček, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Marek Siwiec, Charles Tannock, Inese Vaidere, Kristian Vigenin, Sir Graham Watson
Bij de eindstemming aanwezige vaste plaatsvervanger(s)	Laima Liucija Andrikienė, Elena Băsescu, Tanja Fajon, Diogo Feio, Monica Luisa Macovei, Emilio Menéndez del Valle, György Schöpflin, Traian Ungureanu, Ivo Vajgl, Renate Weber, Janusz Władysław Zemke
Bij de eindstemming aanwezige plaatsvervanger(s) (art. 187, lid 2)	Luís Paulo Alves, Sylvie Guillaume, Vladimir Urutchev

11.11.2011

ADVIES VAN DE COMMISSIE INDUSTRIE, ONDERZOEK EN ENERGIE

aan de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken

over het 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 (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Rapporteur voor advies: Christian Ehler

AMENDEMENTEN

De Commissie industrie, onderzoek en energie verzoekt de ten principale bevoegde Commissie burgerlijke vrijheden, justitie en binnenlandse zaken onderstaande amendementen in haar verslag op te nemen:

Amendement 1

Voorstel voor een richtlijnOverweging 1 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
(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.	(1) Deze richtlijn ***die deel vormt van de algemene strategie van de Unie ter bestrijding van de georganiseerde misdaad, verhoging van de veerkracht van computernetwerken, bescherming van vitale informatie-infrastructuren en gegevensbescherming,*** heeft ten doel de strafrechtelijke bepalingen van de lidstaten inzake aanvallen op informatiesystemen onderling af te stemmen en de samenwerking *te verbeteren* tussen justitiële en andere bevoegde autoriteiten, zoals de politie, andere gespecialiseerde rechtshandhavingsinstanties van de

	lidstaten, ***alsmede de Commissie, Eurojust, Europol, nationale en EU-computernoodhulpteams en het Europees Agentschap voor netwerk- en informatiebeveiliging, teneinde een gezamenlijke en omvattende benadering van de Unie mogelijk te maken***.

Amendement 2

Voorstel voor een richtlijn
Overweging 1 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(1 bis) Informatiesystemen zijn een essentieel onderdeel van de politieke, maatschappelijke en economische interactie in Europa. De samenleving is sterk en in toenemende mate afhankelijk van dit soort systemen. De goede werking en de veiligheid van deze systemen in Europa is essentieel voor de ontwikkeling van de interne markt en van een concurrerende en innovatieve economie. Informatiesystemen bieden grote voordelen, maar houden tegelijk een aantal risico's voor onze veiligheid in door hun complexiteit en kwetsbaarheid voor verschillende soorten computercriminaliteit. Daarom is de veiligheid van informatiesystemen een voortdurend punt van zorg dat van de lidstaten en de Unie een doeltreffende reactie vergt.

Amendement 3

Voorstel voor een richtlijn
Overweging 2

Door de Commissie voorgestelde tekst	*Amendement*
(2) Aanvallen op informatiesystemen, in het bijzonder in het kader van de georganiseerde criminaliteit, vormen een groeiende bedreiging en de bezorgdheid	(2) Aanvallen op informatiesystemen ***kunnen uit verschillende hoeken komen, bijvoorbeeld terroristen,*** georganiseerde criminaliteit, ***staten of geïsoleerde***

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.***

individuen. Zij vormen een groeiende bedreiging ***van de werking van informatiesystemen in de Unie en in de rest van de wereld,*** 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. ***De grensoverschrijdende aard van bepaalde misdrijven en het relatief lage risico en de relatief lage kosten voor de daders, samen met het enorme profijt dat zij uit de aanvallen kunnen trekken en de schade die zij ermee kunnen veroorzaken, maken de bedreiging nog veel groter.*** Dit brengt de totstandbrenging van een veiliger informatiemaatschappij en een ruimte van vrijheid, ***democratie,*** veiligheid en recht in gevaar***, ondermijnt de totstandbrenging van een Europese digitale interne markt,*** en *vergt* derhalve een reactie op het niveau van de Europese Unie ***en op internationaal niveau, bijvoorbeeld via het Verdrag inzake cybercriminaliteit van de Raad van Europa van 2001***.

Amendement 4

Voorstel voor een richtlijn
Overweging 2 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(2 bis) Recente cyberaanvallen op Europese netwerken of informatiesystemen hebben de economie en de veiligheid van de Unie aanzienlijke schade toegebracht.

Motivering

Naar aanleiding van de cyberaanvallen op de Europese instellingen van maart 2011 en de talrijke "inbraken" in de Europese emissiehandelssystemen, waarbij telkens voor miljoenen euro's emissierechten zijn gestolen.

Amendement 5

Voorstel voor een richtlijn
Overweging 3

Door de Commissie voorgestelde tekst	*Amendement*
(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.	(3) Er zijn aanwijzingen dat grootschalige aanvallen***, o.m. via distributed denial-of-service attacks*** op de informatiesystemen die van vitaal belang zijn voor ***internationale organisaties, voor*** staten , voor de Unie of voor specifieke onderdelen van de publieke of particuliere sector steeds gevaarlijker en frequenter worden. ***Deze aanvallen kunnen ernstige economische schade veroorzaken doordat informatiesystemen uitvallen en de communicatie wordt onderbroken en doordat er commercieel belangrijke vertrouwelijke of andere gegevens verloren gaan of worden gewijzigd. Het gevaar bestaat dat met name het innovatief MKB schade ondervindt, daar dit afhankelijk is van het naar behoren functioneren en de beschikbaarheid van informatiesystemen, terwijl het mogelijk minder fondsen kan bestemmen voor de veiligheid van informatie.*** Deze tendens gaat gepaard met de ***snelle*** ontwikkeling van de informatietechnologie en dus van telkens geavanceerder instrumenten die door criminelen kunnen worden gebruikt om diverse soorten cyberaanvallen uit te voeren, ***waarvan sommige grote economische en maatschappelijke schade kunnen veroorzaken.***

Amendement 6

Voorstel voor een richtlijn
Overweging 4

Door de Commissie voorgestelde tekst	*Amendement*
(4) Gemeenschappelijke definities op dit gebied, en in het bijzonder van informatiesystemen en computergegevens,	(4) Gemeenschappelijke definities op dit gebied, en in het bijzonder van informatiesystemen, computergegevens en

zijn van belang om te garanderen dat de richtlijn in de lidstaten coherent wordt toegepast.	***tegen informatiesystemen en gegevens gerichte strafbare handelingen,*** zijn van ***wezenlijk*** belang om te garanderen dat de richtlijn in de lidstaten coherent ***en uniform*** wordt toegepast.

Amendement 7

Voorstel voor een richtlijn
Overweging 6

Door de Commissie voorgestelde tekst	*Amendement*
(6) De lidstaten *dienen* aanvallen op informatiesystemen ***strafbaar te stellen***. De straffen dienen doeltreffend, evenredig en afschrikkend te zijn.	(6) ***In aanvulling op maatregelen van de lidstaten, de Unie en de particuliere sector die gericht zijn op vergroting van de veiligheid en niet-aantasting van informatiesystemen, voorkoming van aanvallen en optimale beperking van de gevolgen daarvan*** *dienen* de lidstaten ***doeltreffende maatregelen te nemen om dergelijke aanvallen te voorkomen en om geharmoniseerde straffen te bepalen voor*** aanvallen op informatiesystemen***. Deze moeten worden vastgesteld in het kader van ruimere nationale strategieën ter afschrikking en bestrijding van dit soort aanvallen***. De straffen dienen doeltreffend, evenredig en afschrikkend te zijn. ***Onderlinge afstemming van de sancties en straffen van de lidstaten is noodzakelijk omdat de bedreigingen vaak grensoverschrijdend zijn, en beoogt de verschillen tussen de lidstaten te verkleinen als het erop aankomt misdrijven aan te pakken die in de Unie worden begaan.***

Amendement 8

Voorstel voor een richtlijn
Overweging 6 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(6 bis) De lidstaten, de Unie en de particuliere sector moeten in

	samenwerking met het Europees Agentschap voor netwerk- en informatiebeveiliging maatregelen nemen om de veiligheid en integriteit van informatiesystemen te vergroten, aanvallen te voorkomen en de gevolgen daarvan tot een minimum te beperken.

Amendement 9

Voorstel voor een richtlijn
Overweging 8

Door de Commissie voorgestelde tekst	*Amendement*
(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.	(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. ***De Raad en de Commissie moeten de lidstaten die dit Verdrag nog niet hebben geratificeerd, aansporen om dat zo spoedig mogelijk te doen.*** Dat Verdrag is het wettelijke referentiekader voor de bestrijding van cybercriminaliteit, waaronder aanvallen op informatiesystemen. In deze richtlijn wordt rekening gehouden met de desbetreffende bepalingen in dat Verdrag.

Amendement 10

Voorstel voor een richtlijn
Overweging 10

Door de Commissie voorgestelde tekst	*Amendement*
(10) Deze richtlijn beoogt niet de strafbaarstelling van feiten die gepleegd worden zonder criminele opzet, zoals het officieel testen of beveiligen van informatiesystemen.	(10) Deze richtlijn ***is niet van toepassing op maatregelen ter waarborging van de veiligheid van informatiesystemen, bij voorbeeld het vermogen van een informatiesysteem misdadige handelingen zoals in onderhavige richtlijn omschreven te weerstaan, of om instrumenten te***

verwijderen die voor dergelijke handelingen gebruikt of bestemd zijn. Evenmin beoogt ***zij*** strafbaarstelling van feiten die gepleegd worden ***volgens de objectieve normen van de in deze richtlijn opgesomde misdrijven maar*** zonder criminele opzet, zoals het officieel testen of beveiligen van informatiesystemen

Motivering

Daar de grens tussen kwaadwillige toegang en niet-kwaadwillige toegang (automatische updates enz.) vaag is, beoogt het amendement duidelijk te maken dat bij voorbeeld de toepassing van virusbestrijdende software of instrumenten om virussen te verwijderen, of het in quarantaine plaatsen van besmette apparatuur geheel en al buiten het toepassingsgebeid van deze richtlijn vallen.

Amendement 11

Voorstel voor een richtlijn
Overweging 11

Door de Commissie voorgestelde tekst	*Amendement*
(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 gegevens, het verzamelen van bewijs, het verstrekken van juridische informatie, het	(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 bewijs voor een strafbaar feit of een poging tot het begaan van een strafbaar feit. Gelet op de snelheid waarmee grootschalige aanvallen kunnen worden uitgevoerd, dienen alle lidstaten, ***de EU en het Europees Agentschap voor netwerk- en informatiebeveiliging*** onverwijld ***en doeltreffend*** 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

identificeren van de ***beschadigde*** en/of buitgemaakte informatie, en het lokaliseren van verdachten.	technisch advies ***o.m. met betrekking tot het herstel van de werking van het informatiesysteem***, het bewaren van gegevens ***overeenkomstig de beginselen inzake de bescherming van persoonlijke gegevens***, het verzamelen van bewijs, het verstrekken van juridische informatie, het identificeren van de ***in gevaar gebrachte*** en/of buitgemaakte informatie, en het lokaliseren ***en identificeren*** van verdachten.

Amendement 12

Voorstel voor een richtlijn
Overweging 11 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(11 bis) Om aanvallen op informatiesystemen te voorkomen en te bestrijden, is het van groot belang dat de overheidsinstanties samenwerken met de particuliere sector en de maatschappelijke organisaties. Met deze partners moet permanent overleg worden gevoerd omdat zij veel gebruik maken van informatiesystemen en omdat de stabiliteit en de goede werking van deze systemen een gedeelde verantwoordelijkheid vereist. Bewustmaking van alle partijen die bij het gebruik van informatiesystemen betrokken zijn, is belangrijk om een cultuur van IT-veiligheid tot stand te brengen.

Amendement 13

Voorstel voor een richtlijn
Overweging 12

Door de Commissie voorgestelde tekst	*Amendement*
(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	(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.

niveau van de Unie en er doeltreffender antwoorden kunnen worden geformuleerd. ***De lidstaten moeten de uitwisseling van informatie over aanvallen op informatiesystemen verbeteren met ondersteuning van de Commissie en het Europees Agentschap voor netwerk- en informatiebeveiliging.*** Met behulp van deze gegevens kunnen gespecialiseerde ***organen en*** agentschappen ***zoals de responsteams voor computernoodgevallen (CERT's, agentschappen zo***als Europol en het Europees Agentschap voor netwerk- en informatiebeveiliging de omvang van cybercriminaliteit en de netwerk- en informatiebeveiliging in ***de Unie*** bovendien beter beoordelen ***en de lidstaten bijstaan bij het formuleren van hun reactie op incidenten rond informatiebeveiliging***. ***Een betere kennis van de huidige en toekomstige risico's zal een betere besluitvorming mogelijk maken over het ontmoedigen en bestrijden van aanvallen op informatiesystemen of het beperken van de daardoor veroorzaakte schade.***

Amendement 14

Voorstel voor een richtlijn
Overweging 12 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(12 bis) onderhavige richtlijn moet voldoen aan strikte eisen voor wat betreft juridische zekerheid en voorspelbaarheid in het strafrecht, maar er bestaat eveneens behoefte aan een soepel mechanisme om aanpassing aan toekomstige ontwikkelingen mogelijk te maken die verbreding van het toepassingsgebied van deze richtlijn tot gevolg kunnen hebben; hierop wordt ingespeeld door de bepalingen in deze richtlijn over het verzamelen van gegevens, uitwisseling van informatie en de verplichting voor de Commissie regelmatig verslag te doen

over de toepassing ervan en alle noodzakelijke voorstellen in te dienen.Tot dergelijke toekomstige ontwikkelingen behoren technische ontwikkelingen die bij voorbeeld doelmatiger handhaving mogelijk maken op het gebied van aanvallen op informatiesystemen of die het voorkomen of opvangen van dit soort aanvallen vergemakkelijken.

Motivering

De invoering van sancties wordt op prijs gesteld, maar een omvattende benadering van de Unie voor het aanpakken van cybermisdaad moet zich niet alleen richten op doelmatige handhaving van de wet, maar eveneens strategieën en instrumenten ontwikkelen om deze misdadige activiteiten te voorkomen.

Amendement 15

Voorstel voor een richtlijn
Overweging 12 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(12 ter) Het Europees Agentschap voor netwerk- en informatiebeveiliging moet een strategische rol spelen in de coördinatie van de maatregelen van lidstaten en instellingen van de Unie. Aan het Agentschap kan bij voorbeeld te taak worden opgedragen toezicht te houden op de onderlinge uitwisseling van informatie, waarbij het als centraal aanspreekpunt fungeert en de cyberveiligheidsincidenten in de Unie registreert. Tevens kan het de opdracht krijgen de statistische gegevens waarnaar in onderhavige richtlijn wordt verwezen op Unieniveau te centraliseren en te gebruiken als grondslag voor de opstelling van verslagen over de toestand van informatiesystemen en computerveiligheid in de gehele Unie.

Amendement 16

Voorstel voor een richtlijn
Overweging 13

Door de Commissie voorgestelde tekst	*Amendement*
(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.	(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 op EU-niveau van het nationale strafrecht op dit gebied. ***Evenzo moet de Unie streven naar meer internationale samenwerking op het gebied van netwerk- en informatieveiligheid met alle internationale betrokken partijen.*** 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.

Amendement 17

Voorstel voor een richtlijn
Artikel 1 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
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	Deze richtlijn definieert strafbare feiten op het gebied van aanvallen op informatiesystemen en stelt geharmoniseerde minimumregels inzake sancties voor dergelijke strafbare feiten vast. Ook beoogt zij gemeenschappelijke bepalingen in te voeren, ***enerzijds*** om dergelijke aanvallen te voorkomen ***en***

samenwerking op dit gebied te verbeteren.	***bestrijden*** en ***anderzijds om*** de Europese samenwerking ***op dit gebied*** te verbeteren, ***met name op strafrechtelijk vlak***.

Amendement 18

Voorstel voor een richtlijn
Artikel 2 – letter d

Door de Commissie voorgestelde tekst	*Amendement*
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.	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 ***of Unie***wetgeving.

Amendement 19

Voorstel voor een richtlijn
Artikel 7 – letter b

Door de Commissie voorgestelde tekst	*Amendement*
b) een computerwachtwoord, toegangscode of soortgelijke gegevens die toegang bieden tot een informatiesysteem of een deel daarvan.	b) een computerwachtwoord, toegangscode, ***digitaal of fysiek veiligheidstoken*** of soortgelijke gegevens die toegang bieden tot een informatiesysteem of een deel daarvan.

Amendement 20

Voorstel voor een richtlijn
Artikel 8 – paragraaf 1 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	1 bis. De lidstaten zorgen ervoor dat de niet-toegestane doorgifte aan derden van enigerlei identificatiegegevens met het oog op het verrichten van de in de artikelen 3 tot en met 7 bedoelde handelingen strafbaar wordt gesteld.

Amendement 21

Voorstel voor een richtlijn
Artikel 8 – paragraaf 1 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	1 ter. De lidstaten zorgen ervoor dat het als verzwarende omstandigheid bij de strafbaarstelling wordt aangemerkt, als de strafbare feiten in de zin van de artikelen 3 tot en met 7 worden begaan door een persoon die uit hoofde van zijn functie toegang heeft tot de beveiligingsmechanismen van informatiesystemen.

Amendement 22

Voorstel voor een richtlijn
Artikel 10 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
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.	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 ***of gevoelige informatie***.

Amendement 23

Voorstel voor een richtlijn
Artikel 13 – lid 1 – letter c

Door de Commissie voorgestelde tekst	*Amendement*
c) zijn gepleegd ten voordele van een rechtspersoon die ***zijn hoofdkantoor*** op het	c) zijn gepleegd ten voordele van een rechtspersoon die ***deel is van een***

grondgebied van ***de betrokken*** lidstaat ***heeft***.

vennootschap op het grondgebied van die lidstaat.

Amendement 24

Voorstel voor een richtlijn
Artikel 14 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
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***.	1. Voor informatie-uitwisseling over strafbare feiten in de zin van de artikelen 3 tot en met 8 ***voorzien*** de lidstaten, met inachtneming van de regels inzake gegevensbescherming, ***in een functioneel nationaal meldpunt*** en maken ze gebruik van het netwerk van operationele meldpunten die vierentwintig uur per dag en zeven dagen per week bereikbaar zijn ***en doen zij deze gegevens eveneens toekomen aan de Commissie en het Europees Agentschap voor netwerk- en informatieveiligheid***. De lidstaten zorgen er tevens voor dat zij over procedures beschikken waarmee zij binnen maximaal acht uur kunnen reageren op dringende verzoeken. Een dergelijke reactie ***moet doeltreffend zijn en dient, al naar gelang het geval, onder meer te bestaan uit het faciliteren of rechtstreeks uitvoeren van onderstaande maatregelen: het verlenen van technisch advies o.m. met betrekking tot het herstel van de werking van het informatiesysteem, het bewaren van gegevens overeenkomstig de beginselen inzake de bescherming van persoonlijke gegevens, het verzamelen van bewijs, het verstrekken van juridische informatie, en het lokaliseren en identificeren van verdachten. De meldpunten*** geven aan hoe ***en binnen welke tijd ze op het verzoek om bijstand zullen reageren.***

Amendement 25

Voorstel voor een richtlijn
Artikel 14 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
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.	2. De lidstaten stellen de Commissie, ***Eurojust en het Europees Agentschap voor netwerk- en informatiebeveiliging*** 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.

Amendement 26

Voorstel voor een richtlijn
Artikel 15 – lid 3

Door de Commissie voorgestelde tekst	*Amendement*
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.	3. De lidstaten verstrekken de overeenkomstig dit artikel verzamelde gegevens aan de Commissie, ***Europol en het Europees Agentschap voor netwerk- en informatiebeveiliging en*** zorgen ervoor dat er een ***periodiek*** geconsolideerd overzicht van hun statistische verslagen wordt gepubliceerd.

Amendement 27

Voorstel voor een richtlijn
Artikel 18 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
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.	1. Uiterlijk op [VIER JAAR VANAF DE GOEDKEURING] en vervolgens om de drie jaar dient de Commissie ***na raadpleging van alle desbetreffende belanghebbenden*** bij het Europees Parlement en de Raad een verslag in over de tenuitvoerlegging van deze richtlijn, met de eventueel noodzakelijke voorstellen. ***In***

	ieder verslag worden technische oplossingen vastgesteld en verwerkt met betrekking tot noodzakelijke voorstellen, die in de Unie een doelmatiger handhaving mogelijk maken op het gebied van aanvallen op informatiesystemen, o.m. technische oplossingen die ertoe kunnen dienen dergelijke aanvallen te voorkomen of op te vangen.

Amendement 28

Voorstel voor een richtlijn
Artikel 18 – lid 2

Door de Commissie voorgestelde tekst	*Amendement*
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.	2. De lidstaten ***en het Europees Agentschap voor netwerk- en informatieveiligheid*** 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.

PROCEDURE

Titel	Aanvallen op informatiesystemen en intrekking van Kaderbesluit 2005/222/JBZ van de Raad
Document- en procedurenummers	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Commissie ten principale Datum bekendmaking	LIBE 7.10.2010
Medeadviserende commissie(s) Datum bekendmaking	ITRE 7.10.2010
Rapporteur(s) Datum benoeming	Christian Ehler 24.11.2010
Behandeling in de commissie	13.4.2011 6.10.2011
Datum goedkeuring	10.11.2011
Uitslag eindstemming	+: 49 –: 0 0: 1

Bij de eindstemming aanwezige leden	Ivo Belet, Bendt Bendtsen, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Ioan Enciu, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Jacky Hénin, Kent Johansson, Romana Jordan Cizelj, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Bogdan Kazimierz Marcinkiewicz, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Anni Podimata, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Jens Rohde, Paul Rübig, Amalia Sartori, Francisco Sosa Wagner, Konrad Szymański, Michael Theurer, Ioannis A. Tsoukalas, Claude Turmes, Niki Tzavela, Marita Ulvskog, Vladimir Urutchev, Adina-Ioana Vălean
Bij de eindstemming aanwezige vaste plaatsvervanger(s)	Antonio Cancian, Jolanta Emilia Hibner, Yannick Jadot, Ivailo Kalfin, Bernd Lange, Werner Langen, Markus Pieper, Mario Pirillo, Hannes Swoboda, Silvia-Adriana Ţicău
Bij de eindstemming aanwezige plaatsvervanger(s) (art. 187, lid 2)	Eider Gardiazábal Rubial

PROCEDURE

Titel	Aanvallen op informatiesystemen en intrekking van Kaderbesluit 2005/222/JBZ van de Raad			
Document- en procedurenummers	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)			
Datum indiening bij EP	30.9.2010			
Commissie ten principale Datum bekendmaking	LIBE 7.10.2010			
Medeadviserende commissie(s) Datum bekendmaking	AFET 7.4.2011	BUDG 7.10.2010	ITRE 7.10.2010	
Geen advies Datum besluit	BUDG 20.10.2010			
Rapporteur(s) Datum benoeming	Monika Hohlmeier 9.12.2010			
Behandeling in de commissie	3.2.2011	25.5.2011	12.1.2012	28.2.2012
	27.3.2012	21.6.2012	6.6.2013	
Datum goedkeuring	6.6.2013			
Uitslag eindstemming	+: –: 0:	36 8 0		
Bij de eindstemming aanwezige leden	Jan Philipp Albrecht, Emine Bozkurt, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Ioan Enciu, Frank Engel, Cornelia Ernst, Kinga Gál, Kinga Göncz, Sylvie Guillaume, Sophia in 't Veld, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Nuno Melo, Roberta Metsola, Antigoni Papadopoulou, Georgios Papanikolaou, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Rui Tavares, Nils Torvalds, Wim van de Camp, Axel Voss, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
Bij de eindstemming aanwezige vaste plaatsvervanger(s)	Dimitrios Droutsas, Mariya Gabriel, Evelyne Gebhardt, Stanimir Ilchev, Franziska Keller, Jean Lambert, Jan Mulder			
Bij de eindstemming aanwezige plaatsvervanger(s) (art. 187, lid 2)	Jens Nilsson, Sabine Verheyen			
Datum indiening	19.6.2013			