EUROPEES PARLEMENT 2009 - 2014

Commissie burgerlijke vrijheden, justitie en binnenlandse zaken

2010/0273(COD)

24.11.2011

***I
ONTWERPVERSLAG

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

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 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 (A7-0000/2011),

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 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	(1) Deze richtlijn heeft ten doel de strafrechtelijke bepalingen van de lidstaten inzake aanvallen op informatiesystemen

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

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.	onderling af te stemmen en de samenwerking tussen justitiële en andere bevoegde autoriteiten, zoals de politie en andere gespecialiseerde rechtshandhavingsinstanties van de lidstaten***, en gespecialiseerde agentschappen van de Unie***, te verbeteren.
	Or. en

Motivering

Gelet op het transnationale karakter van aanvallen op informatiesystemen, is het van wezenlijk belang de samenwerking tussen justitiële en politiële autoriteiten van zowel de lidstaten als de Europese Unie te verbeteren.

Amendement 2

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, 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. ***Aanvallen op vitale infrastructuren kunnen aanzienlijke grensoverschrijdende gevolgen hebben en diensten verstoren of vernietigen die absoluut noodzakelijk zijn voor de beveiliging, de veiligheid, de gezondheid, de mobiliteit, het sociale en economische welzijn van burgers van de Unie en het goed functioneren van overheidsinstellingen, zoals energiecentrales, vervoernetwerken en overheidsnetwerken.*** 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.

Or. en

Motivering

Het is nodig te wijzen op de mogelijke gevolgen en de omvang van cyberaanvallen, in het bijzonder wanneer ze worden gepleegd tegen vitale infrastructuren.

Amendement 3

Voorstel voor een richtlijn
Overweging 7 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(7 bis) Hoewel het verhullen van de ware identiteit van de dader en de schade die hierdoor wordt berokkend aan de rechtmatige bezitter van de identiteit belangrijke elementen zijn voor de vaststelling van straffen binnen het toepassingsgebied van deze richtlijn, dient de Unie een horizontaal instrument te ontwikkelen dat deze en soortgelijke strafbare feiten op een meer omvattende manier dekt, en in het kader waarvan onder meer identiteitsdiefstal, de link met de wetgeving inzake namen van personen en consumentenbescherming worden aangepakt.

Or. en

Motivering

Het verhullen van de ware identiteit van de dader en de schade die wordt berokkend aan de rechtmatige bezitter van de identiteit zijn niet enkel belangrijk voor het bestraffen van de strafbare feiten die binnen het toepassingsgebied van deze richtlijn vallen. Op lange termijn moeten deze en andere strafbare feiten eerder worden aangepakt door middel van een horizontaal instrument dat verder gaat dan aanvallen tegen informatiesystemen.

Amendement 4

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. Dat Verdrag is het wettelijke referentiekader voor de bestrijding van cybercriminaliteit, waaronder aanvallen op informatiesystemen. Deze richtlijn bouwt voort op dat Verdrag. ***Daarom is het essentieel dat de lidstaten die het Verdrag inzake cybercriminaliteit van de Raad van Europa nog niet hebben geratificeerd dit zo spoedig mogelijk doen.***

Or. en

Motivering

Aangezien het Verdrag inzake cybercriminaliteit het centrale internationale juridisch instrument is voor de bestrijding van cybercriminaliteit, dienen de lidstaten die dit verdrag nog niet hebben geratificeerd te worden aangemoedigd om dit te doen, zowel met het oog op coherentie als om een politiek signaal te geven.

Amendement 5

Voorstel voor een richtlijn
Overweging 9

Door de Commissie voorgestelde tekst	*Amendement*
(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	(9) Gelet op de verschillende manieren waarop aanvallen kunnen worden uitgevoerd, en gelet op de snelle ontwikkelingen op het gebied van hardware en software, wordt er in deze richtlijn verwezen naar "instrumenten" die kunnen worden gebruikt voor het plegen

van de in deze richtlijn opgesomde strafbare feiten. Onder instrumenten wordt bijvoorbeeld kwaadaardige software verstaan, zoals botnets, waarmee cyberaanvallen worden gepleegd.	van de in deze richtlijn opgesomde strafbare feiten. Onder instrumenten wordt bijvoorbeeld kwaadaardige software verstaan, zoals botnets, waarmee cyberaanvallen worden gepleegd. ***Deze instrumenten vertegenwoordigen slechts een klein deel van de vele mogelijkheden om informatiesystemen aan te vallen. Tegen deze achtergrond dienen de werkzaamheden aan een strategie van de Unie inzake IT-architectuur, en met name "cloud computing", met inbegrip van een technische normalisatie en een gemeenschappelijk rechtskader, te worden voortgezet en geïntensiveerd.***

Or. en

Motivering

In het licht van de huidige ontwikkelingen op technisch vlak is een verwijzing naar "cloud computing" noodzakelijk. Er is nood aan verdere technische normalisatie en een gemeenschappelijk Europees rechtskader voor "cloud computing". Dit zou eveneens de rol van de EU als leverancier en gebruiker van geavanceerde en veilige IT-structuren versterken.

Amendement 6

Voorstel voor een richtlijn
Overweging 9 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(9 bis) Het doelbewuste onrechtmatige gebruik van een computerprogramma dat is ontworpen om bewijs te verwijderen van de strafbare feiten waarnaar wordt verwezen in deze richtlijn moet ofwel worden beschouwd als een vorm van medeplichtigheid ofwel als een afzonderlijk strafbaar feit.

Or. en

Motivering

Hoewel een computerprogramma dat is ontworpen om bewijs te verwijderen geen instrument is in de zin van artikel 7 van deze richtlijn, ondersteunt het gebruik ervan niettemin cyberaanvallen. De lidstaten moeten er daarom voor zorgen dat het gebruik van dergelijk programma ofwel wordt beschouwd als medeplichtigheid ofwel als afzonderlijk strafbaar feit (zoals de belemmering van strafonderzoeken).

Amendement 7

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 beoogt niet de strafbaarstelling van feiten die gepleegd worden zonder criminele opzet, zoals het ***legaal*** testen of beveiligen van informatiesystemen***, of van situaties waarbij het niet verlenen van toestemming om toegang te krijgen tot een systeem op zich een misbruik van recht is***.

Or. en

Motivering

De bewoording in de Engelse tekst ("authorised testing") kan geïnterpreteerd worden op een manier dat een formele toestemming nodig zou zijn om de beveiliging van eigen informatiesystemen te testen. Dit zou de doeltreffendheid en uitvoerbaarheid van zelftesten zonder criminele opzet volledig ondermijnen. Bovendien mag er geen sprake zijn van strafrechtelijke aansprakelijkheid wanneer de beperking van de toegang tot een systeem op zich illegaal is.

Amendement 8

Voorstel voor een richtlijn
Overweging 12 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(12 bis) In het kader van de vaststelling van beleid van de Unie voor de bestrijding van cybercriminaliteit, werd er in de conclusies van de Raad van 24 oktober

2008, 27-28 november 2008 en 26 april 2010 een specifieke rol toegekend aan Europol om bij te dragen tot de verwezenlijking van deze doelstelling. Daarom moet Europol een Europees platform oprichten en huisvesten als verzamelpunt voor de nationale platformen, dat onder meer ten doel heeft informatie over inbreuken op het internet te verzamelen en te centraliseren. Dit moet informatie omvatten over daders en hun modus operandi. In overeenstemming met het Besluit van de Raad van 6 april 2009 tot oprichting van de Europese politiedienst (Europol)[1], en in het bijzonder de in hoofdstuk V opgenomen regels inzake de bescherming van persoonsgegevens, en overeenkomstig Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken[2], wordt in deze richtlijn rekening gehouden met de aan Europol toevertrouwde taken.

_____

[1] PB L 121 van 15.5.2009, blz. 37.

[2] PB L 350 van 30.12.2008, blz. 60.

Or. en

Motivering

Gelet op het grensoverschrijdende karakter van aanvallen tegen informatiesystemen en de coördinerende rol van Europol, is het nodig de rol van dit agentschap op het vlak van cyberaanvallen te omlijnen. De Europese Raad heeft hiervoor reeds waardevolle richtsnoeren opgesteld, waarmee in deze richtlijn rekening moet worden gehouden.

Amendement 9

Voorstel voor een richtlijn
Overweging 12 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(12 ter) Om cybercriminaliteit op een effectieve manier te kunnen bestrijden, is het eveneens nodig de veerkracht van informatiesystemen te verhogen door ze doeltreffender te beschermen tegen aanvallen. In dit opzicht moet de vaststelling van minimumnormen voor de adequate bescherming van informatiesystemen een centrale rol spelen. Bijgevolg zal de bestrijding van cybercriminaliteit door de Unie en de lidstaten enkel effect hebben indien deze richtlijn vergezeld gaat van preventieve maatregelen tegen dergelijke strafbare feiten, aangenomen in overeenstemming met artikel 67, lid 3, en artikel 84 van het Verdrag betreffende de werking van de Europese Unie.

Or. en

Motivering

Hoewel strafrecht een belangrijk element is voor de bestrijding van cybercriminaliteit, blijft het de allerlaatste stap nadat een aanval heeft plaatsgevonden. Daarom moet de EU meer inspanningen leveren om haar systemen in de eerste plaats beter te beschermen, bijvoorbeeld door middel van minimumnormen voor de adequate bescherming van informatiesystemen.

Amendement 10

Voorstel voor een richtlijn
Overweging 12 quater (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(12 quater) De lidstaten dienen de bescherming van hun informatiesystemen en daarmee samenhangende gegevens te beschouwen als onderdeel van hun zorgplicht. Er dient te worden gezorgd

voor redelijke beschermingsniveaus tegen op een redelijke manier te identificeren dreigingen. De kosten en lasten van dergelijke bescherming dienen evenredig te zijn met de waarschijnlijke schade aan de betrokkenen.

Or. en

Motivering

De lidstaten werken zelf met belangrijke en gevoelige gegevens, zoals informatie betreffende belastingen en ziekteverzekering. Het is bijgevolg hun plicht om deze gegevens adequaat te beschermen tegen aanvallen.

Amendement 11

Voorstel voor een richtlijn
Overweging 12 quinquies (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(12 quinquies) De lidstaten dienen eveneens de nodige maatregelen te nemen om rechtspersonen binnen hun rechtsgebied te verplichten persoonsgegevens waar zij verantwoordelijk voor zijn te beschermen tegen de in deze richtlijn bedoelde strafbare feiten. Rechtspersonen dienen te zorgen voor redelijke beschermingsniveaus tegen op een redelijke manier te identificeren dreigingen. De kosten en lasten van dergelijke bescherming dienen evenredig te zijn met de waarschijnlijke schade aan de betrokkenen. Wanneer een rechtspersoon duidelijk nagelaten heeft te zorgen voor een redelijk beschermingsniveau, en wanneer de als gevolg van dergelijke nalatigheid berokkende schade aanzienlijk is, dienen de lidstaten ervoor te zorgen dat het mogelijk is deze rechtspersoon te vervolgen.

Or. en

Motivering

Wanneer ze met persoonsgegevens omgaan, dragen rechtspersonen de verantwoordelijkheid deze gegevens voldoende te beschermen in het licht van redelijk te identificeren dreigingen. Indien ze niet zorgen voor dit beschermingsniveau, dienen de lidstaten ervoor te zorgen dat het mogelijk is deze rechtspersoon te vervolgen.

Amendement 12

Voorstel voor een richtlijn
Overweging 12 sexies (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(12 sexies) Het is eveneens nodig de samenwerking tussen dienstverleners, producenten, rechtshandhavingsinstanties en justitiële autoriteiten te stimuleren en te verbeteren, en hierbij volledig de rechtsstaat te eerbiedigen, met name met betrekking tot rechtszekerheid en voorspelbaarheid, alsook de rechten van verdachten en beklaagden, zoals het vermoeden van onschuld en de mogelijkheid beroep aan te tekenen. Dit omvat bijvoorbeeld steun door dienstverleners om illegale systemen of functies buiten werking te stellen.

Or. en

Motivering

De samenwerking tussen dienstverleners in de particuliere sector en de openbare sector is cruciaal om cyberaanvallen effectief te kunnen bestrijden.

Amendement 13

Voorstel voor een richtlijn
Overweging 12 septies (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(12 septies) Onverminderd de vrijwillige samenwerking tussen rechtspersonen zoals dienstverleners en producenten enerzijds en rechtshandhavingsinstanties en justitiële autoriteiten anderzijds, dienen de lidstaten te bepalen in welke gevallen nalatigheid op zich een criminele gedraging kan vormen.

Or. en

Motivering

Het niet samenwerken of de belemmering van strafonderzoeken door rechtspersonen is uitermate gewichtig en dient bijvoorbeeld te worden beschouwd als medeplichtigheid aan de strafbare feiten die zijn opgenomen in deze richtlijn.

Amendement 14

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	(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.	de vervolging van aanvallen op informatiesystemen te worden vergemakkelijkt door de ***adequate uitvoering en toepassing*** van Kaderbesluit 2009/948/JBZ van de Raad over het voorkomen en beslechten van geschillen over de uitoefening van rechtsmacht bij strafprocedures.

Or. en

Motivering

Taalkundige correctie.

Amendement 15

Voorstel voor een richtlijn
Overweging 13 bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(13 bis) Een verbeterde samenwerking tussen rechtshandhavingsinstanties en justitiële autoriteiten in de hele Unie is van wezenlijk belang voor de effectieve bestrijding van cybercriminaliteit. In deze context moeten de Commissie en de lidstaten meer inspanningen leveren op het vlak van passende opleidingen voor rechtshandhavingsinstanties en justitiële autoriteiten om te zorgen voor meer inzicht in cybercriminaliteit en de impact ervan, en samenwerking en de uitwisseling van beste praktijken bevorderen, bijvoorbeeld in het kader van het Europees justitieel netwerk, met medewerking van Europol, Eurojust en het Europees Agentschap voor netwerk- en informatiebeveiliging.

Or. en

Motivering

Passende opleiding van de actoren die betrokken zijn bij de vervolging van cybercriminelen is van cruciaal belang in de strijd tegen cybercriminaliteit. Bovendien bestaan er op EU-niveau reeds instrumenten om deze samenwerking en opleiding te verbeteren. Dit wordt nog belangrijker gemaakt door het feit dat de politie en de gerechtelijke instanties geconfronteerd worden met rechtsstelsels in het kader waarvan strafbare feiten anders worden omschreven en gedefinieerd. Wederzijds begrip is dan ook cruciaal.

Amendement 16

Voorstel voor een richtlijn
Overweging 13 ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	(13 ter) Dergelijke opleidingen en uitwisselingen van informatie moeten zorgen voor meer kennis van de verschillen in nationale rechtsstelsels en van de problemen bij strafrechtelijke vervolging door verschillende nationale bepalingen betreffende de ernst van de feiten, zoals de omvang van de schade, en de verdeling van bevoegdheden tussen de nationale rechtshandhavingsinstanties.

Or. en

Motivering

Bij de vervolging van cyberaanvallen worden de politie en de gerechtelijke instanties geconfronteerd met rechtsstelsels in het kader waarvan strafbare feiten anders worden omschreven en gedefinieerd. Wederzijds begrip is dan ook cruciaal.

Amendement 17

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	d) "onrechtmatig": toegang***, gebruik*** of verstoring, niet toegestaan door de eigenaar of een andere houder van rechten op het systeem of op een deel daarvan, ***voor zover***

krachtens de nationale wetgeving**.**	***het niet verlenen van dergelijke toestemming op zich geen misbruik van recht is,*** of niet toegestaan krachtens de nationale wetgeving***;***

Or. en

Motivering

De vrije uitwisseling van informatie mag niet worden beperkt op een manier dat het niet verlenen van toestemming zorgt voor een schending van andere rechten, zoals het recht op de vrijheid van informatie. Het niet verlenen van toestemming kan bijgevolg zelf een misbruik van recht zijn.

Amendement 18

Voorstel voor een richtlijn
Artikel 2 – letter d bis (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	d bis) "onbeduidend geval": een geval kan als onbeduidend worden beschouwd wanneer de schade en/of het gevaar dat het oplevert voor openbare of particuliere belangen, zoals de integriteit van een informatiesysteem of van computergegevens, of de integriteit, de rechten en andere belangen van een persoon, onbeduidend 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;

Or. en

Motivering

"Onbeduidende gevallen" vormen een wezenlijk onderdeel van deze richtlijn voor het omschrijven van een strafbaar feit. Met het oog op rechtszekerheid dient deze term gedefinieerd te worden.

Amendement 19

Voorstel voor een richtlijn
Artikel 2 – letter d ter (nieuw)

Door de Commissie voorgestelde tekst	*Amendement*
	d ter) "informatiesysteem dat deel uitmaakt van de vitale infrastructuur": een informatiesysteem dat deel uitmaakt van infrastructuur die van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, waarvan de verstoring of vernietiging in een lidstaat aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken.

Or. en

Motivering

Met het oog op rechtszekerheid dient te term "informatiesysteem dat deel uitmaakt van de vitale infrastructuur" te worden verduidelijkt. Het groenboek COM(2005)576 van de Commissie en de mededelingen COM(2011)163 en COM(2009)149 over de bescherming van kritieke infrastructuur zijn waardevolle bronnen hiervoor.

Amendement 20

Voorstel voor een richtlijn
Artikel 3

Door de Commissie voorgestelde tekst	*Amendement*
Iedere lidstaat treft de nodige maatregelen om opzettelijke, onrechtmatige toegang tot een informatiesysteem of enig onderdeel daarvan strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.	Iedere lidstaat treft de nodige maatregelen om opzettelijke, onrechtmatige toegang – ***dit wil zeggen het zich verschaffen van toegang*** tot een informatiesysteem of enig onderdeel daarvan – strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn. ***Iedere lidstaat kan beslissen dat de in lid 1 bedoelde gedragingen alleen strafbaar worden gesteld indien het feit wordt gepleegd door een inbreuk op de***

beveiligingsmaatregelen.

Or. en

Motivering

Met het oog op rechtszekerheid dient "toegang" te worden gedefinieerd. Bovendien dient onrechtmatige toegang een inbreuk op de beveiligingsmaatregelen te impliceren. Anders kan bijvoorbeeld niet-toegestane toegang tot een open draadloos netwerk als een strafbaar feit worden beschouwd.

Amendement 21

Voorstel voor een richtlijn
Artikel 6

Door de Commissie voorgestelde tekst	*Amendement*
De lidstaten treffen de nodige maatregelen om het opzettelijk met technische middelen onderscheppen van niet-openbare transmissies van computergegevens naar, vanuit of binnen een computersysteem, met inbegrip van elektromagnetische emissies uit een computersysteem dat zulke computergegevens draagt, indien onrechtmatig begaan, strafbaar te stellen.	De lidstaten treffen de nodige maatregelen om het opzettelijk met technische middelen onderscheppen van niet-openbare transmissies van computergegevens naar, vanuit of binnen een computersysteem, met inbegrip van elektromagnetische emissies uit een computersysteem dat zulke computergegevens draagt, indien onrechtmatig begaan, ***en in elk geval voor de gevallen die niet onbeduidend zijn,*** strafbaar te stellen. ***Het met technische middelen onderscheppen omvat 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 het informatiesysteem, ofwel indirect, door middel van het gebruik van elektronische afluister of aftapapparatuur, bekomen van de inhoud van gegevens. Onderschepping kan eveneens gepaard gaan met registreren.*** ***Technische middelen omvatten technische voorzieningen bevestigd op transmissielijnen, alsook apparaten om draadloze communicaties te verzamelen***

en te registreren, met inbegrip van het gebruik van software, wachtwoorden en codes.

Or. en

Motivering

In overeenstemming met artikelen 3 en 5 mag ook dit artikel onbeduidende gevallen niet als strafbaar feit aanmerken. Bovendien is een definitie van "onderschepping" nodig. Alinea 53 van de toelichting bij het Verdrag inzake cybercriminaliteit is nuttig hiervoor. Met het oog op rechtszekerheid dient de term "technische middelen " te worden verduidelijkt. In het tweede deel van alinea 53 van de toelichting bij het Verdrag inzake cybercriminaliteit wordt een nuttige definitie aangeleverd.

Amendement 22

Voorstel voor een richtlijn
Artikel 7

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

Or. en

Motivering

Aangezien het mogelijk is programma's op verschillende manieren te gebruiken, namelijk zowel voor wettelijk toegelaten als voor criminele doeleinden, moet het bezit van een instrument op zich niet strafbaar zijn. Bovendien dienen de in dit artikel beschreven handelingen enkel strafbaar te zijn indien ze duidelijk met het oog op het plegen van een strafbaar feit worden uitgevoerd.

Amendement 23

Voorstel voor een richtlijn
Artikel 7 – letter a

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

Or. en

Motivering

De term "instrument" zorgt voor rechtsonzekerheid, aangezien hij eenvoudige hardware, zoals een computer of een camera, zou kunnen omvatten. Deze term dient derhalve te worden geschrapt. Bovendien is de term "hoofdzakelijk" niet voldoende helder. "Duidelijk" is specifieker.

Amendement 24

Voorstel voor een richtlijn
Artikel 8 – titel

Door de Commissie voorgestelde tekst	*Amendement*
Uitlokking, deelneming, medeplichtigheid en poging	*(Niet van toepassing op de Nederlandse versie.)*

Or. en

Motivering

Taalkundige correctie in de Engelse versie.

Amendement 25

Voorstel voor een richtlijn
Artikel 8 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
1. De lidstaten zorgen ervoor dat uitlokking van, alsmede deelneming en medeplichtigheid aan een van de in de artikelen 3 tot en met 7 genoemde feiten strafbaar wordt gesteld.	*(Niet van toepassing op de Nederlandse versie.)*

Or. en

Motivering

Taalkundige correcties in de Engelse versie.

Amendement 26

Voorstel voor een richtlijn
Artikel 9 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de artikelen 3 tot en met 8 bedoelde feiten strafbaar worden gesteld met doeltreffende, evenredige en afschrikkende strafrechtelijke sancties.	*(Niet van toepassing op de Nederlandse versie.)*

Or. en

Motivering

Taalkundige correctie in de Engelse versie.

Amendement 27

Voorstel voor een richtlijn
Artikel 10 – lid 1

Door de Commissie voorgestelde tekst	*Amendement*
1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de ***artikelen 3 tot en met 7*** bedoelde feiten strafbaar worden gesteld met een maximale gevangenisstraf van ten minste vijf jaar wanneer deze worden gepleegd in het kader van een criminele organisatie zoals gedefinieerd in Kaderbesluit 2008/841/JBZ.	1. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de ***artikelen 4 tot en met 7*** bedoelde feiten strafbaar worden gesteld met een maximale gevangenisstraf van ten minste vijf jaar wanneer deze worden gepleegd in het kader van een criminele organisatie zoals gedefinieerd in Kaderbesluit 2008/841/JBZ. ***In deze gevallen zijn de in dit kaderbesluit vastgestelde straffen niet van toepassing.***

Or. en

Motivering

Artikel 3 van Kaderbesluit 2008/841/JBZ voorziet in gevangenisstraffen van twee tot vijf jaar voor strafbare feiten die worden gepleegd in het kader van een criminele organisatie; terwijl artikel 10 van dit voorstel voorziet in een maximumgevangenisstraf van ten minste vijf jaar. Met het oog op rechtszekerheid moet daarom worden verduidelijkt welke strafmaat moet gelden voor cybercriminaliteit binnen het kader van een criminele organisatie.

Amendement 28

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	2. De lidstaten nemen de nodige maatregelen om ervoor te zorgen dat de in de ***artikelen 4 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 ***ernstige*** schade veroorzaken, zoals ontregelde systeemdiensten, financiële

kosten of verlies van persoonsgegevens.	kosten of verlies van persoonsgegevens***, of wanneer ze worden gepleegd tegen een informatiesysteem dat deel uitmaakt van de vitale infrastructuur***.

Or. en

Motivering

Artikelen 4 tot en met 6 behandelen bijzonder ernstige strafbare feiten die op grote schaal worden gepleegd en ernstige schade veroorzaken, of die worden gepleegd tegen informatiesystemen die deel uitmaken van de vitale infrastructuur.

Amendement 29

Voorstel voor een richtlijn
Artikel 14 – titel

Door de Commissie voorgestelde tekst	*Amendement*
Informatie-uitwisseling	Informatie-uitwisseling ***en samenwerking***

Or. en

Motivering

In overeenstemming met de volgende amendementen dient het toepassingsgebied van dit artikel eveneens samenwerking te omvatten. Bijgevolg moet de titel van dit artikel worden aangepast.

Amendement 30

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.	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.	De lidstaten zorgen er tevens voor dat zij over procedures beschikken waarmee zij binnen maximaal acht uur kunnen reageren op dringende verzoeken***, door te vermelden*** of en hoe het verzoek om bijstand ***zal worden*** ingewilligd en wanneer. ***Dergelijke informatie-uitwisseling doet geen afbreuk aan de nationale regelgeving van de lidstaten betreffende het verzamelen of de ontvankelijkheid van bewijsmateriaal met betrekking tot het gebruik van dergelijke informatie in verdere strafprocedures.***

Or. en

Motivering

Hoewel de snelle uitwisseling van informatie en wederzijdse bijstand van essentieel belang zijn bij de gezamenlijke bestrijding van grensoverschrijdende cyberaanvallen, doen deze regels geen afbreuk aan de ontvankelijkheid van bewijsmateriaal in mogelijke verdere strafprocedures.

Amendement 31

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

Door de Commissie voorgestelde tekst	*Amendement*
	2 bis. Voor informatie-uitwisseling over strafbare feiten in de zin van de artikelen 3 tot en met 8 zorgen de lidstaten, met inachtneming van de regels inzake gegevensbescherming, voor de totstandbrenging van netwerken voor samenwerking en partnerschappen met dienstverleners en producenten.

Or. en

Motivering

Naast de samenwerking tussen de autoriteiten, is het van cruciaal belang de samenwerking tussen de particuliere sector en de overheidsinstanties te verbeteren om cyberaanvallen effectief te kunnen bestrijden en de veerkracht van zowel openbare als particuliere netwerken

te vergroten.

Amendement 32

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 ***en aan het Europees Agentschap voor netwerk- en informatiebeveiliging met het oog op de beoordeling van de netwerk- en informatiebeveiliging in overeenstemming met Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging[1].*** ***De lidstaten verstrekken eveneens de statistische gegevens en andere beschikbare gegevens over de modus operandi van de daders aan Europol met het oog op dreigingsevaluatie en strategische analyses van cybercriminaliteit in overeenstemming met Besluit 2009/371/JBZ van de Raad.*** De ***Commissie en de*** lidstaten zorgen er ***samen*** tevens voor dat een geconsolideerd overzicht van hun statistische verslagen wordt gepubliceerd.

[1] PB L 77 van 13.3.2004, blz. 1.

Or. en

Motivering

Gelet op het grensoverschrijdende karakter van aanvallen tegen informatiesystemen en de mogelijke gevolgen voor de hele Unie, is het nodig te zorgen voor een grotere betrokkenheid van zowel het Europees Agentschap voor netwerk- en informatiebeveiliging als Europol bij de beoordeling van de relevante gegevens. In overeenstemming met de richtsnoeren van de Europese Raad, dient Europol voor de uitvoering van zijn taken met name gegevens te

ontvangen over de modus operandi van daders.

Amendement 33

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 bij het Europees Parlement en de Raad een verslag in over de tenuitvoerlegging van deze richtlijn, met de eventueel noodzakelijke voorstellen. ***Bij de herziening houdt de Commissie eveneens rekening met de technische en juridische ontwikkelingen op het vlak van cybercriminaliteit, met name met betrekking tot het toepassingsgebied van deze richtlijn.***

Or. en

Motivering

Gelet op de snelle ontwikkelingen op het vlak van cybertechnologieën is het nodig regelmatig te herzien of de regelgevende inhoud van deze richtlijn geschikt is om de huidige technische mogelijkheden te dekken en of veranderingen aan het rechtskader, eveneens op het niveau van de EU, een invloed hebben op het toepassingsgebied van deze richtlijn, bijvoorbeeld met betrekking tot toekomstig EU-beleid inzake "cloud computing".