EUROPEES PARLEMENT 2009 - 2014

Commissie industrie, onderzoek en energie

2010/0273(COD)

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

PA_Legam

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 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 ***kunnen uit verschillende hoeken komen, bijvoorbeeld terroristen,*** georganiseerde criminaliteit, ***staten of geïsoleerde 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, zijn van belang om te garanderen dat de richtlijn in de lidstaten coherent wordt toegepast.	(4) Gemeenschappelijke definities op dit gebied, en in het bijzonder van informatiesystemen, computergegevens en ***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	(6) ***In aanvulling op maatregelen van de lidstaten, de Unie en de particuliere sector die gericht zijn op vergroting van de***

afschrikkend te zijn.	***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 identificeren van de ***beschadigde*** en/of buitgemaakte informatie, en het lokaliseren van verdachten.	(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 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 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	(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 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

Europa bovendien beter beoordelen.	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	(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.	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 samenwerking op dit gebied te verbeteren.	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 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 grondgebied van ***de betrokken*** lidstaat ***heeft***.	c) zijn gepleegd ten voordele van een rechtspersoon die ***deel is van een 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