Commissie buitenlandse zaken

2010/0273(COD)

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

PA_Legam

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	(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***

vrijheid, veiligheid en recht in gevaar en maakt derhalve een reactie op het niveau van de Europese Unie noodzakelijk.	***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 voeren.	(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 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 behoefte bestaat aan verdere onderlinge afstemming van het strafrecht op dit gebied. Bovendien dient de coördinatie van de vervolging van aanvallen op	(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 het niveau van de Unie*** van het strafrecht op dit gebied. ***De Unie moet ook streven naar meer internationale***

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.	***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