22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 1082 herdruk *) Brief van de staatssecretaris van Buitenlandse Zaken

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 november 2010

Overeenkomstig de bestaande afspraken heb ik de eer u hierbij drie fiches aan te bieden die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC):

1. Fiche 1: richtlijn aanvallen op informatiesystemen
   Fiche 2: verordening precursoren van explosieven (kamerstuk 22 112, nr. 1083)
   Fiche 3: verordening geïntegreerd maritiem beleid (2011-2013) (kamerstuk 22 112, nr. 1084)

De staatssecretaris van Buitenlandse Zaken,
H.P.M. Knapen

*) het eerder onder kamerstuk 22 112, nr. 1082 gepubliceerde stuk komt hiermee te vervallen.

Fiche : richtlijn aanvallen op informatiesystemen

1. Algemene gegevens

Titel voorstel
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.

Datum Commissiedocument
30 september 2010

Nr. Commissiedocument
COM (2010) 517

Prelex http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:NL:PDF

Nr. impact-assessment Commissie en Opinie Impact-assessment Board
SEC(2010)1122, SEC(2010)1123 (samenvatting), SEC (2010)1124 (IAB opinion)

Behandelingstraject Raad
Raadswerkgroep DROIPEN, CATS, JBZ-Raad

Eerstverantwoordelijk ministerie
Ministerie van Veiligheid en Justitie

Rechtsbasis, stemwijze Raad, rol Europees Parlement en comitologie
a) Rechtsbasis: artikel 83 lid 1 VWEU
b) Stemwijze Raad en rol Europees Parlement : gewone wetgevingsprocedure (gekwalificeerde meerderheidsbesluitvorming in de Raad, medebeslissing Europees Parlement
c) Delegatie en/of comitologie : n.v.t.

2. Samenvatting BNC-fiche

Korte inhoud voorstel
Het voorstel beoogt minimumregels vast te stellen over aanvallen op informatiesystemen. Het betreft omzetting in een richtlijn van het bestaande kaderbesluit van 2005 ter zake. Het voorstel bevat ten opzichte van het kaderbesluit enkele aanvullingen. Het gaat daarbij onder andere om bepalingen over de maximale gevangenisstraffen en strafverzwarende omstandigheden. Ook wordt de justitiële samenwerking verder versterkt door lidstaten ertoe te verplichten snel - via het al bestaande 24/7 netwerk van contactpunten voor cybercriminaliteit – te reageren op urgente informatieverzoeken.

Het oordeel van Nederland is positief ten aanzien van subsidiariteit en proportionaliteit.

Nederland staat positief tegenover het voorstel. De aanpak van cybercriminaliteit op het niveau van de Europese Unie is een uit het Stockholm Programma voortvloeiende prioriteit. Ondersteuning daarvan ligt in het verlengde van de in het regeerakkoord opgenomen ambitie van de regering inzake de totstandkoming van een integrale aanpak op het gebied van cybercrime.

3. Samenvatting voorstel

- *Inhoud voorstel*

  De richtlijn strekt tot verbetering van de justitiële samenwerking tussen de lidstaten door onderlinge aanpassing van het strafrecht inzake aanvallen op informatiesystemen. De richtlijn vervangt het bestaande kaderbesluit van 2005 en komt met een aanvulling hierop. Daarnaast bevat de richtlijn ten opzichte van het kaderbesluit enkele aanvullingen. Voor een deel zijn deze aanvullingen ontleend aan het Cybercrimeverdrag van de Raad van Europa, zoals strafbaarstelling van het met een technisch hulpmiddel aftappen of opnemen van gegevensoverdracht via informatiesystemen, alsmede strafbaarstelling van het voorhanden hebben, verkopen etc. van hulpmiddelen zoals computerprogrammatuur om daarmee vervolgens een of meer van de in de richtlijn bedoelde strafbare feiten te begaan. Voor een ander deel zijn deze aanvullingen (ook ten opzichte van het Cybercrimeverdrag) nieuw. Het voorstel verplicht de lidstaten ertoe om op de feiten, die in de nationale wetgeving strafbaar moeten worden gesteld, doeltreffende, evenredige en afschrikkende sancties te stellen, waaronder gevangenisstraffen met een maximum van ten minste twee jaar. Ook nieuw zijn bepalingen over strafverzwarende omstandigheden, over het uitwisselen van statistische informatie en over het verder versterken van de justitiële samenwerking door lidstaten ertoe te verplichten snel - via het al bestaande 24/7 netwerk van contactpunten voor cybercrime – te reageren op urgente informatieverzoeken.

- *Impact assessment Commissie*

  De Commissie heeft ter onderbouwing van het voorstel een *impact assessment* uitgevoerd. Daarin wordt gewezen op de uitkomsten van een rapport over de implementatie van het kaderbesluit dat op 14 juli 2008 is uitgebracht. Ook wijst de Commissie erop dat dit voorstel volledig aansluit op het Cybercrimeverdrag van de Raad van Europa dat door alle lidstaten is ondertekend en door vijftien van hen is geratificeerd, en dat het voorstel in lijn is met de Europese beleidsnoties betreffende het bestrijden van georganiseerde criminaliteit, het uitvoeren van de digitale agenda en de bescherming van de kritische infrastructuur waar het betreft informatiesystemen en de integriteit van data. Het voorstel wil de justitiële samenwerking tussen de lidstaten door onderlinge aanpassing van het strafrecht inzake aanvallen op informatiesystemen verder versterken. Dat is nodig gelet op de voortschrijdende technische ontwikkeling en gebruik van informatie- en communicatietechnologie. Naast de vele voordelen van ICT voor de samenleving en de economische ontwikkeling staan nadelen van een toenemende vatbaarheid van informatiesystemen voor grootscheepse

aanvallen, zoals door *denial of service* of door virusverspreiding. Steeds vaker worden er zogenoemde botnets (verzameling van computers die tegen de wil en buiten medeweten van eindgebruikers door een derde worden aangestuurd voor het plegen van cybercriminaliteit) gesignaleerd die voor zulke aanvallen worden ingezet en die grote schade kunnen toebrengen aan informatiesystemen en hun werking. Als gevolg van het samenstel van de voorgestelde maatregelen – zoals dat hierboven is omschreven - zullen blijkens het impact assessment de lidstaten beter voorbereid zijn op grootscheepse aanvallen op informatiesystemen, en zullen de veiligheid en de veerkracht van kritische infrastructuur voor informatietechnologie en communicatie toenemen.

4. Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel

a) *Bevoegdheid:* artikel 83, eerste lid, VWEU. Nederland acht dit de juiste rechtsbasis voor dit voorstel.

b) *Functionele toets*

45 Subsidiariteit: positief

45 Proportionaliteit: positief

45 Onderbouwing:

Cybercrime is met name een grensoverschrijdend probleem en kan om deze reden beter – door middel van in een richtlijn op te nemen minimumregels - op het niveau van de Europese Unie worden aangepakt dan door de lidstaten afzonderlijk. Daarom wordt de subsidiariteit van het voorstel positief beoordeeld.

Het voorstel bevat minimumregels die niet verder gaan dan nodig is om de aan het voorstel ten grondslag liggende doelen te bereiken. Het bevat enkele aanvullingen die in lijn zijn met het door Nederland geratificeerde Cybercrimeverdrag en daarop voortbouwen. Door het voorstel wordt een meer uniforme toepassing van dat verdrag binnen de Europese Unie mogelijk. Het voorstel kan bijdragen aan onderlinge samenwerking tussen de lidstaten bij de aanpak van cybercriminaliteit die veelal een grensoverschrijdende dimensie heeft. Derhalve wordt de proportionaliteit van het voorstel positief beoordeeld.

c) *Nederlands oordeel*

Omdat cybercrime een probleem is met een veelal grensoverschrijdende dimensie, is de Nederlandse regering van oordeel dat een verdere versterking van de justitiële samenwerking gewenst is door op het niveau van de Europese Unie minimumregels vast te stellen.

5. Implicaties financieel

a) *Consequenties EU-begroting*

De Commissie schat de financiële implicaties op een bedrag van EUR 5.913.000, dat voor 90 % door de lidstaten zal worden gedragen. Overigens worden deze kosten ook nu al gemaakt onder het huidige kaderbesluit. Er wordt ook gewezen op de mogelijkheid om uit verschillende EUstimuleringsprogramma's – bijvoorbeeld het Safer Internet Programme – om subsidie te vragen. Nederland onderschrijft deze inschatting van de Commissie.

b) *Financiële consequenties (incl. personele) voor rijksoverheid en/ of decentrale overheden*
De inschatting van de kosten van EUR 5.913.000 zullen voor 90 % door de lidstaten worden gedragen, waarbij voor Nederland maximaal 5% van dit bedrag (EUR 295.650) relevant is. . Indien het voorstel budgettaire gevolgen heeft, worden deze ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels van de budgetdiscipline. Op dit moment functioneert er al bij het KLPD een 24/7 contactpunt. Nog niet is te overzien of de extra aanvragen als gevolg van deze richtlijn nopen tot uitbereiding en daarmee tot meerkosten. Nederland is verder van mening is dat financiële middelen gevonden dienen te worden binnen de bestaande financiële kaders van de EU-begroting.

c) *Financiële consequenties (incl. personele) voor bedrijfsleven en burger*
Geen verandering t.o.v. het eerdere kaderbesluit op dit gebied.

d) *Administratieve lasten voor rijksoverheid, decentrale overheden en/of bedrijfsleven en burger*
Geen verandering t.o.v. het eerdere kaderbesluit op dit gebied.

6. Implicaties juridisch

a) *Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid*
Implementatie zal vermoedelijk leiden tot enkele (vooral technische) aanpassingen van het Wetboek van Strafrecht.

b) *Voorgestelde implementatietermijn*
Twee jaar na inwerkingtreding van het voorstel. Omdat het hier gaat om enkele (vooral technische) aanpassingen van het Wetboek van Strafrecht (zie onder a) is deze implementatietermijn haalbaar.

c) *Wenselijkheid evaluatie-/horizonbepaling*
Vier jaar na inwerkingtreding van het voorstel en vervolgens iedere drie jaar daarna stelt de Commissie een rapport op over de implementatie van de richtlijn. Nederland onderschrijft het belang van periodieke evaluatie van de toepassing van de richtlijn.

7. Implicaties voor uitvoering en handhaving

a) *Uitvoerbaarheid*
De uitvoerbaarheid van het voorstel wordt positief beoordeeld.

b) *Handhaafbaarheid*
De handhaafbaarheid van het voorstel wordt positief beoordeeld.

8. Implicaties voor ontwikkelingslanden

Geen.

9. Nederlandse positie (belangen en eerste algemene standpunt)

De Nederlandse regering staat positief tegenover het voorstel. De aanpak van het misbruik van het internet door terroristen, (niet) statelijke actoren en vooral criminelen. De aanpak van cybercriminaliteit op het niveau van de Europese Unie is een uit het Stockholm Programma voortvloeiende prioriteit. Ondersteuning

daarvan ligt in het verlengde van de in het regeerakkoord opgenomen ambitie van de regering om te komen tot een integrale aanpak op het gebied van cybercrime. Het initiatief van de Commissie sluit aan bij de bestaande praktijk in de aanpak van cybercriminaliteit die inmiddels - mede ter uitvoering van het Cybercrimeverdrag van de Raad van Europa is ontstaan. Nederland is van oordeel dat een richtlijn op het niveau van de Europese Unie op dit terrein zinvol is omdat dit - gelet op de stand van de ratificaties van het Cybercrimeverdrag - een meer uniforme uitvoering van dit verdrag binnen de Unie mogelijk maakt. De vaststelling van minimumvoorschriften op het terrein van de strafbaarstellingen binnen de Unie kan daarnaast op zichzelf ook bijdragen aan de onderlinge samenwerking tussen de lidstaten bij de aanpak van - naar zijn aard veelal grensoverschrijdende – cybercriminaliteit en politiek of terroristisch gemotiveerde aanvallen op informatiesystemen.