Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

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

Nr. 2201 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 9 september 2016

Overeenkomstig de bestaande afspraken ontvangt u hierbij tien fiches, die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC).

Fiche: Besluit meerjarenkader 2018–2022 EU-grondrechtenagentschap (FRA) (Kamerstuk 22 112, nr. 2197)
Fiche: Mededeling over roadmap Commissie voorstellen naar aanleiding van de Panama Papers (Kamerstuk 22 112, nr. 2198)
Fiche: Wijziging vierde anti-witwasrichtlijn en de richtlijn vennootschapsrecht (Kamerstuk 22 112, nr. 2199)
Fiche: Wijziging richtlijn administratieve samenwerking op het gebied van Belastingen (Kamerstuk 22 112, nr. 2200)
Fiche: Verordening integratie LULUCF (Kamerstuk 34 535, nr. 2)
Fiche: Mededeling Een snellere overgang van Europa naar een koolstofarme economie (Kamerstuk 34 535, nr. 3)
Fiche: Mededeling Europese strategie voor emissiearme mobiliteit (Kamerstuk 34 535, nr. 4)
Fiche: Mededeling versterking cyberbeveiligingssysteem en bevorderen cyberbeveiligingsbranche
Fiche: Verordening Brussel IIbis (herschikking) (Kamerstuk 22 112, nr. 2202)
Fiche: Verordening financiering capaciteitsopbouw voor veiligheid en ontwikkeling (Kamerstuk 22 112, nr. 2203)

De Minister van Buitenlandse Zaken,
A.G. Koenders

kst-22112-2201
ISSN 0921 - 7371
's-Gravenhage 2016

Fiche: Mededeling versterking cyberbeveiligingssysteem en bevorderen cyberbeveiligingsbranche

1. Algemene gegevens

a) *Titel voorstel*
Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's – Versterking van het Europese cyberbeveiligingssysteem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche
b) *Datum ontvangst Commissiedocument*
5 juli 2016
c) *Nr. Commissiedocument*
COM(2016) 410
d) *EUR-Lex*
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1470130105280&uri=CELEX:52016DC0410
e) *Nr. impact assessment Commissie en Opinie Impact-assessment Board*
Niet opgesteld
f) *Behandelingstraject Raad*
Raadsconclusies zullen worden besproken in the Friends of Presidency Cyber.
g) *Eerstverantwoordelijk ministerie*
Het Ministerie van Veiligheid en Justitie in nauwe samenwerking met het Ministerie van Economische Zaken.

2. Essentie voorstel

De mededeling van de Commissie is een reactie op de zich voortdurend wijzigende situatie op het gebied van cyberbeveiliging. Het voorstel richt zich op het versterken van de samenwerking, kennis en capaciteit op Europees niveau (hoofdstuk 2), met als doel de weerbaarheid tegen grootschalige grensoverschrijdende cyberdreigingen en -incidenten te verhogen. Dit dekt onder meer preventie (gericht op vitale infrastructuur), respons (met sterkere rol voor EU-instanties zoals Enisa en Europol) en vervolging. Er wordt ook ingezet op versterking van bestaande Europese netwerken. Hiertoe zal er een blauwdruk voor Europese samenwerking worden gepresenteerd uiterlijk in 2017.

Daarnaast richt de mededeling zich op het aanpakken van knelpunten op de Europese eengemaakte markt voor cyberbeveiliging (hoofdstuk 3) en het stimuleren van innovatie (hoofdstuk 4). Het doel hiervan is het wegnemen van geografische versnippering en het stimuleren van de concurrentiepositie van de Europese cyberbeveiligingsbranche. Hiertoe wordt door de Commissie onder meer ingezet op het tot stand brengen van interoperabele technische en procesnormen, en ook EU-wijde certificeringsmechanismen en labeling. Ter stimulering van de concurrentiepositie en innovatie is recent een contractueel Publiek-Privaat Partnerschap (cPPP) opgericht. Daarnaast zullen ook bestaande instrumenten worden aangewend, met aandacht voor het MKB.

3. Nederlandse positie ten aanzien van de mededeling/aanbeveling

a) Essentie Nederlands beleid op dit terrein

Nederland zet samen met zijn internationale partners in op een vrij, open en veilig cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden

en fundamentele rechten en waarden worden beschermd. De samenhang tussen veiligheid, vrijheid en maatschappelijke groei wordt hiertoe, in een dynamische balans, tot stand gebracht in een constante open en pragmatische dialoog tussen alle stakeholders, zowel nationaal als internationaal.

De concrete uitwerking van deze visie is vastgelegd in de Nationale Cyber Security Strategie 2 (NCSS2). Deze uitwerking vindt plaats aan de hand van de volgende vijf door het kabinet gestelde strategische doelstellingen:

1. Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het cyberdomein.
2. Nederland pakt cybercriminaliteit aan.
3. Nederland investeert in veilige en privacybeschermende ICT-producten en -diensten.
4. Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het cyberdomein.
5. Nederland beschikt over voldoende cybersecuritykennis en -kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te behalen.

b) Beoordeling + inzet ten aanzien van dit voorstel

De door de Commissie geschetste dreiging van cyberbeveiligingsincidenten en de knelpunten binnen de Europese eengemaakte markt voor de cyberbeveiligingsbranche worden door het kabinet herkend en onderschreven. Aangezien deze dreigingen en knelpunten inherent grensoverschrijdend zijn is Europese en internationale samenwerking op dit terrein noodzakelijk. De recentelijk aangenomen NIB-richtlijn biedt hierbinnen een goede basis. Het kabinet is daarom blij dat de mededeling van de Commissie dit erkent.

Een aantal van de voornemens en plannen die worden aangekondigd in de mededeling zullen bijdragen aan het realiseren van een aantal van bovengenoemde doelstellingen binnen de NCSS2. Hoewel de concrete uitwerking van die plannen nog door de Commissie zal worden gedeeld met de lidstaten, heeft Nederland een positieve grondhouding ten opzichte van de mededeling.

De mededeling wordt over het algemeen beoordeeld als zijnde voldoende wat betreft subsidiariteit en proportionaliteit. Bij het beoordelen van de concrete plannen, met name die plannen die zich richten op verdergaande samenwerking binnen de EU en opbouw van kennis en capaciteit, behoeven zowel bevoegdheid, subsidiariteit als proportionaliteit extra aandacht.

Nederland zal zich in algemene zin teweerstellen tegen plannen die strijdig zijn met de verdragsrechtelijke afspraken betreffende de bevoegdheid van lidstaten op het gebied van nationale veiligheid. Ook zal erop worden ingezet om zoveel mogelijk uit te gaan van en aansluiting te zoeken bij bestaande structuren, organisaties, initiatieven en mechanismen, in plaats van in te zetten op nieuwe. Daarnaast zal Nederland inzetten op versterking van de Europese cyberbeveiligingsmarkt binnen een open mondiale markt, in plaats van Europa hiervan af te grendelen. Nederland had graag een integrale aanpak gezien, door in lijn met het brede karakter van de Strategie inzake cyberbeveiliging van de Europese Unie ook onderwerpen als cybercriminaliteit, cyberdiplomatie, cyber capaciteitsopbouw en digitale rechten in de mededeling te adresseren. In de verdere uitwerking van de verschillende plannen de komende jaren zal Nederland het belang van een integrale aanpak blijven benadrukken. Daarom steunt Nederland het voornemen van de Commissie om in de

nabije toekomst te onderzoeken of de EU-strategie voor cyberbeveiliging van 2013 moet worden bijgewerkt.

Meer concreet zal Nederland de nog te volgen concretiseringen van de Commissie langs onderstaande hoofdlijnen beoordelen.

Op het gebied van versterken van de samenwerking, kennis en capaciteit (hoofdstuk 2):

- De blauwdruk voor Europese samenwerking voor cyberincidenten evenals versterking van EU-instellingen als Enisa moet aansluiten op bestaande (crisismanagement) mechanismen en netwerken. Deze versterking op Europees niveau dient de informatievergaring en informatiepositie van nationale CSIRT's niet te bemoeilijken of te verzwakken.
- Nederland zal zijn ervaring met publiek-private samenwerking, zoals vormgegeven binnen de Cyber Security Raad (CSR), het Platform Internetstandaarden en ISAC's, uitdragen richting de EU.
- Nederland zal kritisch kijken naar de aangekondigde voornemens om te komen tot verdere specifieke regels en/of richtsnoeren voor de vitale infrastructuur inzake de paraatheid voor cyberrisico's, vanwege mogelijke extra regeldruk als raakvlakken met nationale veiligheid. Ook zal worden benadrukt dat het belangrijk is de effecten van de NIB richtlijn waar relevant hierin worden meegenomen.
- Nederland herkent het belang van voldoende en goed opgeleide cyberbeveiligingsprofessionals. De Nederlandse onderwijsinstellingen kennen veel beleidsruimte en eigen verantwoordelijkheid ten aanzien van het onderwijsaanbod en de opleidingscurricula. Zij zijn zelf aan zet om een kwalitatief goed onderwijsaanbod op te zetten dat aansluit op de vraag van de arbeidsmarkt. Recent zijn verscheidene opleidingen en expertisecentra gestart op het vlak van cyberbeveiliging, zowel in het middelbaar als hoger beroepsonderwijs. Ook is in april 2016 het platform Dcypher van start gegaan, dat onder meer gericht is op het in kaart brengen van vraag en aanbod van cyberbeveiligingopleidingen in het hoger onderwijs en het beter later aansluiten van de cyberbeveiligingopleidingen op de eisen vanuit de arbeidsmarkt. Dit platform kan een goede brugfunctie vervullen naar het door de Commissie beoogde opleidingenplatform.

Op het gebied van de Europese eengemaakte markt voor cyberbeveiliging en het stimuleren van innovatie (hoofdstuk 3 en 4):

- Nederland steunt een samenhangende EU-brede benadering van normering/standaardisering, certificering en labeling, mits deze geen uitsluitende werking heeft voor niet-EU aanbieders en past binnen reeds bestaande structuren (Zoals SOG-IS[1]) en indien mogelijk aangesloten wordt op bestaande open standaarden en via bestaande instanties. Er dient hierbij ook oog te zijn voor de verschillen tussen producten, systemen en diensten, met bijvoorbeeld aandacht voor certificering van trusted hulpverleners, zowel wat betreft aanbod- als vraagkant.[2] Nederland zal proactief blijven in het aanmelden op Europees niveau van relevante open standaarden die cyberveiligheid stimuleren en ondersteunen.
- Het is voor Nederland van belang dat er, bijvoorbeeld bij beleid voor standaardisering en certificering, onderscheid wordt gemaakt tussen

[1] Betrokken landen, naast Nederland, zijn: Duitsland, Finland, Frankrijk, Italië, Noorwegen, Oostenrijk, Spanje, het Verenigd Koninkrijk en Zweden.

[2] Voor meer informatie over trusted hulpverleners zie actie 13 van het Actieprogramma 2014–2016 horende bij de Nationale Cyber Security Strategie 2 en het verslag van het Algemeen Overleg Informatie- en Communicatietechnologie van 5 maart 2015, Kamerstuk 26 643, nr. 354.

producten, systemen en diensten voor de consumentenmarkt en die voor gespecialiseerde afnemers zoals de vitale infrastructuur, die kunnen raken aan nationale veiligheid.
- Het belang van awareness en het bieden van handelingsperspectieven verdient continue aandacht, of dit nu ten behoeve van consumenten, mkb-ers of de boardroom van grotere bedrijven is. Nederland zal de Commissie vragen hier ook voldoende aandacht voor te hebben en te houden.
- Nederland steunt het cPPP en zal via de reguliere Horizon 2020 structuren inhoudelijke input geven. Hierbij zal NL erop wijzen dat het cPPP de snelheid en dynamiek van de markt niet moet belemmeren, en dat het cPPP flexibel genoeg moet zijn om aangesloten te blijven bij marktontwikkelingen, bijvoorbeeld middels projecten die aansluiten bij lopende initiatieven in lidstaten.

c) Eerste inschatting van krachtenveld

De in de mededeling aangekondigde plannen gericht op de Europese eengemaakte markt en innovatie zullen naar verwachting op principesteun van lidstaten en het EP kunnen rekenen. Waar de verdere gedetailleerdere uitwerking van die plannen wellicht ingaat tegen al bestaande nationale initiatieven en structuren, bijvoorbeeld op het gebied van certificering, kan er meer weerstand vanuit lidstaten komen.

De plannen gericht op het versterken van de samenwerking, kennis en capaciteit binnen Europa zullen wegens hun raakvlakken met nationale veiligheid en bevoegdheden naar verwachting meer tegenstand oproepen vanuit de lidstaten. Wat aan deze tegenstand zal bijdragen is het feit dat veel lidstaten de komende twee jaar veel werk zullen hebben aan de transpositie van de NIB richtlijn naar nationale wetgeving en daarom weinig animo zullen hebben voor nog meer aanvullende regelgeving uit Brussel, voordat de transpositie is afgerond.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen op het gebied van regeldruk en administratieve lasten

Hoofdstuk 2 in de mededeling, dat gaat over versterken van de samenwerking, kennis en capaciteit binnen Europa, bevat oplossingen voor politiek-bestuurlijke en veiligheidsvraagstukken rondom cyberbeveiliging. Het is hiermee van een ander karakter dan hoofdstukken 3 en 4, die zich richten op economische vraagstukken rondom de Europese eengemaakte markt. Per onderdeel zullen daarom hoofdstuk 2 en hoofdstuk 3 en 4 separaat van elkaar worden beoordeeld.

a) Bevoegdheid

<u>Versterking samenwerking, kennis en capaciteit</u>

Een aantal van de aangekondigde acties en plannen bevinden zich dicht tegen of op het terrein van nationale veiligheid. Bij het beoordelen van de concrete plannen van de Commissie zal daarom nauwgezet moeten worden gekeken of de Commissie zijn bevoegdheden niet overschrijdt. Het betreft hier een aanvullende bevoegdheid van Unie (zie artikel 6, onder 3, VWEU). Hetzelfde geldt voor de bevoegdheden op het gebied van onderwijs. Wel kan worden ingestemd met het vervroegen van de aanpassing van het mandaat van Enisa. In algemene zin heeft NL een positieve grondhouding ten opzichte van meer Europese samenwerking op dit vlak.

Europese eengemaakte markt en bevordering innovatie

Gezien de bevoegdheid van de Europese Unie op economisch vlak vallen de plannen binnen de mededeling wat betreft de Europese eengemaakte markt en voor bevordering van innovatie grotendeels binnen de bevoegdheden van de EU. Het betreft hier een gedeelde bevoegdheid van de Unie en de lidstaten in het kader van de interne markt (artikel 4, lid 2, sub a, VWEU). Een (potentiële) uitzondering hierop is de standaardisering en certificering van high-end producten, vanwege de mogelijke link met nationale veiligheid. Voor dergelijke producten is het belangrijk dat in de uitwerking van toepassing zijnde verdragsrechtelijke bepalingen in acht worden genomen.

b) Subsidiariteit

Versterking samenwerking, kennis en capaciteit

Gezien het inherent grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging heeft NL een positieve grondhouding met betrekking tot het versterken van de samenwerking, kennis en capaciteit op Europees niveau. Niettemin zal Nederland er scherp op toezien dat niet uit het oog wordt verloren dat nationale veiligheid een exclusieve competentie is van de lidstaten zelf.

Europese eengemaakte markt en bevordering innovatie

Het wegnemen van knelpunten binnen de Europese eengemaakte markt om zo een gelijk speelveld voor de cyberbeveiligingsbranche te creëren kan enkel op EU-niveau gebeuren. Hiertoe wordt de subsidiariteit van deze mededeling in principe positief beoordeeld.

c) Proportionaliteit

De proportionaliteit van de mededeling kan pas echt worden beoordeeld nadat de verschillende plannen erin verder geconcretiseerd worden. Nederland zal er bij deze concretisering steeds op aandringen om zoveel mogelijk aansluiting te zoeken bij bestaande structuren, netwerken en initiatieven. Het creëren van geheel nieuwe structuren zal als disproportioneel worden beoordeeld.

Versterking samenwerking, kennis en capaciteit

Voor het versterken van de samenwerking, kennis en capaciteit zal een specifiek aandachtspunt zijn dat er met name binnen de bestaande (crisis)plannen en structuren wordt gewerkt en er geen nieuwe structuren worden opgetuigd waar dit niet nodig is. Bij eventuele regels voor de vitale infrastructuur zal erop worden gelet dat deze voldoende rekening houden met de eventuele effecten van de NIB richtlijn. De transpositie hiervan is immers pas net begonnen en zal pas medio 2018 door alle lidstaten zijn afgerond.

Europese eengemaakte markt en bevordering innovatie

Een goed functionerende Europese eengemaakte markt met hoogwaardige cyberbeveiligingsproducten en -diensten is van groot belang. Samenwerking met het bedrijfsleven en het verkennen van de mogelijkheden van standaardisatie en certificering op Europees niveau zijn logische stappen op weg naar dat doel.

d) Financiële gevolgen

Zoals beneden nader wordt aangegeven is het mogelijk dat een of meerdere van de aangegeven voornemens zal leiden tot uitgaven vanuit de EU begroting die nu nog niet worden gedaan. Nederland is van mening dat de benodigde EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2014–2020 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Op nationaal niveau zullen (eventuele) budgettaire gevolgen worden ingepast op de begroting van het/de beleidsverantwoordelijk(e) departement(en), conform de regels van de budgetdiscipline.

Versterking samenwerking, kennis en capaciteit

De plannen gericht op versterking van de weerbaarheid tegen pan-Europese cyberincidenten, zoals de op te richten informatiehub en de nieuw op te richten adviesgroep op hoog niveau, kunnen een impact hebben op de benodigde capaciteit bij betrokken organisaties en ondersteunende uitgaven hiertoe. Ook de wijziging of verlenging van het Enisa-mandaat kan gevolgen hebben voor de grootte van deze organisatie en het gevraagde budget. Nederland zal de Commissie vragen precies aan te geven wat het financieel beslag van de toekomstige voorstellen zal zijn en deze beoordelen binnen de afgesproken financiële kaders.

Europese eengemaakte markt en bevordering innovatie

De EU financiële inbreng in het cPPP zal worden gefinancierd vanuit bestaande Horizon 2020 fondsen. De verhoging van de investeringen in cyberbeveiliging en ondersteuning van het MKB zal ook via bestaande financieringsfaciliteiten, oproepen en fondsen gebeuren, zoals de financieringsfaciliteit voor Europese verbindingen, de COSMO oproepen en het Europees Fonds voor strategische investeringen (EFSI). Deze betekenen daarmee geen budgetverhoging voor de EU. Het genoemde nieuwe investeringsplatform voor cyberbeveiliging dat nader zal worden onderzocht zal wellicht financiering nodig hebben. Nederland zal de Commissie vragen precies aan te geven wat het financieel beslag van de toekomstige voorstellen zal zijn.

e) Gevolgen voor regeldruk, administratieve lasten en concurrentiekracht

Versterking samenwerking, kennis en capaciteit

Of de mededeling gevolgen zal hebben voor regeldruk of administratieve lasten zal per concreet voorstel moeten worden bekeken. Indien er van toename sprake zal zijn, zal dit naar verwachting voor de rijksoverheid voortvloeien uit de uitwerking van de blauwdruk rondom crisismanagement en mogelijke extra regels en/of richtsnoeren inzake de paraatheid van vitale sectoren. Dat laatste zal mogelijk ook gevolgen hebben voor de administratieve lasten voor het bedrijfsleven. De beoogde integratie van cyberbeveiliging in de Europese sectorale beleidsmaatregelen kan tevens gevolgen hebben voor regeldruk voor het bedrijfsleven en ook diens internationale concurrentiekracht. Nederland zal de nog op te richten vertrouwelijke kanalen voor vrijwillige melding van cyberdiefstal van bedrijfsgeheimen nauwgezet volgen met het oog op eventuele gevolgen wat betreft regeldruk, administratieve lasten en concurrentiekracht.

Europese eengemaakte markt en bevordering innovatie

Het wegnemen van obstakels tussen landen binnen de EU en het stimuleren van EU-brede afspraken rondom certificering en labeling, en van innovatie zal naar verwachting positief bijdragen aan de concurrentiekracht van Nederlandse en Europese bedrijven wereldwijd. De impact hiervan is zonder meer concrete voorstellen op het moment nog niet te kwantificeren.

Voor zowel de maatregelen gericht op versterking samenwerking, kennis en capaciteit als voor de Europese eengemaakte markt geldt dat onvoorziene stijgingen van de administratieve lasten dienen te worden gecompenseerd door het beleidsverantwoordelijke departement, waarbij compensaties zoveel mogelijk dienen te geschieden binnen het domein waarin de tegenvaller plaatsvindt.