Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2012–2013

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

33 602 EU-voorstel: Netwerk- en informatiebeveiliging in de Unie COM(2013)48

GC[1]

BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 15 maart 2013

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

Fiche 1: Wijziging verordening GNSS-Agentschap
Fiche 2: Richtlijn strafrechtelijke bescherming tegen eurovalsemunterij
Fiche 3: Richtlijn netwerk- en informatiebeveiliging
Fiche 4: Mededeling strategie inzake cyberbeveiliging van de Europese Unie
Fiche 5: Verordening veiligheid consumentenproducten

De minister van Buitenlandse Zaken,
F.C.G.M. Timmermans

[1] Deze letters hebben alleen betrekking op 22112.

kst-22112-GC
ISSN 0921 - 7371
's-Gravenhage 2014

Fiche 4: Mededeling Strategie inzake cyberbeveiliging van de Europese Unie

1. Algemene gegevens

Titel voorstel
Gezamenlijke mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's over de strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace.

Datum ontvangst Commissiedocument
7 februari 2013

Nr. Commissiedocument
JOIN(2013)1

Pre-lex
Er is geen link in Pre-lex naar dit document.

Nr. impact assessment Commissie en Opinie Impact-assessment Board
Niet opgesteld.

Behandelingstraject Raad
JBZ-Raad

Eerstverantwoordelijk ministerie
Ministerie van Veiligheid en Justitie

2. Essentie voorstel

De Europese Commissie en de Hoge Vertegenwoordiger onderkennen dat een open, veilig en betrouwbaar internet van fundamenteel belang is voor onze welvaart en welzijn. Het internet biedt kansen, maar als het onveilig en onbetrouwbaar is, verhoogt het ook de kwetsbaarheid van een samenleving waarin steeds meer vitale producten en diensten met elkaar verweven zijn. Een moedwillige of onopzettelijke verstoring als gevolg van technische storing of menselijk handelen of door natuurlijke oorzaken kan leiden tot maatschappelijke ontwrichting.
De mededeling voorziet in een strategie om de digitale omgeving in de EU de veiligste in de wereld te maken. Hiertoe beschrijft de mededeling de vereiste maatregelen die hiervoor nodig zijn op basis van een sterke en effectieve bescherming en bevordering van de rechten van de burgers. De EU wil openheid en vrijheid op het internet bevorderen, de ontwikkeling van gedragsnormen aanmoedigen en bestaande internationale wetgeving in cyberspace toepassen. Hierbij gelden onverkort de kernwaarden van de EU, namelijk de menselijke waardigheid, vrijheid, democratie, gelijkheid, de rechtstaat en de eerbiediging van de grondrechten.
De mededeling gaat uit van een aantal principes: dezelfde wetten en normen; de kernwaarden van de EU gelden net zo goed voor de digitale als voor de fysieke wereld; bescherming van grondrechten, vrijheden en bescherming van persoonsgegevens en persoonlijke levenssfeer; vrije toegang tot internet; democratische en efficiënte *multistakeholder-governance*; en, tot slot, gedeelde verantwoordelijkheid van de private en publieke sector alsmede burgers om bij te dragen aan een veilig internet.
De mededeling benoemt vijf strategische prioriteiten: een veerkrachtiger cyberspace, drastische vermindering van cybercriminaliteit, ontwikkeling van cyberdefensiebeleid- en capaciteit in het kader van het gemeenschappelijke veiligheids- en defensiebeleid, ontwikkeling van industriële en technologische voorzieningen voor cyberbeveiliging en tot slot de

ontwikkeling van een coherent internationaal cyberbeveiligingsbeleid voor de EU en het uitdragen van de kernwaarden van de EU.

3. Wat is de Nederlandse grondhouding ten aanzien van de bevoegdheidsvaststelling, subsidiariteit en proportionaliteit van deze mededeling en de eventueel daarin aangekondigde concrete wet- en regelgeving? Hoe schat Nederland de financiële gevolgen in, alsmede de gevolgen op het gebied van regeldruk en administratieve lasten?

Bevoegdheidsvaststelling

Nederland onderschrijft het standpunt van de Europese Commissie en de Hoge Vertegenwoordiger dat om de veerkracht van cyberspace in de EU te bevorderen, zowel overheden als de private sector capaciteiten moeten ontwikkelen en doeltreffend moeten samenwerken. De Europese Commissie en de Hoge Vertegenwoordiger constateren dat op basis van vrijwillige verplichtingen er wel vooruitgang is geboekt, maar binnen de EU er nog steeds lacunes zijn. Met name op het gebied van nationale capaciteit van cyberbeveiliging, coördinatie bij grensoverschrijdende incidenten en de betrokkenheid van de private sector. Verder wordt er aandacht gevraagd voor het (grensoverschrijdend) uitwisselen van *best practices* tussen de publieke en private sector om zo de paraatheid van alle partijen te verhogen. Nederland is van mening dat de Europese Commissie en de Hoge Vertegenwoordiger een belangrijke rol kunnen spelen in het creëren van een gelijkwaardig niveau tussen lidstaten op het terrein van cyberbeveiliging. Omdat cyberdreigingen veelal een internationaal karakter hebben heeft Nederland een direct belang bij een goede cyberbeveiliging in andere EU-lidstaten.
In de mededeling doen de Europese Commissie en de Hoge Vertegenwoordiger een beroep op publieke en private partijen, maar ook aan de lidstaten om de gedeelde verantwoordelijkheid te erkennen, maatregelen te nemen en zo nodig te zorgen voor een gecoördineerde reactie om de cyber beveiliging te versterken. Voor verplichtende maatregelen wordt in de mededeling verwezen naar het NIS ontwerpvoorstel.

Subsidiariteit

Positieve grondhouding. Nederland ondersteunt het doel van de mededeling om meer gelijkwaardigheid tussen lidstaten te realiseren op het terrein van cyberbeveiliging. Momenteel heeft elke lidstaat de vrijheid om te besluiten hoe en in welke mate de cyberbeveiliging wordt ingericht. Hierdoor bestaan er grote verschillen tussen de lidstaten. Nederland maakt echter wel een voorbehoud ten aanzien van de specifieke maatregelen zoals deze benoemd worden in de strategie.
Uit de mededeling komt niet duidelijk naar voren of de voorgenomen maatregelen ook hun weerslag hebben op de bescherming van de nationale veiligheid en openbare orde. Nederland is van mening dat de bescherming van de openbare orde en veiligheid een nationale aangelegenheid is.

Dit neemt niet weg dat de Europese Commissie en de Hoge Vertegenwoordiger een belangrijke rol spelen om samenwerking tussen EU-lidstaten onderling en binnen de EU te bevorderen. Dit is van belang bij bijvoorbeeld grensoverschrijdende cyberincidenten. Door goede internationale afspraken tussen CERTs (*Computer Emergency Response Team*) en crisisautoriteiten kunnen adequate maatregelen genomen worden om een crisis vroegtijdig te beheersen.
Een aantal maatregelen zoals beschreven in de strategie, wordt nader uitgewerkt in het bijbehorende voorstel voor een richtlijn van het

Europese Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen (2013/0027 (COD)). Zie voor de subsidiariteit en proportionaliteit van dit voorstel het BNC COM(2012)48 richtlijn netwerk en informatie beveiliging.

Proportionaliteit

Positief. Bij de uitwerking van de maatregelen zoals voorgesteld in de mededeling zal Nederland per maatregel de proportionaliteit beoordelen. Nederland beschouwt de voorgestelde maatregelen op het gebied van cyberbeveiliging in EU-verband een effectieve manier om meer gelijkwaardigheid tussen de lidstaten te realiseren. Dit is van belang om betrouwbaar, effectief en tijdig informatie uit te wisselen over incidenten. De Europese strategie sluit aan bij de nationale inspanningen op het gebied van cyberbeveiliging. Nederland is wel van mening dat zoveel mogelijk gebruik moet worden gemaakt van bestaande nationale en internationale structuren. Dus geen nieuwe structuren die bestaande structuren binnen lidstaten vervangen of dupliceren op Europees niveau. Daarnaast verwelkomt Nederland de voorgestelde maatregelen om vanuit de EU de lidstaten te ondersteunen bij het opbouwen van cybercapaciteiten en het versterken van samenwerkingsverbanden.

Financiële gevolgen:

Indien het voorstel budgettaire gevolgen heeft, zullen deze worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels budgetdiscipline.

De financiering van de strategie valt binnen de bedragen die zijn uitgetrokken voor elk van de desbetreffende beleidsterreinen (Connecting Europe Facility (CEF), Horizon 2020, het fonds voor interne veiligheid, Gemeenschappelijk Buitenlands en Veiligheidsbeleid en externe samenwerking, met name het stabiliteitsinstrument), zoals vastgelegd in het voorstel van de Commissie voor het meerjarig financieel kader 2014–2020 (afhankelijk van de goedkeuring van de begrotingsautoriteit en de bedragen die uiteindelijk in het meerjarig financieel kader voor 2014–2020 worden vastgesteld). Agentschappen (European Police College (CEPOL), European Defense Agency, ENISA, EUROJUST en EuropOL/ Europees Cyber Crime Centrum) die op grond van deze mededeling worden verzocht nieuwe taken op zich te nemen, worden aangemoedigd dit te doen. Dit voor zover het daadwerkelijke vermogen van het agentschap om meer middelen te absorberen is vastgesteld en alle mogelijkheden voor herindeling zijn bepaald.

4. Nederlandse positie over de mededeling

Nederland is positief dat er een cyberbeveiligingsstrategie van de Europese Unie is voorgesteld. Tevens onderstreept Nederland het belang dat de verschillende onderdelen binnen de Europese Commissie die zich met cyberbeveiliging en cyberspace bezighouden in samenhang optrekken. Deze breed ingestoken Europese cyberbeveiligingsstrategie draagt bij aan versterking van de integrale markt en samenwerking binnen de EU op dit onderwerp.

Deze strategie ziet Nederland als een volgende belangrijke stap om binnen de EU een meer gelijkwaardig niveau van cyberbeveiliging te realiseren. Dit bevordert het onderling vertrouwen en de samenwerking tussen lidstaten op dit onderwerp, wat belangrijk is omdat cyberdreigingen en de bestrijding ervan vaak grensoverschrijdend zijn.

Nederland staat positief tegenover de mededeling van de Europese Commissie en de Hoge Vertegenwoordiger om een open, vrije en beveiligde cyberomgeving voor de EU te creëren. Deze uitdaging gaat de EU aan samen met haar internationale partners en organisaties, de private sector en het maatschappelijke middenveld. De EU wil openheid en vrijheid op het internet bevorderen, de ontwikkeling van gedragsnormen aanmoedigen en bestaande internationale wetgeving in cyberspace toepassen. Hierbij gaat zij uit van de kernwaarden van de EU, namelijk waardigheid, vrijheid, democratie, gelijkheid, rechtsstatelijkheid en eerbiediging van de grondrechten. Nederland onderschrijft deze kernwaarden en ziet deze als het fundament waarop de mededeling is gebouwd.

Nederland onderschrijft het standpunt dat om de veerkracht en weerbaarheid van cyberspace in de EU te bevorderen, zowel overheden als de private sector capaciteiten moeten ontwikkelen en doeltreffend moeten samenwerken. De Europese Commissie en de Hoge Vertegenwoordiger constateren dat op basis van vrijwillige verplichtingen er wel vooruitgang is geboekt, maar binnen de EU er nog steeds lacunes zijn. Met name op het gebied van nationale capaciteit voor cyberbeveiliging, coördinatie bij grensoverschrijdende incidenten en de betrokkenheid van de private sector. Verder wordt er aandacht gevraagd voor het (grensoverschrijdend) uitwisselen van *best practices* tussen de publieke en private sector om zo de paraatheid van alle partijen te verhogen. Ook in de Nederlandse cyberbeveiligingstrategie vormt de publiek-private samenwerking een basis principe.

In het kader van het terugdringen van cybercrime ligt bij de strategie de nadruk op de implementatie van reeds overeengekomen kaders. Bijvoorbeeld de *cyber crime* conventie van de Raad van Europa en de EU-richtlijn ter bestrijding van kinderporno. Verder staat de vergroting van de operationele capaciteit om *cyber crime* aan te pakken centraal. De Europese Commissie en de Hoge Vertegenwoordiger zullen daarvoor EU financieringsprogramma's inzetten en samenwerking zoeken met het onlangs opgerichte European Cybercrime Centre (EuropOL/EC3). Nederland vindt het van belang dat de door de Europese Commissie en de Hoge Vertegenwoordiger voorgenomen stappen richting European Cybercrime Centre (EuropOL/EC3), EUROJUST passen in de kaders en prioriteitstelling van deze organisaties.

Nederland hecht ook belang aan een goede samenwerking van de Europese Unie met internationale organisaties (o.a. de NAVO zoals ook eerder opgenomen in de kabinetsreactie op het AIV/CAVV-advies Digitale Oorlogsvoering) en strategische landen (o.a. Verenigde Staten, India, maar ook China). In dit kader is Nederland voorstander van expliciete en aparte aandacht voor internationale samenwerking, naast het uitdragen van EU-waarden.

Nederland steunt de voorstellen gericht op het verbeteren van de intrinsieke veiligheid van ICT-producten. Daarbij zal een goede balans moeten worden gevonden tussen de zorgplicht van ontwikkelaars en leveranciers van deze producten en goed opdrachtgeverschap aan de zijde van de afnemers ervan. Een goede vraagarticulatie naar veilige producten geeft ook een impuls aan de verbetering ervan. Nederland onderschrijft het standpunt van de Europese Commissie en de Hoge Vertegenwoordiger dat het voortouw voor normering en standaarden bij de industrie ligt maar dat initiatieven zoals een gezamenlijk platform van bedrijfsleven en overheid, alsmede richtsnoeren hieraan kunnen bijdragen.

In de mededeling is een groot aantal voorgenomen maatregelen opgenomen. Bij de prioritering en verdere uitwerking van deze maatregelen acht Nederland de volgende aandachtspunten van belang:

- De maatregelen dienen zoveel mogelijk aan te sluiten bij bestaande structuren in en tussen de lidstaten en de Europese Unie.
- De noodzaak van vertrouwelijkheid, privacy en proportionaliteit dient geborgd te zijn bij het bevorderen van het delen van informatie tussen lidstaten en binnen de EU. Dit is met name van belang daar waar het gaat om het melden van incidenten of het delen van specifieke dreigingsinformatie welke in vertrouwelijkheid is verkregen van publieke en private organisaties. Nederland is voorstander een gedeeld dreigingsbeeld middels het ontwikkelen en uitwisselen van concrete scenario's op Europees niveau.
- Nederland hecht belang aan proportionaliteit en nationaal maatwerk bij de uitwerking van maatregelen, onder andere bij het invullen van de sectoren in het kader van een meldplicht zoals omschreven in het voorstel voor een richtlijn netwerk- en informatiebeveiliging. Nederland is voorstander om de meldplicht te beperken tot de sectoren waar een aanzienlijke impact is te verwachten indien deze uitvallen. Voor de energiesector zou dit bijvoorbeeld de netbeheerders kunnen betreffen. Vanuit het oogpunt van bewustmaking vindt Nederland het positief wanneer scholen aandacht aan cyberbeveiliging besteden. Nederland zal dit – met het oog op de autonomie van de scholen – echter niet voorschrijven.
- Nederland steunt het voorstel om na 12 maanden de voortgang van de uitwerking van de mededeling te bekijken.

Ten slotte,
Nederland ziet deze mededeling als een belangrijke stap voor verbeterde integrale samenwerking op het niveau van de Europese Unie, vergelijkbaar met haar eigen nationale cyber security strategie welke in 2011 is ontwikkeld. Cyberbeveiliging is een beleidsterrein in ontwikkeling met vele facetten. Het is voor Nederland van belang dat dit beleidsterrein in zijn geheel wordt blijven bezien. In de visie van Nederland mag in een volgende stap meer aandacht zijn voor:

- Publiek-private samenwerking.
- Onderzoek en ontwikkeling
- Civiel-militaire samenwerking en de externe coördinatie bij internationale samenwerking, inclusief verdere verduidelijking van de plek van cyberbeveiliging in het GVDB als onderdeel van het GBVB.
- Verdere invulling van de *governance* structuur.
- Intensivering van de Europese samenwerking bij opsporing (rol EC3/Europol)