

Ministerie van Buitenlandse Zaken

Aan de Voorzitter van de
Tweede Kamer der Staten-Generaal
Binnenhof 4
Den Haag

Bezuidenhoutseweg 67
2594 AC Den Haag
Postbus 20061
Nederland
www.minbuza.nl

Contactpersoon
Joop Nijssen

T 0031 70 348 4858
DIE-BNC@minbuza.nl

Onze Referentie
Minbuza-2013.125861

Bijlage(n)
fichedocument

Datum 15 maart 2013
Betreft Informatievoorziening over nieuwe Commissievoorstellen

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,

Frans Timmermans

Fiche 1: Wijziging verordening GNSS-Agentschap

1. Algemene gegevens

Titel voorstel Verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 912/2010 tot oprichting van het Europese GNSS-Agentschap

Datum ontvangst Commissiedocument

06 februari 2013

Nr. Commissiedocument

COM(2013) 40

Prelex: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=nl&DosId=202362

Nr. Impact Assessment Commissie en Opinie Impact Assessment Board

Niet opgesteld

Behandelingstraject Raad

Raad voor transport, telecommunicatie en energie

Eerstverantwoordelijk ministerie

Infrastructuur en Milieu

Rechtsbasis, besluitvormingsprocedure Raad, rol Europees Parlement, gedelegeerde en/of uitvoeringshandelingen

- a) *Rechtsbasis:* Artikel 172 van het Verdrag betreffende de werking van de Europese Unie (VWEU)
- b) *Besluitvormingsprocedure Raad en rol Europees Parlement:*
Gewone wetgevingsprocedure als vastgelegd in artikel 172 van het VWEU. Gekwalificeerde meerderheid in de Raad en medebeslissing van het Europees Parlement.
- c) *Gedelegeerde en/of uitvoeringshandelingen:*
Niet van toepassing.

2. Samenvatting BNC-fiche

- *Korte inhoud voorstel*

Het voorstel voor de toekomstige GNSS (Global Navigation Satellite System) verordening (COM(2011)814) legt het toekomstige bestuur van de exploitatiefase voor de Europese programma's vast en voorziet in een verantwoordelijkheid voor de Europese GNSS Autoriteit (GSA) voor de exploitatie van het systeem. Hierdoor dient de huidige taak van de GSA op het

gebied van veiligheidsaccreditatie (oordeel over de mate waarin wordt voldaan aan vooraf geformuleerde veiligheidseisen) meer onafhankelijk te worden verankerd om belangenverstrengeling te voorkomen. De Commissie kiest ervoor om veiligheidsaccreditatie een zelfstandige en onafhankelijke taak binnen het GNSS agentschap te maken. Het voorstel beoogt deze onafhankelijkheid te realiseren door de Security Accreditation Board (SAB) een positie te geven die vergelijkbaar is met de Directeur en de Administrative Board. Verder krijgt de SAB de bevoegdheid om de eigen planning van activiteiten en de rapportages vast te stellen.

- *Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel*: Positief.
- *Implicaties/risico's/kansen*

Het voorstel incorporeert tevens het gemeenschappelijk standpunt van Raad, Commissie en Europees Parlement over de harmonisering van de werkwijze van agentschappen. Het voorstel is gedaan onder voorwaarde van overeenstemming over de GNSS verordening, die verordening 683/2008 moet vervangen. Financiële dekking komt uit de middelen die in het MFK 2014-2020 zijn voorzien.

- *Nederlandse positie*

Nederland staat positief tegenover het voorstel onder voorwaarde van goedkeuring van het Meerjarig Financieel Kader en de GNSS verordening. Het voorstel is een logische uitwerking van de beoogde taakverdeling in de exploitatiefase van de Europese GNSS systemen.

3. Samenvatting voorstel

- *Inhoud voorstel*

Het voorstel voor de toekomstige GNSS verordening (implementatie en exploitatie van de systemen) brengt een toename van de bevoegdheden van het GNSS-Agentschap met zich mee. Met name het beheer en exploitatie van de twee satellietssystemen is vanwege mogelijke belangenconflicten niet verenigbaar met de huidige inbedding van de taak van het agentschap op het gebied van veiligheidsaccreditatie (verordening 912/2010). Deze exploitatietaken starten al in 2014, vandaar dat haast is geboden met dit voorstel. De Commissie verkent een zestal mogelijkheden van inbedding en komt tot de conclusie dat veiligheidsaccreditatie een zelfstandige en onafhankelijke taak binnen het GNSS agentschap moet worden.

Deze positie wordt in het voorstel op de volgende wijze uitgewerkt:

- Een positie van de Security Accreditation Board (SAB) en haar voorzitter die vergelijkbaar is met die van de Directeur en de Administrative Board;
- De Board stelt het eigen gedeelte van het meerjarige werkprogramma en verslaglegging vast en kan op verzoek aan het Europees Parlement rapporteren.

Het voorstel maakt de weg vrij voor uitbreiding van de staf van de GSA om de nieuwe taken uit te voeren voortvloeiend uit de toekomstige exploitatie van de GNSS-systemen die nu onder verantwoordelijkheid van de Commissie worden ontwikkeld. Het gaat om een toename van 94 (2013) tot 156 (2020). Deze wordt gefinancierd uit het Meerjarig Financieel Kader 2014-2020.

Deze uitbreiding wordt gedeeltelijk gecompenseerd door een afname van 30 fte's bij de Commissie.

Een derde deel van de wijzigingen heeft te maken met het aanpassen van deze verordening aan de gemeenschappelijke aanpak door het Europees Parlement, de Raad en de Commissie over gedecentraliseerde agentschappen.

- *Impact assessment Commissie*

De Commissie heeft geen impact assessment uitgevoerd omdat over het bestuur van de Europese programma's voor satellietnavigatie al op hoofdlijnen overeenstemming bestaat tussen Raad, Commissie en Europees Parlement. Het functioneren van de GSA zal uiterlijk in 2016 worden geëvalueerd.

4. Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel

a) *Bevoegdheid*

De EU is bevoegd op grond van 172 WVEU. Nederland kan zich daarin vinden.

b) *Subsidiariteits- en proportionaliteitsoordeel*

De subsidiariteit wordt positief beoordeeld. De beoogde activiteiten hebben betrekking op een gemeenschappelijk systeem dat in het kader van het lopende Europese programma voor satellietnavigatie wordt opgebouwd. De subsidiariteit voor ontwikkeling en bouw van dit systeem is eerder positief beoordeeld. Ook de exploitatie kan alleen op Europees niveau worden uitgevoerd. De proportionaliteit wordt positief beoordeeld. De Commissie kiest door inbedding in de bestaande GNSS structuur voor een kostenefficiënte oplossing die in de bestaande bestuurlijke context past.

c) *Nederlands oordeel over de voorstellen op het gebied van gedelegeerde en/of uitvoeringshandelingen*

Het voorstel bevat geen gedelegeerde en uitvoeringshandelingen.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) *Consequenties EU-begroting*

De dekking van de kosten voor de nieuwe taken van de GSA maakt onderdeel uit van de middelen die in het meerjarig financieel kader 2014-2020 zijn opgenomen voor de Europese GNSS Programma's. U bent hierover geïnformeerd via het BNC-fiche EU-satelliet navigatie systemen (kamerstuk 22112-1312).

b) *Financiële consequenties voor rijksoverheid en/ of decentrale overheden:* Geen, echter mocht toch blijken dat er budgettaire gevolgen zijn, dan worden deze ingepast op de begroting van het beleidsverantwoordelijk departement(en), conform de regels van de budgetdiscipline.

c) *Financiële consequenties voor bedrijfsleven en burger:* Geen.

d) *Gevolgen voor regeldruk/administratieve lasten voor rijksoverheid, decentrale overheden, bedrijfsleven en burger:* Geen.

6. Implicaties juridisch

- a) *Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo):* Geen.
- b) *Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en beschikkingen) met commentaar t.a.v. haalbaarheid:* N.v.t.
- c) *Wenselijkheid evaluatie-/horizonbepaling:* De nieuwe GNSS verordening voorziet in een midterm evaluatie van het programma.

7. Implicaties voor uitvoering en handhaving

- a) *Uitvoerbaarheid:* Geen.
- b) *Handhaafbaarheid:* Geen.

8. Implicaties voor ontwikkelingslanden

Geen.

9. Nederlandse positie

Nederland staat positief tegenover het voorstel. Door de te wijzigen taken van de GSA in de nieuwe GNSS verordening zou een belangentegenstelling kunnen ontstaan tussen accreditatieactiviteiten en de verantwoordelijkheid voor exploitatie.

Vanwege overwegingen van (kosten)efficiëntie steunt Nederland het als zelfstandige activiteit onderbrengen van de accreditatieactiviteiten binnen de GSA.

Nederland heeft de volgende aandachtspunten/opmerkingen:

- De aanwijzingen van de Commissie zoals opgenomen in art. 3.2 (aanwijzingen van de Commissie) mogen niet de inhoud van de securityactiviteiten aangaan;
- Art. 4 (Rechtspositie en lokale vestigingen) dient in overeenstemming te zijn met het geldende nationale beleid;
- Art. 6d dient in overeenstemming te worden gebracht met besluitvorming over additionele vestigingen van het GNSS programma; die dienen toegevoegd te worden.

Fiche 2: Richtlijn strafrechtelijke bescherming tegen eurovalsemunterij

1. Algemene gegevens

Titel voorstel

Ontwerp-richtlijn van het Europees Parlement en de Raad betreffende de strafrechtelijke bescherming van de euro en andere munten tegen valsemunterij en ter vervanging van Kaderbesluit 2000/383/JBZ van de Raad

Datum ontvangst Commissiedocument

6 februari 2013

Nr. Commissiedocument

COM(2013)42

Prelex

http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=nl&DosId=202363

Nr. Impact Assessment Commissie en Opinie Impact Assessment Board

SWD(2013)19

Behandelingstraject Raad

De richtlijn wordt behandeld in de JBZ-Raad.

Eerstverantwoordelijk ministerie

Ministerie van Veiligheid en Justitie

Rechtsbasis, besluitvormingsprocedure Raad, rol Europees Parlement, gedelegeerde en/of uitvoeringshandelingen

- a) *Rechtsbasis*: artikel 83, eerste lid, VWEU
- b) *Besluitvormingsprocedure Raad en rol Europees Parlement*: gewone wetgevingsprocedure
- c) *Gedelegeerde en/of uitvoeringshandelingen*: n.v.t.

2. Samenvatting BNC-fiche

- *Korte inhoud voorstel*

De ontwerp-richtlijn stelt minimumregels vast voor de strafbaarstelling van een reeks van gedragingen die verband houden met (euro)valsemunterij. Het voorstel bevat daarnaast onder meer voorschriften over straffen, rechtsmacht, onderzoeksmiddelen en over de analyse, identificatie en opsporing van vals geld.

- *Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel*

Het voorstel is terecht gebaseerd op artikel 83, eerste lid, VWEU voor zover het de beoogde harmonisering van de strafbepalingen inzake eurovalsemunterij betreft. Voor zover het betreft de voorstellen op het punt van de onderlinge afstemming van de strafvorderlijke voorzieningen worden nadrukkelijk vraagtekens gezet bij de gekozen rechtsgrondslag.

Subsidiariteit: positief

Proportionaliteit: positief, maar negatief ten aanzien van het voorstel van minimumstraffen.

- *Implicaties/risico's/kansen*

Het voorstel kan Uniebreed de strafrechtelijke bestrijding van eurovalsemunterij versterken.

- *Nederlandse positie*

Nederland onderschrijft het belang van een krachtig strafrechtelijk instrumentarium om eurovalsemunterij tegen te gaan. Daarbij past dat alle lidstaten een vergelijkbaar niveau van strafrechtelijke bescherming bieden tegen gedragingen die te maken hebben met het vervalsen van de euro. Inhoudelijk gaat de aandacht primair uit naar de rechtsgrondslag voor de voorgestelde strafvorderlijke maatregelen en de evenredigheid van de voorgestelde sancties. Nederland wijst de in deze regeling voorgestelde minimumstraffen af.

3. Samenvatting voorstel

- *Inhoud voorstel*

De voorgestelde richtlijn vervangt het kaderbesluit 2000/383/JBZ van de Raad tot versterking, door middel van strafrechtelijke en andere sancties, van de bescherming tegen valsemunterij in verband met het in omloop brengen van de euro (PbEG 2000, L 140). De ontwerp-richtlijn beschrijft een reeks van gedragingen die strafbaar moeten worden gesteld, zoals het op bedrieglijke wijze vervaardigen of wijzigen van munt en het bedrieglijk in omloop brengen van valse munt. De omschrijvingen van de strafbaar te stellen gedragingen zijn vrijwel geheel overgenomen van het kaderbesluit. Daarnaast bevat de ontwerp-richtlijn de – ook uit andere EU-instrumenten bekende – bepalingen betreffende de vestiging van strafrechtelijke aansprakelijkheid wegens deelneming aan en poging tot de strafbaar te stellen gedragingen alsmede betreffende de strafbaarheid van rechtspersonen. Ten opzichte van het kaderbesluit zijn in de ontwerp-richtlijn de

te voorziene straffen uitgewerkt, in de vorm van minimumstraffen en bevat het voorschriften betreffende strafvorderlijke bevoegdheden. Zo moet bij strafrechtelijk onderzoek de toepassing van bijzondere opsporingsbevoegdheden mogelijk zijn en wordt een voorschrift voorgesteld op grond waarvan autoriteiten verplicht zijn valse munten in te leveren bij de nationale analysecentra.

- *Impact assessment Commissie*

De Commissie heeft verschillende partijen over de effectiviteit van de strafrechtelijke aanpak van eurovalsemunterij geraadpleegd. Volgens de Commissie kan uit die raadpleging de conclusie worden getrokken dat de strafrechtelijke autoriteiten de euro en andere munten beter moeten kunnen beschermen met behulp van strafrechtelijke maatregelen.

Uit het daaropvolgende impact assessment is volgens de Commissie gebleken dat het de voorkeur heeft die verbetering te realiseren met handhaving van de meeste bepalingen van het kaderbesluit 2000/383/JBZ en door de invoering van minimumstraffen en invoering van een tweetal strafvorderlijke voorzieningen.

4. Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel

a) Bevoegdheid

Het voorstel is gebaseerd op artikel 83, eerste lid, van het VWEU. Dat is de juiste rechtsgrondslag voor zover het gaat om bij richtlijn vast te stellen minimumvoorschriften betreffende de bepaling van strafbare feiten en sancties in verband met de in artikel 83, eerste lid, genoemde vormen van bijzonder zware criminaliteit met een grensoverschrijdende dimensie. De vervalsing van betaalmiddelen wordt als een zodanige vorm van criminaliteit in artikel 83, eerste lid, VWEU genoemd.

Deze rechtsgrondslag biedt evenwel geen ruimte om daarop de in de ontwerp-richtlijn opgenomen strafvorderlijke maatregelen (bijvoorbeeld bijzondere opsporingsbevoegdheden) te baseren. De vraag is of deze maatregelen hun grondslag kunnen vinden in een van de overige leden van de artikelen 82 en 83 van het VWEU. In dat geval zou onderbrenging onder artikel 83, eerste lid, VWEU kunnen worden gerechtvaardigd vanuit de gedachte dat laatstgenoemd artikellid de dominante rechtsgrondslag voor de ontwerp-richtlijn vormt. Voor de voorgestelde strafvorderlijke maatregelen lijkt echter ook in de andere leden van de artikelen 82 en 83 VWEU geen rechtsgrondslag te vinden. Zij beogen namelijk uitsluitend aanpassingen in de nationale strafvorderlijke praktijk zonder dat die aanpassingen in de sleutel staan van de politie en justitiële samenwerking in strafzaken. Nederland is derhalve niet overtuigd dat de strafvorderlijke maatregelen in hun huidige redactie onder de gekozen rechtsgrondslag kunnen worden gebracht.

b) *Subsidiariteits- en proportionaliteitsoordeel*

Subsidiariteit: positief

Proportionaliteit: positief, maar negatief ten aanzien van het voorstel van minimumstraffen.

Subsidiariteit

Ten aanzien van de subsidiariteit is het oordeel positief. Een adequate (internationale) bestrijding van eurovalsemunterij kan niet worden gerealiseerd wanneer de strafbaarstelling van eurovalsemunterij en daarmee verband houdende sancties aan de lidstaten worden overgelaten. Optreden, zoals reeds met het kaderbesluit 2000/383/JBZ ingezet, door de Unie is derhalve gewenst.

Proportionaliteit

Ten aanzien van de proportionaliteit is het oordeel positief, maar ten aanzien van specifiek het voorstel voor minimumstraffen is het oordeel negatief.

Nederland is van mening dat de voorgestelde strafbaarstellingen – die geheel zijn overgenomen uit het kaderbesluit 2000/383/JBZ – een goed kader bieden voor de bestrijding van eurovalsemunterij, maar dat het voorgestelde stelsel van minimumstraffen verder gaat dan nodig is om het beoogde doel van een effectieve strafrechtelijke handhaving van eurovalsemunterij te realiseren. Naast de ontwerp-richtlijn bescherming van de financiële belangen van de Unie (PIF-richtlijn, COM(2012)363) is dit de tweede ontwerp-richtlijn waarin door de Commissie minimumstraffen worden voorgesteld. Daarmee wijkt de Commissie af van de gebruikelijke wijze van afspraken over strafniveaus op Europees niveau, namelijk dat wordt gewerkt met het voorschrijven van minimale maximumstraffen, waarmee wordt bedoeld dat lidstaten een strafbare gedraging met een maximale straf van tenminste een bepaalde hoogte (in geval van geldboetes) of duur (in geval van gevangenisstraf) bedreigt.

De Commissie is blijkens haar impact assessment van oordeel dat het bestaande strafrechtelijke acquis, zoals vervat in het kaderbesluit 2000/383/JBZ, door het ontbreken van toereikende strafminima onvoldoende afschrikwekkend is. Aan de hand van gevallen van valsemunterij die zich hebben voorgedaan in lidstaten waar toereikende strafminima ontbreken, wordt betoogd dat die lidstaten daardoor aantrekkelijk zijn als toevluchtsoord voor valsemunters. Bij deze analyse is evenwel niet betrokken welke straffen daadwerkelijk in die landen worden opgelegd. Daarnaast zou het ontbreken van toereikende strafminima volgens de Commissie duiden op een lage opsporingsprioriteit, hetgeen ook de internationale samenwerking bemoeilijkt. Nederland meent dat ook deze stellingname niet overtuigend wordt onderbouwd. Als er al een verband tussen een opsporingsprioriteit en de hoogte van sancties zou bestaan, ligt niet een koppeling van de opsporingsprioriteiten aan de hoogte van de strafminima voor de hand maar juist aan de strafmaxima. Het strafmaximum brengt immers de ernst van het feit tot uitdrukking.

Nederland wijst het voorstel voor minimumstraffen af. Nederland wil bij de harmonisatie van straffen blijven werken met de gebruikelijke systematiek van minimale maximumstraffen (een maximumstraf van ten minste een bepaalde duur), zoals ook door de Raad tot uitgangspunt is genomen in de Raadsconclusies ter zake de te volgen methode voor de harmonisatie van straffen uit 2002.

- c) *Nederlands oordeel over de voorstellen op het gebied van gedelegeerde en/of uitvoeringshandelingen: n.v.t.*

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

- a) *Consequenties EU-begroting: geen*

- b) *Financiële consequenties (incl. personele) voor rijksoverheid en/ of decentrale overheden*

De voorgestelde strafbaarstellingen betreffende valsemunterij zullen op zichzelf geen financiële consequenties hebben. Mogelijke financiële gevolgen, worden opgevangen binnen de begrotingen van de beleidsverantwoordelijke departementen.

- c) *Financiële consequenties (incl. personele) voor bedrijfsleven en burger: geen*

- d) *Gevolgen voor regeldruk/administratieve lasten voor rijksoverheid, decentrale overheden, bedrijfsleven en burger: geen*

6. Implicaties juridisch

- a) *Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)*

Vooralsnog kan naar het oordeel van het kabinet ter implementatie van de ontwerp-richtlijn worden volstaan met de bestaande strafbaarstellingen in het Wetboek van Strafrecht, zoals aangepast ter uitvoering van het kaderbesluit 2000/383/JBZ. Het betreft de artikelen 208 tot en met 215 van het Wetboek van Strafrecht.

- b) *Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en beschikkingen) met commentaar t.a.v. haalbaarheid*

Het voorstel stelt een implementatietermijn voor van achttien maanden na vaststelling van de richtlijn. Nederland is – om precedentwerking op dit terrein te voorkomen – van mening dat deze termijn te kort is. Nederland beijvert zich consequent voor het gebruik van realistische implementatietermijnen en zet met betrekking tot het onderhavige voorstel in op een implementatietermijn van ten minste twee jaar.

c) *Wenselijkheid evaluatie-/horizonbepaling*

Het voorstel bevat een evaluatiebepaling. Uiterlijk vijf jaar na inwerkingtreding van de richtlijn dient de Commissie verslag uit te brengen aan het Europees Parlement en de Raad over de toepassing van de richtlijn. Nederland kan met deze bepaling instemmen.

7. Implicaties voor uitvoering en handhaving

a) *Uitvoerbaarheid*

Er worden geen problemen met betrekking tot de uitvoerbaarheid verwacht.

b) *Handhaafbaarheid*

De in de richtlijn voorgestelde strafbaarstellingen dienen eenduidig te zijn geformuleerd en afgebakend, opdat de doelstelling van een effectieve handhaving, waarbij samenwerking met andere lidstaten nodig kan zijn, kan worden bereikt.

8. Implicaties voor ontwikkelingslanden: geen

9. Nederlandse positie

Met de Commissie is Nederland van mening dat de lidstaten op dezelfde manier strafrechtelijk tegen valsemunterij moeten optreden en dat valsemunters in vergelijkbare situaties vergelijkbare sancties moeten worden opgelegd. De omzetting van het strafrechtelijk acquis van het kaderbesluit 2000/383/JBZ in een richtlijn kan tegen die achtergrond worden onderschreven.

Nederland wijst evenwel het in deze regeling voorgestelde stelsel van minimumstraffen voor eurovalsemunterij af. Nederland wil bij de harmonisatie van straffen blijven werken met de gebruikelijke systematiek van minimale maximumstraffen (een maximumstraf van ten minste een bepaalde duur). Op dit punt kan het bestaande strafrechtelijke acquis ter bestrijding van eurovalsemunterij worden aangevuld en heeft de ontwerp-richtlijn een toegevoegde waarde ten opzichte van het kaderbesluit 2000/383/JBZ. Voorts is Nederland van mening dat bij de rechtsgrondslag voor de in de richtlijn opgenomen aanvullende maatregelen van strafvorderlijke aard in hun huidige vorm nadrukkelijk vraagtekens kunnen worden gesteld omdat zij niet in de sleutel zijn geplaatst van justitiële samenwerking in strafzaken tussen de lidstaten. Het gaat onder meer om een voorschrift op grond waarvan ter bestrijding van eurovalsemunterij de toepassing van bijzondere opsporingsbevoegdheden mogelijk moet zijn.

Fiche 3: Richtlijn netwerk- en informatiebeveiliging

1. Algemene gegevens

Titel voorstel

Voorstel voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen.

Datum ontvangst Commissiedocument

7 februari 2013

Nr. Commissiedocument

COM(2013)48

Prelex

http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=nl&DosId=202368

Nr. Impact Assessment Commissie en Opinie Impact Assessment Board

IA:SWD(2013)32, <http://eur->

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013SC0032:EN:NOT](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013SC0032:EN:NOT)

IAB: http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2013/sec_2013_0098_en.pdf

Behandelingstraject Raad

JBZ-Raad

Eerstverantwoordelijk ministerie

Ministerie van Veiligheid en Justitie

Rechtsbasis, besluitvormingsprocedure Raad, rol Europees Parlement, gedelegeerde en/of uitvoeringshandelingen

a) Rechtsbasis

Artikel 114 Verdrag betreffende de werking van de Europese Unie

b) Besluitvormingsprocedure Raad en rol Europees Parlement

Gewone wetgevingsprocedure: gekwalificeerde meerderheid binnen de Raad en medebeslissing van het Europees Parlement (commissie Interne markt en consumentenbescherming)

c) Gedelegeerde en/of uitvoeringshandelingen

Het voorstel kent diverse bepalingen waarin aan de Commissie de bevoegdheid wordt toegekend om gedelegeerde handelingen of uitvoeringshandelingen vast te stellen. Zo geeft art. 9(2) de Commissie de bevoegdheid gedelegeerde handelingen vast te stellen m.b.t. de bepaling van de criteria die een lidstaat moet nakomen om aan het beveiligde informatie-uitwisselingsnetwerk te mogen deelnemen. Op grond van art. 9(3) krijgt de Commissie de bevoegdheid door middel van uitvoeringshandelingen besluiten te nemen inzake de toegang van de lidstaten tot de beveiligde infrastructuur. Deze uitvoeringshandelingen worden vastgesteld aan de hand van de onderzoeksprocedure (met een beslissende stem voor de lidstaten, vertegenwoordigd in het onderzoekscomité). Art.10(5) geeft de Commissie de bevoegdheid gedelegeerde handelingen vast te stellen tot verdere omschrijving van de risico's en incidenten die aanleiding geven tot vroegtijdige waarschuwing binnen het waarschuwingsnetwerk. Art.12 van het voorstel geeft de Commissie de bevoegdheid een NIB-samenwerkingsplan van de Unie vast te stellen. Deze uitvoeringshandelingen worden vastgesteld aan de hand van de onderzoeksprocedure (met een beslissende stem voor de lidstaten, vertegenwoordigd in het onderzoekscomité). Op grond van art. 14(5) heeft de Commissie de bevoegdheid gedelegeerde handelingen vast te stellen m.b.t. de omschrijving van de omstandigheden waarin overheden en marktdeelnemers incidenten moeten melden. Art. 14(7) van het voorstel is vooralsnog onduidelijk. Dit artikel lijkt abusievelijk te spreken van een combinatie van gedelegeerde en uitvoeringshandelingen tot vaststelling van de formaten en procedures voor de toepassing van art. 14(2) van het voorstel (dat lidstaten opdraagt ervoor te zorgen dat overheden en marktdeelnemers incidenten, met een aanzienlijke impact op de beveiliging van de door hen verleende kerndiensten, aan de bevoegde autoriteiten melden).

2. Samenvatting BNC-fiche

- *Korte inhoud voorstel*

Doel van de voorgestelde richtlijn is het waarborgen van een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging (NIB). Dit niveau verschilt momenteel per lidstaat. Dit leidt tot een sterk wisselend niveau van paraatheid bij incidenten en een ongelijk niveau van bescherming van consumenten en bedrijven. De Europese Commissie wil de beveiliging van het internet en de particuliere netwerken en informatiesystemen verbeteren door de lidstaten ertoe te verplichten hun paraatheid te verbeteren, beter met elkaar samen te werken en door vitale partijen (banken, energiebedrijven, vervoersbedrijven, gezondheidszorg, internetdiensten, overheden) te verplichten adequate maatregelen te nemen om beveiligingsrisico's te beheren en ernstige incidenten aan de nationale bevoegde autoriteiten te rapporteren. Het voorstel verplicht lidstaten te beschikken over een nationale NIB-strategie, een NIB-samenwerkingsplan, een instantie belast met de coördinatie van NIB-zaken en een goed functionerend *Computer Emergency Response Team* (CERT) (zie art. 5 t/m 7).

- *Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel*

De Europese Commissie baseert de bevoegdheid van de EU op artikel 114 VWEU.

Nederland beschouwt de subsidiariteit en de proportionaliteit van het voorstel positief, met kanttekeningen ten aanzien van met name de privacy-aspecten bij het uitwisselen van gegevens bij cyberincidenten, de nalevingskosten van het voorstel en de geringe mate waarin het voorstel aansluit bij bestaande nationale en internationale structuren.

- *Implicaties/risico's/kansen*

Aanzienlijke toename regeldruk (administratieve lasten en nalevingskosten)

- *Nederlandse positie*

Nederland is het eens met de constatering van de Commissie dat op basis van vrijwillig aangegane verplichtingen veel is bereikt, maar dat er in de EU nog steeds lacunes zijn, met name op het gebied van nationale capaciteit, coördinatie bij grensoverschrijdende incidenten en de betrokkenheid en paraatheid van de private sector. Het voorstel verplicht de lidstaten om nationale instanties aan te wijzen die voor NIB bevoegd zijn, om een goed functionerend CERT op te richten en om een nationale strategie en nationaal samenwerkingsplan inzake NIB vast te stellen. Nederland heeft zelf nationaal reeds veel onderdelen van het voorstel gerealiseerd. Derhalve kan Nederland het voorstel in grote lijnen ondersteunen. Nederland is voorstander van een sterke CERT-gemeenschap in de EU. Daarnaast hecht Nederland veel waarde aan de publiek-private samenwerking.

Nederland heeft bij het voorstel wel een aantal aandachtspunten. Nederland pleit voor behoud van reeds bestaande structuren, zowel op nationaal, internationaal als op Europees niveau. Daarnaast dient de uitwerking plaats te vinden binnen de kaders van het Verdrag van de Europese Unie op het terrein van nationale veiligheid, hier ligt de verantwoordelijkheid bij de lidstaten zelf. Tevens dienen de lidstaten zelf invulling te kunnen geven hoe op nationaal niveau wordt samengewerkt tussen betrokken sectoren. Nederland is van mening dat mede door dit voorstel de fragmentatie op het gebied van meld- en zorgplichten verder toe dreigt te nemen, doordat de voorgestelde richtlijn stelt dat de verplichtingen niet van toepassing zijn op aanbieders van openbare communicatienetwerken of openbare elektronische communicatiediensten in de zin van Richtlijn 2002/21/EG. Nederland constateert tenslotte afwijkingen met de Nederlandse situatie zoals het begrip "incident", de reikwijdte en bevoegdheden van de voorgestelde bevoegde autoriteit en het benoemen van vitale partijen die verschilt met de Nederlandse lijst van vitale partijen.

3. Samenvatting voorstel

- *Inhoud voorstel*

Doel van de voorgestelde richtlijn is het waarborgen van een hoog gemeenschappelijk niveau van NIB. Momenteel is de bestaande capaciteit van netwerk- en informatiebeveiliging per lidstaat verschillend. Dit leidt tot een sterk wisselend niveau van paraatheid bij incidenten en een ongelijk niveau van bescherming van consumenten en bedrijven.

Deze fragmentatie leidt er mede toe dat informatie over dreigingen en incidenten niet uitgewisseld wordt. Een andere reden voor gebrekkige uitwisseling komt door het ontbreken van voldoende vertrouwen.

De Commissie wil dat de beveiliging van het internet en de particuliere netwerken en informatiesystemen die de werking van onze samenleving en economie ondersteunen, wordt verbeterd. De Commissie wil dit bereiken door de lidstaten ertoe te verplichten hun paraatheid te verbeteren en beter met elkaar samen te werken, en door zowel exploitanten van kritieke infrastructuur als essentiële aanbieders van informatiemaatschappijdiensten en overheden (banken, energiebedrijven, vervoersbedrijven, gezondheidszorg, internetdiensten) ertoe te verplichten adequate maatregelen te nemen om beveiligingsrisico's te beheren en ernstige incidenten aan de nationale bevoegde autoriteiten te rapporteren. Het voorstel verplicht lidstaten te beschikken over een nationale NIB-strategie, een NIB-samenwerkingsplan, een instantie belast met de coördinatie van NIB-zaken en een goed functionerende Computer Emergency Response Team (CERT).

- *Impact assessment Commissie*

De Commissie constateert dat het gemeenschappelijk niveau van netwerk- en informatiebeveiliging binnen de EU onvoldoende is. Momenteel is de bestaande capaciteit van netwerk- en informatiebeveiliging per lidstaat verschillend. Dit leidt tot een sterk wisselend niveau van paraatheid bij incidenten en een ongelijk niveau van bescherming van consumenten en bedrijven.

Beveiligingsincidenten ondermijnen het goed functioneren van de interne markt, bovendien kunnen dergelijke incidenten nationale grenzen overstijgen. De oorzaak is een ongelijk niveau van expertise in de lidstaten en onvoldoende uitwisseling van informatie over incidenten, risico's en dreigingen. Hiertoe stelt de Commissie 3 opties voor: 1) bestaande praktijk (lidstaten nemen beveiligingsmaatregelen op basis van vrijwilligheid), 2) de regulerende aanpak (lidstaten dienen te voldoen aan minimum vereisten en dienen verplicht samen te werken op EU niveau) of 3) een gemengde aanpak (lidstaten nemen beveiligingsmaatregelen op basis van vrijwilligheid, waarbij regulering geldt voor vitale partijen en overheidsinstellingen). De Commissie pleit voor optie 2.

De *impact assessment board* stelt in haar advies dat goede argumentatie voor het opleggen van wettelijke verplichtingen rondom rapportages, risico management en verplichte samenwerking aan publiek en private instellingen (incl. MKB) ontbreekt. Nederland zal de Europese Commissie dan ook vragen om een nadere onderbouwing van de raming en reikwijdte van de kosten die bedrijven zullen moeten maken.

4. Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel

a) Bevoegdheid

De Commissie baseert de bevoegdheid van de EU op artikel 114 VWEU. Het kabinet is van mening dat artikel 114 VWEU een grondslag biedt om maatregelen te nemen inzake de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die de instelling en de werking van de interne markt betreffen. De algemene richtlijn ter bescherming van kritieke infrastructuren

(2011/0461 (COD)) echter heeft een andere rechtsbasis, namelijk artikel 308 EG (oud), thans 352 VWEU. Het kabinet ziet dus graag nadere toelichting op dit verschil.

b) Subsidiariteits- en proportionaliteitsoordeel

Nederland beschouwt de subsidiariteit van het voorstel positief. Nederland is van mening dat de voorgestelde maatregelen op het gebied van cyberbeveiliging over het algemeen beter in EU-verband dan op nationaal niveau bereikt kunnen worden. Een Europese aanpak is een effectieve manier om tussen alle lidstaten een gelijkwaardig niveau van cyberbeveiliging te realiseren waardoor het mogelijk wordt om betrouwbaar, effectief en tijdig informatie uit te wisselen over incidenten en dreigingen. Het voorstel sluit ook aan bij de nationale inspanningen op het gebied van cyberbeveiliging. Er is op basis van vrijwillige verplichtingen veel bereikt. Zo vindt dagelijks tussen sommige lidstaten afstemming plaats over cyberincidenten en -kwetsbaarheden. Er zijn echter in de EU nog steeds lacunes, met name op het gebied van nationale cyberbeveiligingscapaciteiten, formalisering van taken, bevoegdheden en coördinatie bij grensoverschrijdende incidenten die een crisissituatie kunnen opleveren en de betrokkenheid en paraatheid van de private sector. Nederland is wel van mening dat een aantal van de voorgestelde maatregelen in de Richtlijn net zo goed op niveau van de lidstaten kunnen worden geregeld. Van belang is dat bestaande nationale en internationale structuren zoals bijvoorbeeld de European Government CERT's (EGC) benoemd, erkend en in stand blijven en niet gedupliceerd worden.

Het oordeel over de proportionaliteit van de voorgestelde acties is positief met kanttekeningen. De verplichtingen die worden opgelegd aan lidstaten, marktpartijen en publieke overheden gaan niet verder dan nodig is om het beoogde gelijkwaardige niveau van cyberbeveiliging te bereiken en gaten in het juridische raamwerk te dichten. Het is goed dat de lidstaten verplicht worden om nationale instanties aan te wijzen die voor NIB bevoegd zijn, om een goed functionerend CERT op te richten en om een nationale strategie en nationaal samenwerkingsplan inzake NIB vast te stellen. Nederland heeft reeds veel van deze voorgenomen verplichtingen gerealiseerd, zo heeft Nederland reeds een strategie, een goed functionerend CERT, worden periodiek cyberdreigingsbeelden opgesteld en is een cybersecurity coördinator aangesteld.

Wel heeft Nederland kanttekeningen ten aanzien van de reikwijdte van de richtlijn en de wijze waarop de voorgestelde verplichtingen worden ingevuld. Daarnaast plaatst Nederland kritische kanttekeningen bij het voorstel met betrekking tot de privacy en andere vertrouwelijkheidsaspecten bij het uitwisselen van gegevens bij cyberincidenten. Voorkomen dient te worden dat in vertrouwen verstrekte gegevens door instanties worden doorgestuurd naar derden of onvoldoende beveiligd zijn.

Verder is Nederland kritisch ten aanzien van de nalevingskosten van het voorstel en het feit dat het voorstel in onvoldoende mate aansluit bij bestaande nationale en internationale structuren.

c) Nederlands oordeel over de voorstellen op het gebied van gedelegeerde en/of uitvoeringshandelingen

Nederland staat over het algemeen positief tegenover het voorstel van de Commissie om aan de Commissie de bevoegdheid te verlenen om gedelegeerde of uitvoeringshandelingen vast te stellen ter nadere uitwerking van de richtlijn. De bepalingen in het voorstel over bevoegdheidsdelegatie en uitvoering zijn vrijwel alle niet controversieel voor Nederland. Nederland is echter negatief ten aanzien van de mogelijkheid die artikel 10(5) van het voorstel biedt, nl. dat de Commissie - d.m.v. gedelegeerde handelingen - een nadere omschrijving kan geven van de risico's en incidenten die aanleiding geven tot vroegtijdige waarschuwing binnen het waarschuwingsnetwerk. Nederland wil dat de Commissie deze nadere omschrijving door middel van een uitvoeringshandeling vaststelt. De keuze voor bevoegdheidsdelegatie, in plaats van uitvoering, in art. 10(5) van het voorstel verhoudt zich naar de mening van Nederland niet met art. 12(2) onder (a) (tweede gedachtestreepje) van het voorstel. Dit artikel geeft de Commissie de bevoegdheid om d.m.v. *uitvoeringshandelingen* de criteria te bepalen voor de beoordeling van de risico's en incidenten door het samenwerkingsnetwerk. Nederland plaatst tevens vraagtekens bij art. 14(7) van het voorstel dat een combinatie bevat van gedelegeerde en uitvoeringshandelingen die zich niet tot elkaar verhoudt en die niet past binnen het Verdragsrechtelijke kader van art. 290 en 291 VWEU.

Nederland is voorstander van een meldplicht ingericht volgens onze criteria. Hierbij stelt Nederland strikte eisen ten aanzien van bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens. Voorkomen dient te worden dat vertrouwelijk verstrekte gegevens doorgestuurd worden naar derden.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) Consequenties EU-begroting

De Commissie stelt dat zowel de samenwerking als de uitwisseling van informatie tussen de lidstaten moet worden ondersteund door een beveiligde infrastructuur. Dit voorstel zal volgens de Commissie slechts gevolgen voor de begroting hebben indien de lidstaten opteren voor de aanpassing van een bestaande infrastructuur en zij de Commissie opdragen dit ten uitvoer te leggen binnen het meerjarig financieel kader voor de periode 2014-2020. De eenmalige kosten worden geraamd op € 1.250.000,- en zouden ten laste van de EU-begroting komen (CEF budget).

b) Financiële consequenties (incl. personeel) voor rijksoverheid en/ of decentrale overheden

In het voorstel worden 3 opties voorgesteld: 1) bestaande praktijk (lidstaten nemen beveiligingsmaatregelen op basis van vrijwilligheid), 2) de regulerende aanpak (lidstaten dienen te voldoen aan minimum vereisten en dienen verplicht samen te werken op EU niveau) of 3) een gemengde aanpak (lidstaten nemen beveiligingsmaatregelen op basis van vrijwilligheid, waarbij regulering geldt voor vitale partijen en overheidsinstellingen).

Bij optie 1) zijn de financiële gevolgen voor Nederland minimaal. Immers, het huidige beleid en investeringen kunnen ongewijzigd gecontinueerd worden. De keuze voor optie 2) zal de grootste financiële consequenties hebben voor Nederland. Bij deze optie worden lidstaten verplicht maatregelen te nemen in overeenstemming met het voorstel. Nederland voldoet reeds aan veel van de gevraagde maatregelen en verwacht dat de nalevingskosten voor Nederland beperkt zullen zijn. Nederland zal hier in de onderhandelingen kritisch op zijn. De kosten blijven relatief laag. Verwachte kosten liggen voornamelijk bij de verruimde taak van het NCSC (die de door de Commissie bedoelde CERT-functie herbergt). Deze zal ondermeer 24/7 bemenst moeten worden en de systemen dienen volledig redundant te zijn. Bovendien zal volgens het voorstel een autoriteit worden aangewezen die over technische en financiële middelen beschikt en uitvoerings- en handhavingstaken krijgt. Bij keuze voor de derde optie zullen de kosten voornamelijk liggen bij vitale partijen en overheidsinstellingen. Hiervoor geldt eveneens dat Nederland reeds in grote mate voldoet aan de voorgestelde verplichtingen. Nederland zal zijn keuze laten afhangen van een nadere onderbouwing door de Europese Commissie van de raming en reikwijdte van de kosten die bedrijven en de overheid zullen moeten maken. Bij alle opties geldt dat de budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

c) Financiële consequenties (incl. personele) voor bedrijfsleven en burger

De Commissie komt tot de slotsom dat de kosten voor de particuliere sector binnen de perken blijven aangezien veel betrokken organisaties verondersteld worden reeds aan de bestaande beveiligingseisen te voldoen. De dwingende verplichtingen in het voorstel kunnen sterke effecten hebben op het gekozen publiek-private samenwerkingsmodel in Nederland.

d) Gevolgen voor regeldruk/administratieve lasten voor rijksoverheid, decentrale overheden, bedrijfsleven en burger

(Mede)-overheden worden volgens het voorstel verplicht om de nationale autoriteit informatie te verschaffen die nodig is om de beveiliging van hun netwerken en informatiesystemen te beoordelen, met inbegrip van gedocumenteerde beleidsmaatregelen op het gebied van beveiliging. De hoogte van deze lasten zijn nog niet nader bekend.

Volgens de *Impact Assessment* bedragen de totale additionele kosten in de EU om te voldoen aan het voorstel tussen de 1 en 2 miljard euro. Nederland zal de Europese Commissie vragen om een nadere onderbouwing van de raming en reikwijdte van de kosten die bedrijven en overheden, per lidstaat zullen moeten maken.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

Momenteel wordt door het ministerie van V&J ontwerp-wetgeving voorbereid, die strekt tot de regeling van een meldplicht voor de overheid en private bedrijven in randvoorwaardelijke sectoren (drinkwater,

energie, etc.) van cyberincidenten met een potentieel maatschappelijk ontwrichtende werking. Afhankelijk van de uiteindelijke tekst van de richtlijn zal moeten worden gezien of en in welke mate deze nationale (ontwerp-)wetgeving hiermee in overeenstemming is.

b) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en beschikkingen) met commentaar t.a.v. haalbaarheid

De door de Europese Commissie voorgestelde termijn van achttien maanden is voor Nederland haalbaar. Nederland heeft reeds veel onderdelen van het voorstel gerealiseerd.

c) Wenselijkheid evaluatie-/horizonbepaling

De Commissie evalueert de werking van deze richtlijn en brengt verslag uit aan het Europees Parlement en de Raad. Het eerste verslag wordt uiterlijk drie jaar na de in artikel 21 bedoelde omzettingsdatum ingediend. Daartoe kan de Commissie de lidstaten verzoeken onverwijld informatie te verstrekken.

7. Implicaties voor uitvoering en handhaving

a) Uitvoerbaarheid

Het voorstel is uitvoerbaar en er zijn geen bijzondere implicaties voor de uitvoering voorzien.

b) Handhaafbaarheid

Het voorstel is handhaafbaar en er zijn geen bijzondere implicaties voor de handhaving voorzien. Momenteel is de handhaving in Nederland sectoraal geregeld. Onduidelijk is hoe de situatie zal worden met de eventuele komst van een "bevoegde autoriteit". Nederland hecht eraan om vast te houden aan de bestaande structuur van sectorale bevoegdheden en verantwoordelijkheden waarbij wel de bewustwording van bestuurders vergroot dient te worden, verplichte zelfregulering ingevoerd moet worden en een goede samenwerking bewerkstelligd dient te worden.

8. Implicaties voor ontwikkelingslanden

Geen

9. Nederlandse positie

Nederland is het eens met de constatering van de Commissie dat op basis van vrijwillige verplichtingen veel is bereikt, maar dat er in de EU nog steeds lacunes zijn, met name op het gebied van nationale capaciteit, coördinatie bij grensoverschrijdende incidenten en de betrokkenheid en paraatheid van de private sector. Het voorstel verplicht de lidstaten om nationale instanties aan te wijzen die voor NIB bevoegd zijn, om een goed functionerend CERT op te richten en om een nationale strategie en nationaal samenwerkingsplan inzake NIB vast te stellen. Nederland heeft reeds veel van deze voorgenomen verplichtingen gerealiseerd. De Nederlandse Nationale Cybersecurity Strategie regelt veel onderwerpen die de Commissie in haar voorstel wil regelen. Zo heeft Nederland reeds een strategie, een goed functionerende CERT (ondergebracht bij het NCSC), worden periodiek

cyberdreigingsbeelden opgesteld en is een cybersecurity coördinator aangesteld. Derhalve kan Nederland het voorstel in grote lijnen ondersteunen. Het voorstel biedt lidstaten handvatten om de eigen cyberbeveiliging naar een hoger niveau te brengen. Nederland hecht veel waarde aan de publiek-private samenwerking. Aangezien het overgrote deel van de netwerk- en informatiesystemen eigendom is van de private sector en door deze sector wordt geëxploiteerd, is het van essentieel belang dat de private sector meer wordt betrokken bij het bevorderen van cyberbeveiliging. De private sector dient eigen technische capaciteiten en opleidingen op het gebied van weerbaarheid in cyberspace te ontwikkelen en *best practices* binnen alle branches te delen. Een *top-down* benadering van gedetailleerde verplichtingen is hierbij niet effectief.

Nederland is eveneens voorstander van een sterke CERT gemeenschap in de EU. Door een gelijkwaardig niveau tussen lidstaten van cyberbeveiliging te creëren wordt het mogelijk om betrouwbaar, effectief en tijdig informatie uit te wisselen over incidenten en dreigingen. Onderzoek naar en het creëren van randvoorwaarden voor versterking van EU-breed crisismanagement op het gebied van ICT-veiligheid (al dan niet via de CERT-structuren) is gewenst.

Wel gaat het voorstel van de Commissie op sommige onderdelen verder of juist minder ver dan de Nederlandse situatie. Nederland pleit voor behoud van reeds bestaande structuren, zowel op nationaal als op Europees niveau waarbij eveneens aansluiting wordt gezocht bij bestaande, geaccepteerde standaarden (zoals bijvoorbeeld ISO 27001/27002). Hierbij zou ruimte moeten bestaan om accenten te leggen die meer in overeenstemming zijn met de nationale bestuurscultuur. Nederland is tegen opgelegde verplichtingen vanuit de EU die raken aan de nationale veiligheid en dus aan nationale bevoegdheden. Ook moeten lidstaten zelf kunnen bepalen hoe op nationaal niveau wordt samengewerkt tussen betrokken partijen.

Daarnaast plaatst Nederland kritische kanttekeningen bij het voorstel met betrekking tot de privacy en andere vertrouwelijkheidsaspecten bij het uitwisselen van gegevens bij cyberincidenten. Voorkomen dient te worden dat in vertrouwen verstrekte gegevens door instanties worden doorgestuurd naar derden of onvoldoende beveiligd zijn.

Nederland is van mening dat mede door dit voorstel de fragmentatie op het gebied van meld- en zorgplichten verder dreigt toe te nemen. Het is van belang dat het overzicht wordt bewaard en een eenduidige lijn wordt gehanteerd. De voorgestelde richtlijn stelt namelijk dat de verplichtingen niet van toepassing zijn op aanbieders van openbare communicatienetwerken of openbare elektronische communicatiediensten in de zin van Richtlijn 2002/21/EG. Deze partijen zijn onderworpen aan artikel 13 bis van genoemde Richtlijn. Bij nadere lezing blijkt dat de meldplicht in richtlijn 2002/21/EG anders is geformuleerd dan de meldplicht in voorgestelde richtlijn.

Daarnaast werkt Nederland al aan de invoering van een meldplicht voor veiligheidslekken die zowel qua beschrijving als scope afwijkt van het voorstel van de Commissie. Zo introduceert de Commissie het begrip "bevoegde autoriteit". Onduidelijk is hoe deze bevoegde autoriteit zich verhoudt tot de sectorale toezichthouders. Uit het voorstel kan worden opgemaakt dat in Nederland het NCSC bedoeld wordt, echter het voorstel verplicht de lidstaten om de bevoegde autoriteit uitvoerende en

toezichhoudende bevoegdheden toe te kennen, zowel ten opzichte van marktdeelnemers als ten opzichte van overheidspartijen. Deze bevoegdheden zijn in Nederland bewust niet aan het NCSC toegekend, maar gekoppeld aan sectorale toezichthouders. Het kabinet heeft gekozen voor zo min mogelijk interbestuurlijk toezicht. Nederland hecht eraan om vast te houden aan de bestaande structuur van sectorale bevoegdheden en verantwoordelijkheden waarbij wel de bewustwording van bestuurders vergroot dient te worden, verplichte zelfregulering ingevoerd moet worden en een goede samenwerking bewerkstelligd wordt.

Verder benoemt het voorstel in de Annex een aantal vitale partijen waarvan in een aantal gevallen niet helder is waarom die partijen als vitaal worden beschouwd. Bijvoorbeeld internetdienstverleners als zoekmachines en *application stores*. Daarnaast komt deze opsomming niet overeen met de vitale partijen zoals deze in Nederland zijn benoemd. Zo benoemt het voorstel zorginstellingen als ziekenhuizen en privéklinieken tot vitale partij, terwijl deze categorie in Nederland niet als vitale partij wordt aangemerkt. Daarnaast benoemt Nederland de drinkwatersector en het keren en beheren van oppervlaktewateren als vitale sector waar het voorstel deze sector niet benoemt. Tot slot is de energiesector te breed benoemd, enkel de netwerkbeheerders zijn als vitaal aangemerkt binnen het Nederlandse Nationale Veiligheidsprogramma. Voor andere energiepartijen geldt een hoge mate van redundantie. Hoewel de lijst met vitale partijen opgesomd in het voorstel niet uitputtend is en minimum harmonisatie wordt beoogd, is Nederland van mening dat het voorstel een basislijst moet benoemen van vitale partijen waar een aanzienlijke impact is te verwachten indien deze uitvallen. Deze lijst zou dan minder vitale partijen bevatten dan het voorstel momenteel beschrijft. Deze basislijst zou vervolgens door lidstaten uitgebreid dienen te worden met voor betreffende lidstaat relevante vitale partij. Nederland kijkt kritisch naar de voorgestelde bevoegdheden van de Commissie om middels gedelegeerde handelingen de risico's en incidenten die aanleiding geven tot vroegtijdige waarschuwing binnen het waarschuwingsnetwerk nader te specificeren. Hierbij wordt opgemerkt dat het voorstel geen onderscheid maakt tussen crisis en incident. Deze begrippen dienen verduidelijkt te worden.

Tot slot, wat betreft de financiële gevolgen, zal Nederland tijdens de onderhandelingen kritisch zijn op de nalevingskosten voor Nederland. Nederland voldoet overigens reeds aan veel van de gevraagde maatregelen en verwacht dat de nalevingskosten voor Nederland beperkt zullen zijn. Volgens de Impact Assessment bedragen de totale additionele kosten in de EU om te voldoen aan het voorstel tussen de 1 en 2 miljard euro. Nederland zal de Europese Commissie vragen om een nadere onderbouwing van de raming en reikwijdte van de kosten die bedrijven en overheden, per lidstaat, zullen moeten maken

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 cyberbeveiliging 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 cyberbeveiligingsstrategie 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 voorgenen 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 voorgenen 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 gezien. 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)

Fiche 5: Verordening veiligheid consumentenproducten

1. Algemene gegevens

Titel voorstel

Verordening van het Europees Parlement en de Raad betreffende de veiligheid van consumentenproducten en tot intrekking van Richtlijn 87/357/EEG van de Raad en Richtlijn 2001/95/EG van de Raad

Datum ontvangst Commissiedocument

13 februari 2013

Nr. Commissiedocument

COM (2013) 78

Prelex

<http://ec.europa.eu/prelex/apcnet.cfm?CL=nl>

Nr. Impact Assessment Commissie en Opinie Impact Assessment Board

http://ec.europa.eu/governance/impact/ia_carried_out/cia_2013_en.htm

SWD (2013) 33 final/2

http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2013/swd_2013_0033_en.pdf

SWD (2013) 34 final

http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2013/swd_2013_0034_en.pdf

SEC (2013)99

http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2013/sec_2013_0099_en.pdf

Behandelingstraject Raad

Raad Concurrentievermogen

Eerstverantwoordelijk ministerie

Ministerie van Volksgezondheid, welzijn en Sport

Rechtsbasis, besluitvormingsprocedure Raad, rol Europees Parlement, gedelegeerde en/of uitvoeringshandelingen

a) Rechtsbasis

De rechtsbasis van de verordening is artikel 114 VWEU.

b) *Besluitvormingsprocedure Raad en rol Europees Parlement*

Voor de verordening geldt de gewone wetgevingsprocedure. De commissie voor de interne markt en consumentenbescherming (IMCO) van het Europees parlement zal dit dossier behandelen.

c) *Gedelegeerde en/of uitvoeringshandelingen*

De commissie heeft onder voorwaarden de bevoegdheid fabrikanten, importeurs en distributeurs vrijstelling te verlenen van bepaalde verplichtingen om markttoezichtautoriteiten in te lichten. De situaties waarop vrijstelling van toepassing is worden vastgesteld door middel van uitvoeringshandelingen overeenkomstig de onderzoeksprocedure. [artikel 13.2]

Voor producten met een gering risico heeft de commissie de bevoegdheid om gedelegeerde handelingen vast te stellen om te bepalen welke producten, categorieën of groepen producten ontheffing krijgen van de verplichting om bepaalde informatie aan te brengen op het product zelf.[artikel 13.3]

De commissie kan voor bepaalde producten, categorieën of groepen producten, die een aanzienlijk risico voor de gezondheid en de veiligheid van personen kunnen vormen, van marktdeelnemers eisen een traceerbaarheidssysteem in te stellen of daar bij aan te sluiten en daarvoor bepaalde gegevens te vergaren en op te slaan. De commissie heeft de bevoegdheid gedelegeerde handelingen vast te stellen om te bepalen welke producten, categorieën of groepen producten daarvoor in aanmerking komen en welke gegevens marktdeelnemers moeten vergaren en opslaan.[artikel 15.3].

Onderdeel van het traceerbaarheidssysteem is de plaatsing van een aanduiding op het product, de verpakking of de begeleidende documenten. De commissie kan door middel van uitvoeringshandelingen het type aanduiding en de plaatsing daarvan vaststellen. De uitvoeringshandelingen worden vastgesteld volgens de onderzoeksprocedure. [art. 15.4]

De commissie kan een of meer Europese normalisatieorganisaties verzoeken om een Europese norm op te stellen of een bestaande Europese norm aan te wijzen als zogenaamde geharmoniseerde norm. Naleving van een dergelijke norm levert een vermoeden van overeenstemming met de algemene veiligheidseis van de verordening op. Het verzoek wordt door de commissie vastgesteld door middel van een uitvoeringsbesluit overeenkomstig de onderzoekprocedure [art. 16.1]. In het verzoek worden de essentiële eisen opgenomen waaraan de normen dienen te voldoen.

Wanneer een lidstaat of het Europees parlement van mening is dat een Europese norm [artikel 16] niet voldoet aan de verwachte eisen en aan het algemene veiligheidsvoorschrift, stelt zij daarvan de commissie in kennis. De commissie kan volgens de raadplegingprocedure [art. 17.4] besluiten om de (nog niet gepubliceerde) referenties aan de betrokken Europese norm wel of niet met beperkingen in het *Publicatieblad van de Europese Unie* bekend te maken of zij kan volgens de

onderzoeksprocedure besluiten om de referenties aan de betrokken norm in het *Publicatieblad van de Europese Unie* te handhaven, te handhaven met beperkingen of in te trekken[art.17.5].

2. Samenvatting BNC-fiche

- *Korte inhoud voorstel*

Dit voorstel betreft een verordening voor de veiligheid van consumentenproducten ter vervanging van Richtlijn 2001/95/EG van het Europees Parlement en de Raad inzake algemene productveiligheid.

- *Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel*

Het voorstel is gebaseerd op artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU).

Subsidiariteit: positief

Proportionaliteit: positief met kanttekeningen. Nederland heeft bedenkingen bij een aantal gedelegeerde bevoegdheden in het huidige voorstel, op basis waarvan de Commissie kan bepalen voor welke producten, categorieën en groepen producten marktdeelnemers een traceringsstelsel moeten inrichten. Bovendien is Nederland geen voorstander van het voorstel om het land van oorsprong te vermelden zoals verwoord in artikel 7. Nederland steunt dit niet omdat het zorgt voor lastenverzwaring, meer toezicht vergt en weinig toegevoegde waarde zal hebben. Ook is het niet in de impact assessment meegenomen. De maatregel zou mogelijk kunnen worden beschouwd als een niet-tarifaire handelsbelemmering en is mogelijk in strijd met onze WTO-verplichtingen.

- *Implicaties/risico's/kansen*

Het voorstel bewerkstelligt een verregaande harmonisatie en vereenvoudiging van de bestaande wetgeving voor consumentenproducten voor zowel het bedrijfsleven als voor de rijksoverheid.

- *Nederlandse positie*

Ten algemene staat Nederland positief tegenover het voorstel maar plaatst wel een aantal kanttekeningen. Het onderhavige voorstel bevat maatregelen voor consumenten producten die niet in verticale productrichtlijnen geregeld zijn. Deze voorstellen verschillen op sommige punten met maatregelen die in specifieke productrichtlijnen zijn opgenomen. Nederland zal hier vragen over stellen. Nederland is geen voorstander van de verplichting om het land van oorsprong te vermelden. Ook wil Nederland nog kritisch kijken naar de gedelegeerde handelingen in de artikelen 13.3 en 15.3. Bij artikel 13.3 wenst Nederland nadere informatie over de strekking van het voorstel alvorens een definitief standpunt in te nemen of het overdragen van de bevoegdheden aan de Europese Commissie wenselijk is.

Voor artikel 15.3 wil Nederland nader onderzoeken of in deze gevallen de gedelegeerde handelingen wel wenselijk zijn en niet beter gekozen kan worden voor uitvoeringshandelingen met de onderzoeksprocedure. In het huidige voorstel kan de Commissie namelijk bepalen voor welke

producten, categorieën en groepen producten marktdeelnemers een traceringsstelsel moeten inrichten. Dit heeft vergaande consequenties voor marktdeelnemers.

Verder wil NL de mogelijkheid onderzoeken om de verordening te verbreden tot een verordening die veiligheids- en gezondheidseisen stelt aan alle producten. Dit omdat er signalen zijn dat sommige producten buiten de productveiligheidsregelgeving vallen.

3. Samenvatting voorstel

- *Inhoud voorstel*

Het productveiligheid en markttoezicht pakket bestaat uit een mededeling met daarin een meerjarenplan voor markttoezicht, een rapport over de implementatie van verordening (EC) Nr. 765/2008, een voorstel voor een op zichzelf staande verordening voor markttoezicht en buitengrenscontroles op producten en een voorstel voor een nieuwe verordening voor de veiligheid van consumentenproducten. Dit fiche gaat over de nieuwe verordening voor de veiligheid van consumentenproducten. Voor de verordening voor markttoezicht op producten en een meerjarenplan voor markttoezicht is een apart fiche opgesteld.

Dit voorstel voor een verordening betreffende de veiligheid van Consumentenproducten ter vervanging van Richtlijn 2001/95/EG van het Europees Parlement en de Raad inzake algemene productveiligheid (hierna "de richtlijn algemene productveiligheid" genoemd). Dit voorstel betreft alle consumentengoederen, behalve de onder art. 2 lid 2 genoemde producten, zoals voeding en medische hulpmiddelen. Net als de richtlijn algemene productveiligheid stelt de voorgestelde verordening met het oog op de vereiste veiligheid van consumentenproducten een aantal verplichtingen voor de marktdeelnemers vast en bevat zij bepalingen voor het vaststellen van Europese normen tot naleving van de algemene veiligheidsverplichting.

De toepassing van de voorgestelde verordening en haar wisselwerking met andere EU-wetgeving zullen aanzienlijk worden gestroomlijnd en vereenvoudigd, zonder evenwel afbreuk te doen aan een hoog niveau van bescherming van de gezondheid en de veiligheid van de consument.

Een aantal overlappingen van voorschriften inzake markttoezicht en van verplichtingen van marktdeelnemers uit diverse stukken EU-wetgeving (de richtlijn algemene productveiligheid, Verordening (EG) nr. 765/2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en sectorspecifieke harmonisatiewetgeving van de Unie waarmee ook consumentenproducten worden bestreken) hebben tot verwarring geleid bij de marktdeelnemers en de nationale autoriteiten. Hierdoor wordt de naleving door de marktdeelnemers van hun verplichtingen en de doeltreffendheid van het

markttoezicht in de Unie aanzienlijk gehinderd.

Dit voorstel beoogt klaarheid te scheppen in het regelgevende kader voor consumentenproducten, rekening houdend met de recente ontwikkeling van de wetgeving, zoals het nieuwe, in 2008 goedgekeurde wetgevingskader voor het in de handel brengen van producten (Besluit van raad en EP, 768/2008), de aanpassing van sectorspecifieke harmonisatiewetgeving van de Unie aan dat nieuwe kader (het alignement pakket) en de inwerkingtreding op 1 januari 2013 van een nieuwe verordening betreffende Europese normalisatie.

Goede Europese normen bevorderen de naleving door marktdeelnemers van de algemene veiligheidseis van de verordening en vergemakkelijkt het markttoezicht. Het voorstel beoogt het proces te versnellen waarmee de Commissie de Europese normalisatie instellingen opdracht (mandaat) kan geven om Europese normen op te stellen dan wel bestaande Europese normen te identificeren die voldoen aan de criteria die door de commissie in haar mandaat zijn gedicteerd. Tenslotte introduceert het voorstel een aantal aspecten die zowel door de marktdeelnemers als de toezichthouders moeten worden meegenomen bij de vraag of een product wel of niet veilig is indien geen Europese normen bestaan noch nationale wetgeving van de lidstaat waar het product wordt aangeboden

- *Impact assessment Commissie*

In de impact assessment zijn verschillende beleidsopties om op de interne markt een hoog niveau van bescherming van consumenten en andere gebruikers te bereiken door het aantal producten dat niet aan de eisen voldoet te verminderen. De verschillende opties zijn kwalitatief gescoord op onder andere efficiëntie, effectiviteit en kosten. Niet meegenomen zijn de gevolgen van de vermelding van het land van oorsprong in artikel 7 omdat deze toevoeging pas zeer laat is meegenomen in het voorstel. Volgens het impact assessment kunnen de moeilijkheden met het voldoen aan de productveiligheidseisen door marktdeelnemers en de gefragmenteerde situatie in markttoezicht het beste aangepakt worden door een nieuwe verordening voor productveiligheid voor consumentenproducten en een nieuwe verordening voor markttoezicht met een brede scope.

4. Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel

a) Bevoegdheid

Het voorstel is gebaseerd op artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU), dat de rechtsgrondslag is voor het opzetten en functioneren van de interne markt waarop ook de bestaande richtlijn algemene productveiligheid is vastgesteld. Nederland kan zich daarin vinden.

b) *Subsidiariteits- en proportionaliteitsoordeel*

Subsidiariteit

Positief. Binnen de interne markt, waar de vrijheid van verkeer van producten bestaat, kunnen voorschriften inzake productveiligheid slechts op Unie-niveau doeltreffend worden vastgesteld. Dit is noodzakelijk om een hoog niveau van consumentenbescherming te waarborgen (overeenkomstig artikel 169 VWEU en onder verwijzing naar art. 114 VWEU), en ook om te voorkomen dat de lidstaten afwijkende productvoorschriften vaststellen, wat een versnippering van de interne markt tot gevolg zou hebben.

Proportionaliteit

Positief met kanttekeningen. Het voorstel heeft de vorm van een verordening. Dit is het passende rechtsinstrument, aangezien hierbij duidelijke en gedetailleerde regels worden opgelegd die op uniforme wijze en op hetzelfde tijdstip in de gehele Unie van toepassing worden. Hiermee worden divergerende toepassingen in de lidstaten vermeden, hetgeen tot verschillende niveaus van bescherming van de gezondheid en veiligheid zou leiden en belemmeringen voor de interne markt zou opwerpen. De vervanging van de nationale omzettingsmaatregelen leidt ook tot een ingrijpende vereenvoudiging, aangezien de marktdeelnemers zich bij het verrichten van hun bedrijfsactiviteiten kunnen baseren op één regelgevingskader in plaats van een "lappendeken" van nationale wetgevingen van de lidstaten.

Nederland heeft bedenkingen bij een aantal gedelegeerde bevoegdheden in het huidige voorstel, op basis waarvan de Commissie kan bepalen voor welke producten, categorieën en groepen producten marktdeelnemers een traceringsstelsel moeten inrichten (zie onder 4c). Bovendien is Nederland geen voorstander van het voorstel voor de vermelding van het land van oorsprong zoals verwoord in artikel 7. Nederland steunt dit niet omdat het zorgt voor lastenverzwaring, meer toezicht vergt en weinig toegevoegde waarde zal hebben. Ook is het niet in de impact assessment meegenomen. De maatregel zou mogelijk kunnen worden beschouwd als een niet-tarifaire handelsbelemmering en is mogelijk in strijd met onze WTO-verplichtingen.

c) *Nederlands oordeel over de voorstellen op het gebied van gedelegeerde en/of uitvoeringshandelingen*

Nederland kan zich goed vinden in de uitvoeringshandelingen in het voorstel maar is wel kritisch over de voorgestelde gedelegeerde handelingen [artikel 13.3 en 15.3]. Met betrekking tot artikel 13.3 wenst Nederland nadere informatie over de strekking van het voorstel alvorens een definitief standpunt in te nemen of gedelegeerde handelingen wel wenselijk zijn.

Voor artikel 15.3 wil Nederland nader onderzoeken of in deze gevallen gedelegeerde handelingen wel wenselijk zijn en niet beter gekozen kan worden voor uitvoeringshandelingen met de onderzoeksprocedure. In het huidige voorstel kan de Commissie namelijk bepalen voor welke

producten, categorieën en groepen producten marktdeelnemers een traceringsstelsel moeten inrichten. Dit heeft vergaande consequenties voor marktdeelnemers.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) Consequenties EU-begroting

Het voorstel heeft geen andere gevolgen voor de begroting dan die welke betrekking hebben op de correcte toepassing van de verordening, die als richtlijn algemene productveiligheid reeds deel uitmaakt van de wettelijke verworvenheden van de Unie. De gevolgen voor de EU-begroting (12 mln. 2015-2020) werden reeds geanticipeerd in het consumentenprogramma 2014-2020.

b) Financiële consequenties (incl. personele) voor rijksoverheid en/ of decentrale overheden

Het voorstel bewerkstelligt een verregaande harmonisatie en vereenvoudiging van de bestaande wetgeving voor consumentenproducten voor de rijksoverheid wat tot minder controletaken leidt. Wel heeft het voorstel daadwerkelijke potentiële uitbreidingen van het toezichtgebied. Hierbij gaat het over het nieuwe voorschrift dat het land van oorsprong moet worden aangegeven (en dus gecontroleerd) en ook dat producten die in het kader van dienstverlening worden gebruikt en waaraan de consument direct wordt blootgesteld eveneens onder deze verordening vallen. Dit laatste is een uitbreiding want onder de huidige productveiligheidsrichtlijn vallen slechts producten in het kader van dienstverlening die door de consument zelf kunnen worden gebruikt. Ook de bevoegdheden van de commissie met betrekking tot de traceerbaarheid kunnen tot meer controle taken leiden.

Toename van uitvoerings- en handhavingslasten dient zo veel mogelijk te worden voorkomen. Nederland wenst daarom al voor de aanvaarding van dit voorstel duidelijkheid te krijgen over deze aspecten, zodat de kosten voor de rijksoverheid op voorhand te bepalen zijn.

Nederland is van mening dat de financiële middelen gevonden dienen te worden binnen de bestaande financiële kaders van de EU-begroting. Budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

c) Financiële consequenties (incl. personele) voor bedrijfsleven en burger

Er zijn vooralsnog geen financiële consequenties voor de burger. De vereenvoudiging en stroomlijning van de wetgeving zorgt voor lagere kosten voor het bedrijfsleven. Uitbreidingen in het voorstel zoals de traceringsverplichtingen en de verplichting om het land van oorsprong te vermelden kunnen in potentie leiden tot een lastenverzwaring voor het bedrijfsleven.

d) *Gevolgen voor regeldruk/administratieve lasten voor rijksoverheid, decentrale overheden, bedrijfsleven en burger*

Het voorstel heeft vooralsnog geen gevolgen voor regeldruk/administratieve lasten voor de Rijksoverheid. Wel kunnen de bevoegdheden van de Commissie inzake de traceringsverplichtingen leiden tot meer lasten voor het bedrijfsleven omdat ze een elektronisch systeem moeten opzetten. Ook kan de verplichting om het land van oorsprong te vermelden leiden tot meer lasten voor het bedrijfsleven. Daar staat tegenover een vermindering van de lasten vanwege de mogelijkheid het bedrijfsleven in bepaalde situaties vrij te stellen van de informatieplicht/melding van informatie over bepaalde productgroepen en de vereenvoudiging en stroomlijning van de wetgeving. Nederland zal zich tijdens de onderhandelingen inzetten om de administratieve lasten die uit het voorstel voortkomen zo beperkt mogelijk te houden, zonder afbreuk te doen aan de doeltreffendheid van de maatregelen. Nederland zal daartoe oproepen aandacht te hebben voor de lastenlichte variant van de voorgestelde maatregelen, met extra aandacht voor de nalevingkosten die voortkomen uit de maatregelen.

6. Implicaties juridisch

a) *Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)*

Het voorstel leidt tot aanpassing van de Warenwet. Het voorstel bevat een verplichting voor de lidstaten om adequate bestuurlijke en strafrechtelijke sancties vast te stellen als de regels die uitvoering geven aan de verordening niet worden nageleefd. Daarnaast bevat het voorstel een verplichting voor de lidstaten om alle maatregelen te treffen die nodig zijn om de daadwerkelijke toepassing van die sancties te garanderen.

b) *Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en beschikkingen) met commentaar t.a.v. haalbaarheid*

De verordening wordt met ingang van 1 januari 2015 van toepassing. Aangezien hier een wetswijziging noodzakelijk is, is minimaal een uitvoeringstermijn van twee jaar vereist. Nederland zal bij de verdere onderhandelingen van de ontwerpverordening inzetten op een overgangstermijn van ten minste 24 maanden.

c) *Wenselijkheid evaluatie-/horizonbepaling*

In de verordening is een verplichting opgenomen om de toepassing van de verordening te evalueren. Dit zal gebeuren vijf jaar na de datum waarop de verordening van toepassing is in de lidstaten.

7. Implicaties voor uitvoering en handhaving

a) Uitvoerbaarheid.

Het voorstel bewerkstelligt een verregaande harmonisatie en vereenvoudiging van de bestaande wetgeving voor consumentenproducten. Wel blijven er voor zowel marktdeelnemers als toezichthouders situaties bestaan waar onduidelijkheid kan ontstaan over de voor marktdeelnemers geldende verplichtingen. Het gaat daarbij om de vele ondernemers die zowel in niet- geharmoniseerde producten handelen als in wel geharmoniseerde. Het is in de praktijk goed denkbaar dat een ondernemer zowel de verplichtingen uit het voorstel moet nakomen en doorvoeren in zijn bedrijfsvoering als die welke in specifieke productrichtlijnen zijn voorgeschreven.

b) Handhaafbaarheid.

Ook hier geldt dat het voorstel door een verregaande harmonisatie en vereenvoudiging van de bestaande wetgeving voor consumentenproducten een betere handhaafbaarheid bewerkstelligt. Toch blijven voor de toezichthouders situaties bestaan waar mogelijke onduidelijkheid kan ontstaan over de voor marktdeelnemers geldende verplichtingen zoals genoemd bij de uitvoerbaarheid. De toezichthouder zal in zijn controles dan ook rekening moeten houden met deze verschillende regiem al naar gelang de productgroep in kwestie die wordt verhandeld. Daarnaast roept de uitbreiding in de "dienstensfeer" (producten waarmee de consument "in contact komt" in kader dienstverlening) vraagtekens op. Het is vooralsnog onduidelijk om welke producten het gaat en in welke situaties het product dat door een dienstverlener in de aanwezigheid van consumenten wordt gebruikt ook veilig moet zijn.

8. Implicaties voor ontwikkelingslanden

Nederland is geen voorstander van het vermelden van het land van oorsprong. Indien dit onderdeel van het voorstel toch van kracht wordt, zal Nederland ervoor pleiten dat voor producten uit ontwikkelingslanden de oorsprongsregels gelden zoals die zijn vastgelegd onder het Algemeen Preferentieel Stelsel (APS).

9. Nederlandse positie

Ten algemene staat Nederland positief tegenover het voorstel maar plaatst wel een aantal kanttekeningen. Het voorstel bewerkstelligt een verregaande harmonisatie en vereenvoudiging van de bestaande wetgeving voor consumentenproducten voor zowel het bedrijfsleven als voor de rijksoverheid. Het onderhavige voorstel bevat maatregelen voor consumenten producten die niet in verticale productrichtlijnen geregeld zijn. Deze voorstellen verschillen op sommige punten met maatregelen die in specifieke productrichtlijnen zijn opgenomen. Nederland zal hier vragen over stellen.

Ook is Nederland geen voorstander van de verplichting om het land van oorsprong te vermelden. Nederland steunt dit niet omdat het zorgt voor lastenverzwaring, meer toezicht vergt en weinig

toegevoegde waarde zal hebben. Ook is het niet in de impact assessment meegenomen. De maatregel zou mogelijk kunnen worden beschouwd als een niet-tarifaire handelsbelemmering en is mogelijk in strijd met onze WTO-verplichtingen.

Verder wil Nederland nog kritisch kijken naar de gedelegeerde handelingen in de artikelen 13.3 en 15.3. In het huidige voorstel kan de Europese Commissie namelijk (artikel 15.3) bepalen voor welke producten, categorieën en groepen producten marktdeelnemers een traceringsysteem moeten inrichten. Dit heeft vergaande consequenties voor marktdeelnemers. Nederland wil nog nader onderzoeken of in deze gevallen de gedelegeerde handelingen wel wenselijk zijn en niet beter gekozen kan worden voor uitvoeringshandelingen met de onderzoeksprocedure. Met betrekking tot artikel 13.3 wenst Nederland nadere informatie over de strekking van het voorstel alvorens een definitief standpunt in te nemen of gedelegeerde handelingen wel wenselijk zijn. Nederland zal zich tijdens de onderhandelingen inzetten om de administratieve lasten die uit het voorstel voortkomen zo beperkt mogelijk te houden, zonder afbreuk te doen aan de doeltreffendheid van de maatregelen. Nederland zal daartoe oproepen aandacht te hebben voor de lastenlichte variant van de voorgestelde maatregelen, met extra aandacht voor de nalevingkosten die voortkomen uit de maatregelen.

Ook de toename van uitvoerings- en handhavingslasten dient zo veel mogelijk te worden voorkomen. Nederland wenst daarom al voor de aanvaarding van dit voorstel duidelijkheid te krijgen over deze aspecten, zodat de kosten voor de rijksoverheid op voorhand te bepalen zijn. Daarnaast roept de uitbreiding in de "dienstensfeer" (producten waarmee de consument "in contact komt" in kader dienstverlening) vraagtekens op. Het is vooralsnog onduidelijk om welke producten het gaat en in welke situaties het product dat door een dienstverlener in de aanwezigheid van consumenten wordt gebruikt ook veilig moet zijn. Nederland wenst ook hier duidelijkheid te krijgen over deze aspecten.

Wanneer het opnemen van het land van oorsprong toch wordt doorgevoerd, zal Nederland ervoor pleiten dat voor producten uit ontwikkelingslanden de oorsprongsregels gelden zoals die zijn vastgelegd onder het APS.

Tot slot wil Nederland de mogelijkheid onderzoeken om de verordening te verbreden tot een verordening die veiligheids- en gezondheidseisen stelt aan alle producten. Dit omdat er signalen zijn dat sommige producten buiten de productveiligheidsregelgeving vallen.