Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2012–2013

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

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

GB

BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 15 maart 2013

Overeenkomstig de bestaande afspraken heb ik de eer u hierbij vijf fiches aan te bieden die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC).
Fiche 1: Wijziging verordening GNSS-Agentschap
Fiche 2: Richtlijn strafrechtelijke bescherming tegen eurovalsemunterij
Fiche 3: Richtlijn netwerk- en informatiebeveiliging
Fiche 4: Mededeling strategie inzake cyberbeveiliging van de Europese Unie
Fiche 5: Verordening veiligheid consumentenproducten

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

kst-22112-GB
ISSN 0921 - 7371
's-Gravenhage 2013

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://eurlex.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 communicatie-diensten 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. personele) 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 ontwerpwetgeving 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 bezien 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 toezichthoudende 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