Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

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

Nr. 2407 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 oktober 2017

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

Fiche: Gezamenlijke mededeling Bouwen aan sterke cyberbeveiliging voor de EU
Fiche: Verordening agentschap ENISA en Europees kader voor Cyberbeveiligingscertificering (Kamerstuk 22 112, nr. 2408)
Fiche: Richtlijn fraude niet-chartaal geldverkeer (Kamerstuk 22 112, nr. 2409)
Fiche: Verordening betreffende het Europees Burgerinitiatief (Kamerstuk 22 112, nr. 2410)
Fiche: Mededeling vernieuwde strategie voor het industriebeleid van de EU (Kamerstuk 22 112, nr. 2411)

De Minister van Buitenlandse Zaken,
A.G. Koenders

kst-22112-2407
ISSN 0921 - 7371
's-Gravenhage 2017

Fiche: Gezamenlijke Mededeling Bouwen aan sterke cyberbeveiliging voor de EU

1. Algemene gegevens

a) *Titel voorstellen*
1. Gezamenlijke mededeling Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU
2. Mededeling De NIS-richtlijn ten volle benutten – naar de doeltreffende uitvoering van Richtlijn houdende maatregelen voor een hoog gemeenschappelijk niveau van Beveiliging van netwerk – en informatiesystemen in de Unie
3. Aanbeveling inzake een gecoördineerde respons op grootschalige cyberincidenten en crisis

b) *Datum ontvangst Commissiedocumenten*
september 2017

c) *Nr. Commissiedocumenten*
JOIN (2017)450, COM (2017) 476, C (2017) 6100

d) *EUR-Lex*
JOIN(2017)450 Mededeling Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&qid=1505714068092&from=NL
COM(2017)476 Mededeling De NIS-richtlijn ten volle benutten – naar de doeltreffende uitvoering van Richtlijn houdende maatregelen voor een hoog gemeenschappelijk niveau van Beveiliging van netwerk – en informatiesystemen in de Unie: http://eur-lex.europa.eu/resource.html?uri=cellar:d829f91d-9859–11e7-b92d-01aa75ed71a1.0001.02/DOC_1&format=PDF
C (2017) 6100 Aanbeveling van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises: http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32017H1584&rid=1

e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
N.v.t.

f) *Behandelingstraject Raad*
Raad Justitie en Binnenlandse Zaken

g) *Eerstverantwoordelijk ministerie*
Ministerie van Veiligheid en Justitie

2. Essentie voorstel

Het cyberbeveiligingspakket van de Europese Commissie bestaat uit een vijftal voorstellen. In dit BNC-fiche zal het zwaartepunt liggen bij de gezamenlijke mededeling weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU (hierna: gezamenlijke mededeling).
Tevens wordt in dit fiche de mededeling met richtlijnen voor de implementatie van de Europese richtlijn voor Netwerk- en Informatiebeveiligingsrichtlijn[1] (hierna: mededeling NIS-richtlijn) behandeld omdat de volledige uitvoering van de richtlijn een centraal element is in de gezamenlijke mededeling. De aanbeveling voor een blauwdruk voor gecoördineerde crisisrespons in het geval van een grootschalige en grensoverschrijdende cyberincident (hierna: aanbeveling blauwdruk) wordt ook in dit fiche behandeld. Voor de verordening voor het mandaat van het Europese agentschap voor netwerk- en informatiebeveiliging

[1] Richtlijn (EU) 2016/1148 voor een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging (NIS-richtlijn)

(ENISA) en het Europees kader voor cyberbeveiligingscertificering, en het richtlijnvoorstel over de bestrijding van fraude en vervalsing in verband met niet-chartale betaalmiddelen zijn vanwege het wetgevende karakter en/of de impact van de voorstellen separate BNC-fiches opgesteld.
De drie voorstellen die in dit fiche worden behandeld, bouwen voort op de resultaten van de EU Cyberstrategie uit 2013[2] en zijn een reactie op de toegenomen digitale dreiging tegen de EU en haar economieën, democratische vrijheden en waarden.

Gezamenlijke mededeling

Om de toegenomen dreiging het hoofd te bieden wordt in de gezamenlijke mededeling langs een drietal lijnen versterkingen voorgesteld:

1) De EU weerbaarder maken tegen cyberaanvallen
   In dit kader wordt onder meer voorgesteld om ENISA een centrale rol, en een permanent en uitgebreider mandaat te geven. In de mededeling wordt in het kader van weerbaarheidsverhoging een Europees kader voor cyberbeveiligingscertificering voor ICT-producten en -diensten voorgesteld. Binnen het cyberbeveiligingscertificeringskader zal de Commissie, op voorstel van ENISA en na consultatie met stakeholders (inclusief lidstaten), certificeringsschema's vaststellen die EU-breed gaan gelden. Tevens wordt de implementatie van de NIS-richtlijn als speerpunt benoemd. De mededeling van de Commissie met richtlijnen voor de implementatie van de NIS-richtlijn helpt de lidstaten hierbij. Ten behoeve van een gecoördineerde respons in het geval van een grootschalig cyberincident of crises heeft de Commissie een aanbeveling voor een blauwdruk opgesteld. In aanvulling op de al bestaande samenwerking en informatie-uitwisseling wordt een netwerk van (nationale) kenniscentra voor cyberbeveiliging voorgesteld met een centraal nieuw op te richten Europees onderzoeks- en kenniscentrum voor cyberbeveiliging. Dit met als doel de Europese kennisontwikkeling en innovatiepositie te intensiveren.
2) Doeltreffend afschrikken in de EU
   De Commissie constateert dat een effectieve aanpak vanuit de opsporingsdiensten, gericht op detectie, attributie en vervolging van cyber criminelen, centraal staat in het effectief afschrikken. De Commissie kondigt daarom aan met maatregelen te komen dit mogelijk te maken, onder meer via voorstellen en praktische maatregelen om grensoverschrijdende toegang tot elektronisch bewijs te faciliteren. Ook roept de EU de lidstaten op om gebruik te maken van de bestaande mogelijkheden op grond van de Boedapest Conventie van de Raad van Europa. Daarnaast pleit de Commissie voor meer personele en technische capaciteit bij Europol om opsporingsonderzoeken te ondersteunen en internationaal te coördineren. Het kader voor diplomatieke respons tegen agressors die misbruik maken van kwetsbaarheden zal verder worden uitgewerkt, evenals het versterken van situationeel bewustzijn. Het belang van publiek-private samenwerking tegen cybercriminaliteit wordt benadrukt. Tevens worden verschillende voorstellen gedaan ter bevordering van synergiën tussen de militaire en civiele inspanningen op het gebied van cyber.
3) Versterking van de internationale samenwerking op het vlak van cyberbeveiliging
   Voor het verdedigen van de kernwaarden van de EU en het bevorderen van open, vrij en transparant gebruik van cybertechnologieën zet de EU ook in op het versterken van internationale samenwerking. Hiertoe zal de EU in haar internationale contacten met partners en in

[2] JOIN (2016)1 Cybersecurity Strategie van de Europese Unie: een open vrij en veilig cyberspace

de multilaterale context het belang van cyberbeveiliging voor internationale veiligheid en de toepasselijkheid van internationaal recht in cyberspace benadrukken. Daarnaast zal de EU zich richten op capaciteitsopbouw in derde landen. Tevens wordt voorgesteld om de cybersamenwerking op militair gebied te versterken, zowel binnen de EU als met de NAVO, ook in het kader van de aanpak van hybride dreigingen.

Mededeling NIS-richtlijn

De mededeling over de NIS-richtlijn is bedoeld om lidstaten bij hun inspanningen te ondersteunen bij de implementatie van deze in 2016 vastgestelde richtlijn op nationaal niveau. De NIS-richtlijn is gericht op het creëren van een gemeenschappelijk niveau van netwerk- en informatiebeveiliging binnen Europa. In de mededeling worden door de Commissie verdere richtsnoeren gegeven over de wijze waarop de richtlijn in de praktijk moet functioneren, worden goede praktijken uit de lidstaten aangereikt en worden specifieke bepalingen nader uitgelegd.

Aanbeveling blauwdruk

De blauwdruk beschrijft hoe cyberbeveiliging in de bestaande crisisbeheersingsmechanismen op EU-niveau kunnen worden aangepast om in EU-verband te kunnen reageren op grootschalige en grensoverschrijdende cyberincidenten en crises. De blauwdruk doet een aanzet om te komen tot afgestemde samenwerkingsprocedures en -mechanismen, met vastgelegde rollen en verantwoordelijkheden voor de betrokken actoren.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Nederland is als open en internationaal georiënteerde economie gebaat bij een stabiel en vrij toegankelijk cyberdomein. Hiertoe zet Nederland samen met zijn internationale partners en door middel van effectieve Multi stakeholder samenwerking in op een veilig, vrij en open cyberdomein, waarin de kansen die digitalisering onze economie en samenleving biedt volop worden benut, dreigingen het hoofd wordt geboden en fundamentele rechten en waarden worden beschermd.

De samenhang tussen veiligheid, vrijheid en maatschappelijke groei wordt hiertoe, in een dynamische balans, tot stand gebracht in een constante open en pragmatische dialoog tussen alle stakeholders, waaronder overheden, bedrijven, het maatschappelijke middenveld, academici en de technische gemeenschap, zowel nationaal als internationaal. De concrete uitwerking van deze visie op het gebied van veiligheid is vastgelegd in de Nederlandse Nationale Cyber Security Strategie 2 (NCSS2).[3]

Concreet heeft Nederland hier internationaal de afgelopen jaren op een aantal manieren invulling aan gegeven. Zo heeft Nederland tijdens het Europees voorzitterschap van de Raad in 2016 als aanjager opgetreden bij het opstarten van de implementatie van de NIS-richtlijn via onder meer het Europees netwerk van computer security incident response teams (CSIRTs Network) en heeft Nederland de totstandkoming van een diplomatiek raamwerk geïnitieerd waarmee EU-lidstaten individueel en gezamenlijk cyberdreigingen het hoofd kunnen bieden. Op het gebied van

[3] Nationale Cyber Security Strategie 2 (2013) (https://www.ncsc.nl/organisatie/nationale+cybersecurity+strategie)

cybercrime is Nederland internationaal actief in EU en multilateraal verband om de aanpak van deze vorm van grensoverschrijdende criminaliteit te verbeteren.

Bovendien zet Nederland zich in, zoals vervat in de Internationale Cyberstrategie (2017)[4], voor het opbouwen en bevorderen van een internationaal juridisch en normatief kader voor het cyberdomein. Daartoe bouwt Nederland wereldwijd actief aan publiek-private coalities om internationaal recht en internationale gedragsnormen te versterken, internationale (operationele) informatie-uitwisseling te bevorderen en onwettige inperking van fundamentele rechten online te bestrijden. Het gastheerschap van de Global Conference on Cyber Space in 2015, de lancering van het Global Forum on Cyber Expertise (GFCE) en de oprichting van de Global Commission on the Stability of Cyber Space (GCSC) zijn hier concrete voorbeelden van. Ook binnen NAVO-context wordt aandacht aan cyber besteed. Daarnaast is Nederland actief betrokken bij de cross-regionale intergouvernementele Freedom Online Coalitie (FOC) en heeft Nederland zich in VN-verband actief opgesteld als bruggenbouwer tijdens het vastgelopen proces van de VN Governmental Group of Experts (UNGGE).

Steeds meer statelijke actoren gebruiken cybermiddelen om geopolitieke doelstellingen te behalen. Het kabinet is daarom voorstander van intensieve samenwerking tussen EU en NAVO op het gebied van cyber. De ordenende rol van de EU en de veiligheidsbevorderende rol van de NAVO kunnen elkaar hierin versterken.

b) Beoordeling + inzet ten aanzien van deze voorstellen

Gezamenlijke mededeling

De inschatting van de dreigingsontwikkeling van de Commissie, zoals weergegeven in de gezamenlijke mededeling sluit aan bij de inschatting van het kabinet en komt overeen met in het jaarlijkse Cyber Security Beeld Nederland (CSBN)[5]. De noodzaak tot versterking van de inzet op cyberbeveiligingsgebied, zowel door de lidstaten als op Europees niveau, wordt door het kabinet ondersteund.

Om deze dreiging effectief het hoofd te kunnen bieden is een integrale aanpak nodig, waarbij de veiligheid van de digitale interne markt, cybercriminaliteit, cyberdiplomatie, cyber capaciteitsopbouw, digitale rechten en defensie terugkomen. Het kabinet is daarom verheugd dat de gezamenlijke mededeling deze brede aanpak ook voorstaat. Het kabinet heeft daarom een positieve grondhouding en kijkt uit naar de nadere uitwerking van de aangekondigde plannen die de Commissie in 2018 en later zal publiceren.

Bij het formuleren van de reactie van de Raad zal Nederland de waardering voor de gezamenlijke mededeling uitspreken. Het is van belang dat dit een gezamenlijke aanpak betreft; Nederland ondersteunt de integrale aanpak van cyberbeveiliging. Daarbij zal Nederland een aantal aandachtspunten en verwachtingen meegeven. De voorgestelde aanpak van cybercrime is in lijn met Nederlands beleid en inzet en zal worden gesteund. Het toenemende internationale karakter van opsporingsonderzoeken wordt erkend, de roep voor meer samenwerking ondersteund, maar daarbij moet wel rekening gehouden worden met de bestaande nationale bevoegdheden wat betreft de opsporing. De conclusie dat

[4] Internationale Cyberstrategie (2017) Digitaal bruggen slaan (Kamerstuk 26 643, nr. 447)
[5] Cyber Securitybeeld Nederland (2017) (Kamerstuk 26 643, nr. 477)

Europa meer moet investeren in kennis en innovatie op cyberterrein wordt onderschreven. De aandacht voor publiek-private samenwerking (PPS) is positief, en sluit volledig aan bij de Nederlandse visie dat PPS noodzakelijk is voor het succesvol veiliger maken van het internet. Ook is Nederland positief over de oproep dat in alle lidstaten voorwaarden worden vastgesteld voor de gecoördineerde bekendmaking van kwetsbaarheden, voortbouwend op beste praktijken en toepasselijke normen.

Naast bovenstaande zijn er enkele zaken die Nederland bij de verdere uitwerking scherp zal volgen. Zo zal Nederland zich in algemene zin verzetten tegen plannen die strijdig zijn met de verdragsrechtelijke afspraken betreffende de bevoegdheid van lidstaten op het gebied van nationale veiligheid, omdat hier de verantwoordelijkheid bij de lidstaten zelf ligt. Daarnaast zal Nederland inzetten op versterking van de Europese cyberbeveiligingsmarkt binnen een transparante mondiale markt. Voorts is voor Nederland een vrij en open cyberspace evenzeer van essentieel belang. Nederland zal dan ook toezien op een bestendiging van fundamentele rechten en vrijheden binnen het EU-internationale cyberbeleid.

Een belangrijk punt voor Nederland is dat zoveel mogelijk moet worden uitgegaan van en aansluiting moet worden gezocht bij reeds bestaande structuren, organisaties, initiatieven en mechanismen, in plaats van in te zetten op nieuwe initiatieven en organisaties. Voor het voorgestelde Europees onderzoeks- en kenniscentrum voor cyberbeveiliging zal de Commissie worden gevraagd om nadere onderbouwing van de noodzaak hiervan. Tevens zal de Commissie worden gevraagd toe te lichten waarom de beoogde innovatie- en kennisdoelen voor het kenniscentrum niet binnen bestaande structuren, zoals bijvoorbeeld onderzoeksprogramma Horizon2020 en het reeds bestaande Joint Research Centre (JRC) kunnen worden gehaald. De inzet van Nederland is er daarbij op gericht dat Nederlands (kennis)instellingen beschikbare Europese onderzoeksgelden kunnen benutten.

Ten aanzien van het stimuleren van de uitrol van Internet Protocol versie 6 (IPv6) is Nederland positief. Met het oude internetprotocol (IPv4) is het aantal beschikbare IP-adressen beperkt en is er wereldwijd sprake van schaarste. Bij conversie naar IPv6 zijn er (vrijwel) oneindig veel IP-adressen beschikbaar en ontstaat in beginsel de mogelijkheid om eenvoudig één IP-adres per individuele gebruiker/device toe te wijzen. Het stimuleren van de uitrol van IPv6 zal enerzijds ten goede komen aan de opsporing van criminaliteit in het digitale domein, anderzijds zorgt het voor een versterking van het cybersecurityveld. Aanbieders van telecommunicatiediensten en netwerken kunnen door de toepassing van IPv6 meer inzicht krijgen in kwetsbaarheden en misbruik binnen het eigen netwerk, hetgeen in het bredere kader van versterking van cybersecurity relevant is.

Mededeling NIS-richtlijn

De mededeling met richtlijnen voor implementatie van de NIS-richtlijn geeft aan dat de Commissie veel belang hecht aan succesvolle implementatie van de richtlijn. Het kabinet onderschrijft dit belang. Daarom zal het de niet-bindende richtsnoeren, waar bruikbaar voor de specifieke Nederlandse context, meenemen in de nationale implementatie. Tevens wordt hierover gesproken in de Cooperation Group, het samenwerkingsverband van Europese lidstaten om de strategische samenwerking en de uitwisseling van informatie in het kader van onder meer de NIS-richtlijn te faciliteren en te ondersteunen, waaraan Nederland actief deelneemt. Hierin worden actief kennis en ervaringen gedeeld om zo in de hele EU tot een hoog gezamenlijk niveau te komen.

Aanbeveling blauwdruk

De Commissie doet ten behoeve van effectieve EU-response op cybercrisis een aanbeveling inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises. Het kabinet kan de aanbeveling in grote lijnen ondersteunen maar zal benadrukken dat de uitwerking hiervan binnen bestaande werkgroepen en crisisstructuren moet plaatsvinden, en dat crisisrespons een nationale verantwoordelijkheid is, waarbij Europese samenwerking nuttig en nodig kan zijn. Verder dient het initiatief de informatievergaring en informatiepositie van nationale CSIRTs niet te bemoeilijken of te verzwakken en moet het CSIRTs Netwerk de basis blijven voor operationele beeldvorming en initiatieven.

c) Eerste inschatting van krachtenveld

Naast Nederland hebben ook andere lidstaten in het verleden aangegeven het belangrijk te vinden dat de EU Cyberbeveiliging Strategie uit 2013 een vervolg krijgt. Een positieve grondhouding in de Raad wordt daarom verwacht. Naar verwachting zullen lidstaten net als Nederland aandacht vragen voor het belang van de instandhouding van bevoegdheden wat betreft nationale veiligheid en crisisrespons. Daarnaast zal naar verwachting aandacht gevraagd worden voor het tegengaan van dubbelingen en overlap in structuren en organisaties.

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

a) Bevoegdheid

Gezamenlijke mededeling

De plannen van de Commissie en de Hoge Vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid strekken met name ter bescherming van de Europese Unie tegen digitale aanvallen. De plannen passen volgens Nederland op hoofdlijnen binnen de bevoegdheden van de EU op de terreinen interne markt (art. 4 lid 2 onder a en 114 VWEU), gemeenschappelijk buitenlands en veiligheidsbeleid (art. 21 en 24 VEU, art. 220 VWEU) en justitiële samenwerking in strafzaken (art. 82 VWEU). Wel bevindt een aantal van de aangekondigde acties en plannen zich dicht tegen of op het terrein van nationale veiligheid (een exclusieve bevoegdheid van de lidstaten, art. 4 lid 2 VEU) en nationale bevoegdheden op het gebied van crisisbeheersing. Hoewel de Commissie en de Hoge Vertegenwoordiger in de gezamenlijke mededeling vermelden dat lidstaten verantwoordelijk blijven voor nationale veiligheid, stellen zij dat vanwege het grensoverschrijdende karakter van de digitale dreigingen ook de EU hierin een rol heeft. Nederland zal er bij de concretisering van de plannen nauwgezet op toezien dat de Unie de verdragsrechtelijke bepalingen hierin respecteert. Ditzelfde geldt voor de voorstellen op het gebied van de onderwijskundige dimensie van cyberbeveiliging.

In de gezamenlijke mededeling staan voorstellen over elektronisch bewijs op het terrein van de ruimte van vrijheid, veiligheid en recht (Titel V VWEU). Wanneer de voorstellen concreet worden zal in het BNC-fiche over die voorstellen een nadere beoordeling volgen. Het functioneren van Europol valt onder de bevoegdheid van art. 88 VWEU waarin de bevoegdheid voor coördinatie, organisatie en uitvoering van onderzoeken en operationele acties wordt vermeld, die gezamenlijk met de bevoegde autoriteiten van de lidstaten worden uitgevoerd. Nederland heeft een positieve grondhouding ten opzichte van het voorstel voor betere

internationale samenwerking in de opsporing van cybercrime en ziet hier een belangrijke rol voor Europol.

Mededeling NIS-richtlijn

In het geval van de mededeling aangaande de effectieve implementatie van de NIS-richtlijn zijn geen extra bevoegdheden voor de Unie voorzien. De Commissie geeft in deze mededeling een niet-bindende nadere uitleg aan de richtlijn en doet suggesties voor de implementatie. Daartoe is de Commissie bevoegd.

Aanbeveling blauwdruk

De aanbeveling is een van de in de gezamenlijke mededeling genoemde maatregelen, die raken aan de nationale veiligheid een exclusieve bevoegdheid van de lidstaten, op grond van artikel 4 lid 2 VEU) en nationale bevoegdheden op het gebied van crisisbeheersing.

b) Subsidiariteit

Gezamenlijke mededeling

Gezien het inherent grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging heeft Nederland een positieve grondhouding ten opzichte van de subsidiariteit van de gezamenlijke mededeling. Nederland zal daarbij blijven uitdragen dat de Unie op grond van art. 4 lid 2 VEU de bescherming van de nationale veiligheid en crisisbeheersing dient te eerbiedigen en dat voorstellen deze bevoegdheid van de lidstaten onverlet laten.

Mededeling NIS-richtlijn

Zoals gezegd geeft de Commissie in de mededeling over de NIS-richtlijn een niet-bindende nadere uitleg aan de richtlijn en doet suggesties voor de implementatie. Nederland is positief over de subsidiariteit omdat de Commissie op deze manier op Europees niveau de lidstaten helpt met de implementatie van de richtlijn en hen stimuleert tot harmonisatie van hun implementatiekeuzes.

Aanbeveling blauwdruk

Nederland heeft een positieve grondhouding ten aanzien van de subsidiariteit van de blauwdruk omdat samenwerking op EU-niveau in het geval van een incident of crisis essentieel is. Ook binnen Europese crisismechanismes geldt dat de Unie de bevoegdheid van de lidstaten op grond van artikel 4, lid 2, VEU moet respecteren.

c) Proportionaliteit

Gezamenlijke mededeling

De grondhouding van het kabinet ten aanzien van de proportionaliteit van maatregelen die worden aangekondigd in de gezamenlijke mededeling is positief, onder meer omdat zij de cyberveiligheid van Europa op een effectieve en evenredige wijze naar een hoger niveau brengen. De proportionaliteit zal pas echt kunnen worden beoordeeld nadat de voorstellen in de mededeling geconcretiseerd worden.

Mededeling NIS-richtlijn

De mededeling over de NIS-richtlijn betekent geen extra taken, bevoegdheden of middelen voor de Unie die moeten worden beoordeeld op proportionaliteit. De mededeling ondersteunt lidstaten bij hun inspanningen bij de implementatie van de NIS-richtlijn.

Aanbeveling blauwdruk

De grondhouding van het kabinet ten aanzien van de proportionaliteit van de blauwdruk is positief. Aangezien er bij de blauwdruk van de Commissie reeds bestaande crisismechanismes als uitgangspunt worden genomen kan er adequaat en effectief op Europees niveau worden samengewerkt in het geval van een crisis of een incident.

d) Financiële gevolgen

Er wordt geen concrete informatie gegeven over een eventueel verwachte financiële impact op de hoogte van de EU-begroting. Het ligt echter in de rede dat voor de voorgestelde versterking van inzet op kennisontwikkeling en innovatie, inclusief het Europees onderzoeks- en kenniscentrum voor cyberbeveiliging, middelen nodig zijn. Hetzelfde geldt voor het voorgestelde noodfonds en de uitbreiding van het mandaat van ENISA. Nederland is van mening dat de benodigde EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2014–2020 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Eventuele budgettaire gevolgen voor de Nederlandse begroting worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

e) Gevolgen voor regeldruk en administratieve lasten

De stukken waarop dit BNC-fiche betrekking heeft geven op dit moment geen aanleiding gevolgen te verwachten voor regeldruk en administratieve lasten, voor de overheid, bedrijfsleven of burgers. Bij de nog te volgen concretisering zal het kabinet per voorstel nadrukkelijk in de gaten houden of dit veranderd; bijvoorbeeld met name ten aanzien van certificering en in hoeverre daarbij ook rekening wordt gehouden met relevante publiek-private samenwerking. Eventuele stijgingen van de administratieve lasten dienen te worden voorkomen of te worden gemitigeerd. En als de stijgingen onvermijdelijk zijn, dienen deze te worden gecompenseerd door het beleidsverantwoordelijke departement, waarbij compensaties zoveel mogelijk dienen te geschieden binnen het domein waarin de tegenvaller plaatsvindt.