Fiche 5: Herziening richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn)

1. Algemene gegevens

a) Titel voorstel

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148

b) Datum ontvangst Commissiedocument

16 december 2020

c) Nr. Commissiedocument

COM (2020) 823

d) EUR-Lex

https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52020PC0823&qid=1609770678546

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing

SWD (2020) 345

https://ec.europa.eu/digital-single-market/en/news/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union

f) Behandelingstraject Raad

Telecomraad

g) Eerstverantwoordelijk ministerie

Ministerie van Justitie en Veiligheid

h) Rechtsbasis

Artikel 114 Verdrag betreffende de Werking van de Europese Unie (VWEU)

i) Besluitvormingsprocedure Raad

Gekwalificeerde meerderheid

j) Rol Europees Parlement

Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

De Commissie doet een voorstel voor een richtlijn met maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de EU, als vervanging van de oorspronkelijke Netwerk- en informatiebeveiligingsrichtlijn (NIB-richtlijn). De oorspronkelijke NIB-richtlijn regelt de beveiliging

van netwerk- en informatiesystemen van aanbieders van essentiële diensten (AED's) en van digitale dienstverleners (DSP's), onder meer door hen te laten voldoen aan een zorg- en meldplicht. Deze AED's dienen door de lidstaten zelf te worden aangewezen. De Commissie constateert dat sinds het vaststellen van de NIB-richtlijn in 2016 de digitalisering van de eengemaakte markt is toegenomen en dat het dreigingsbeeld zich verder heeft ontwikkeld. Beide ontwikkelingen zijn verder versterkt door de COVID-19 crisis. Daarnaast is er in opdracht van de Commissie een evaluatie van de NIB-richtlijn uitgevoerd, die een aantal knelpunten in het functioneren van de richtlijn identificeert. Op basis van deze ontwikkelingen en de uitkomsten van deze evaluatie heeft de Commissie besloten om een voorstel te doen om de huidige richtlijn te vervangen, voortbouwend op de huidige richtlijn. Het voorstel maakt deel uit van een breder pakket aan maatregelen van de Commissie op het gebied van cybersecurity[1] en de bescherming van vitale infrastructuur,[2] waarover separaat BNC-fiches worden opgesteld die gelijktijdig aan uw Kamer worden verzonden.

De Commissie stelt voor om de huidige NIB-richtlijn op meerdere onderdelen te wijzigen.

Reikwijdte van de richtlijn
Krachtens de huidige richtlijn wijzen lidstaten zelf de AED aan die binnen de reikwijdte van de richtlijn vallen en voor wie de daarbinnen geregelde verplichtingen gelden. DSP's vallen automatisch binnen het bereik van de huidige richtlijn, met een uitzondering voor kleine en micro-organisaties.[3] De Commissie stelt voor de opsomming van sectoren waarbinnen sprake is van 'essentiële entiteiten' uit te breiden met een aantal nieuwe sectoren (afvalwater, overheidsdiensten en ruimtevaart) ten opzichte van de huidige richtlijn. Daarnaast worden in die opsomming binnen de bestaande sectoren extra subsectoren toegevoegd. Ook wordt de categorie 'belangrijke entiteiten' (*important entities*) toegevoegd.[4] DSP's verdwijnen als afzonderlijke categorie, maar de aanbieders daarbinnen blijven binnen de reikwijdte van de richtlijn en worden verdeeld over de categorieën essentieel en belangrijk.

Een belangrijke wijziging is daarnaast dat essentiële entiteiten niet langer worden aangewezen door de lidstaten. In plaats daarvan worden organisaties in de nieuwe richtlijn zelf centraal als zodanig aangemerkt, indien ze in één van de in bijlage 1 genoemde sectoren actief zijn. Daarbij geldt in beginsel een uitzondering voor kleine en micro-aanbieders.[5] Eenzelfde centrale aanwijzing geldt voor de belangrijke entiteiten, die actief zijn in een van de in de tweede bijlage genoemde sectoren. Daarnaast gelden de verplichtingen in de richtlijn ook voor kleine en micro-

[1] COM (2020) 18 - EU-strategie inzake cyberbeveiliging voor het digitale tijdperk
[2] COM (2020) 829 – Richtlijn veerkracht kritieke entiteiten
[3] De huidige richtlijn omvat publieke en private organisaties in zeven sectoren (energie, vervoer, bankwezen, infrastructuur voor de financiële markt, zorg, drinkwater en digitale infrastructuur) en voor drie digitale diensten (online marktplaatsen, zoekmachines en cloudaanbieders).
[4] Deze categorie omvat publieke en private organisaties in de sectoren post- en koeriersdiensten; afvalbeheer; fabricage, productie en distributie van chemicaliën; voedselproductie; verwerking en distributie; maakindustrie; en digitale aanbieders.
[5] COM (2003) 361

ondernemingen in sectoren in de bijlagen, indien zij voldoen aan een van de in deze richtlijn genoemde omstandigheden (bijvoorbeeld als ze de enige aanbieder van een dienst in een lidstaat zijn). Lidstaten houden ook de bevoegdheid om daarnaast nog extra entiteiten, die diensten in de lidstaat aanbieden, aan te wijzen op wie de bepalingen uit de richtlijn van toepassing zijn.

Verplichtingen van aanbieders

Ten opzichte van de huidige richtlijn worden nadere eisen gesteld met betrekking tot het voldoen aan de zorgplicht[6] en de meldplicht[7] door essentiële en belangrijke entiteiten. Zo wordt voor de zorgplicht een lijst met soorten maatregelen toegevoegd, waar aanbieders sowieso aan moeten voldoen (zoals beveiliging van de toeleveringsketen en afhandeling van incidenten). De Commissie kan middels gedelegeerde- en uitvoeringsbesluiten die maatregelen nader specificeren en daar extra soorten maatregelen aan toevoegen. Daarnaast kan de Commissie via gedelegeerde besluiten nader bepalen aan welke categorieën essentiële entiteiten certificeringsverplichtingen worden opgelegd. Voor aanbieders van openbare elektronische communicatienetwerken en/of –diensten en aanbieders van vertrouwensdiensten (bijv. het certificaat voor authenticatie van een website), wordt de zorg- en meldplicht uit de respectievelijke sectorale Europese wetgeving[8] verschoven naar de onderhavige richtlijn, onder intrekking van de betrokken bepalingen in die sectorale Europese regelgeving. Nieuw element is dat het bestuur van een organisatie aansprakelijk kan worden gesteld voor bijvoorbeeld het niet-naleven van de zorgplicht door hun organisatie. Ten aanzien van de meldplicht worden er voorstellen gedaan voor een nadere omschrijving van incidenten die gemeld moeten worden, een verbreding van de meldplicht (zoals de verplichting om afnemers van hun dienstverlening te informeren), en een nadere invulling van de meldprocedure. Essentiële en belangrijke entiteiten dienen door lidstaten ook aangemoedigd te worden om incidenten waarbij het vermoeden van zware criminele activiteit bestaat te melden aan de relevante opsporingsinstanties. Daarbij kunnen Europol en ENISA een faciliterende rol spelen, of kan een nationale CSIRT bijvoorbeeld een aanbieder adviseren om aangifte te doen.

Toezicht

Ten opzichte van de huidige richtlijn geeft het voorstel een nadere invulling van de toezichtsbevoegdheden en handhavingsinstrumenten waarover de autoriteiten minimaal moeten beschikken bij de uitoefening van toezicht. Voor essentiële entiteiten geldt een regime van ex-ante toezicht, belangrijke entiteiten vallen onder ex-post toezicht.

Samenwerking tussen autoriteiten

In aanvulling op de huidige twee groepen om samenwerking tussen de lidstaten te faciliteren, de NIB Samenwerkingsgroep (op strategisch niveau) en het Computer Security Incident Response Team (CSIRT) Netwerk (op technisch niveau) wordt een juridische basis gecreëerd voor het Cyber Crises Liaison Organisation Network (CyCLONe). Dit netwerk voorziet in coördinatie tussen

[6] De eis aan AED's en DSP's om passende technische en organisatorische maatregelen te nemen om hun netwerk en informatiesystemen te beveiligen.
[7] De verplichting om incidenten met aanzienlijke gevolgen voor de dienstverlening te melden.
[8] Richtlijn (EU) 2018/1972 en Verordening (EU) 910/2014

nationale autoriteiten bij grote cyberincidenten en -crises. Het voorstel voegt daarnaast nog meer elementen toe die zien op de samenwerking tussen lidstaten, zoals de organisatie van peer reviews tussen lidstaten, waarbij onder meer de nationale capaciteiten en de effectiviteit van het CSIRT door experts uit andere lidstaten wordt beoordeeld.

Een ander nieuw element is de vereiste aan lidstaten om een raamwerk voor *coordinated vulnerability disclosure* (CVD) op te zetten, inclusief het aanwijzen van een autoriteit die als bemiddelaar kan optreden tijdens een CVD-procedure. ENISA zal een register met bekende kwetsbaarheden gaan bijhouden. Daarnaast dienen lidstaten een maandelijks overzicht van ontvangen meldingen aan ENISA door te geven. Deze informatie zal worden meegenomen in de tweejaarlijkse 'cybersecurity state of the union' die door ENISA zal worden opgesteld.

b) Impact assessment Commissie

De Commissie heeft meerdere opties onderzocht bij het opstellen van de richtlijn, waarbij ook is gekeken naar de optie om de NIB-richtlijn niet aan te passen. Het impact assessment heeft uitgewezen dat de optie om te komen tot een volledig nieuwe richtlijn, gezien de geconstateerde knelpunten en bijbehorende oplossingen, het meest passend wordt geacht. Een nieuwe richtlijn zal een heldere reikwijdte formuleren, de aanwijzing van AED's door de lidstaten gelijktrekken, het handhavingsregime stroomlijnen, informatiedeling tussen de lidstaten verbeteren en het cybersecurity beleid in de gehele Unie verstevigen. Qua doelmatigheid is de Commissie van mening dat, terwijl er additionele implementatie en handhavingskosten verbonden zijn aan de nieuwe richtlijn, dit op de langere termijn opweegt tegen de kosten die bespaard zullen worden door de hogere veiligheidsstandaarden voor een groter aantal organisaties.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Nederland is in hoge mate gedigitaliseerd. Vrijwel alle economische en maatschappelijke processen maken gebruik van digitale middelen. Digitale veiligheid is daarom een noodzakelijke voorwaarde om deze processen draaiende te houden. Daarnaast is Nederland als open en internationaal georiënteerde economie gebaat bij een stabiel cyberdomein. Door digitalisering is de verwevenheid met het buitenland verder toegenomen. Internationale samenwerking op het gebied van digitale veiligheid is daarom een belangrijk onderdeel van de Nederlandse cybersecurityaanpak.

De cybersecurityaanpak van het kabinet is vastgelegd in de Nederlandse Cybersecurity Agenda (NCSA).[9] De NCSA valt uiteen in zeven ambities die bijdragen aan de volgende doelstelling: Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen. Over de voortgang van de NCSA wordt u jaarlijks geïnformeerd.[10] Daarnaast heeft het kabinet in de reactie op het WRR-rapport 'Voorbereiden op digitale ontwrichting' aangegeven hoe het omgaat met crisisbeheersing in het digitale domein.

[9] Kamerstukken II 2017-2018, 26643, nr. 536
[10] Kamerstukken II 2019-2020, 26643, nr. 695

Een belangrijk uitgangspunt van de NCSA is dat iedere private en publieke organisatie zelf primair verantwoordelijk is voor zijn eigen digitale beveiliging. Voor verschillende organisaties die zijn aangemerkt als vitale aanbieder[11] gelden krachtens onder meer de Wet beveiliging netwerk- en informatiesystemen (Wbni) wettelijke verplichtingen. Met de Wbni heeft Nederland de NIB-richtlijn geïmplementeerd. Krachtens de Wbni zijn aanbieders van essentiële diensten (AED's) aangewezen, voor wie de verplichting geldt om passende beveiligingsmaatregelen te nemen voor hun netwerk- en informatiesystemen. Daarnaast dienen deze aanbieders incidenten met aanzienlijke gevolgen voor de verlening van hun dienst te melden bij het NCSC en de sectorale toezichthouder. De toezichthouder ziet toe op de naleving door deze aanbieders van de verplichtingen uit de Wbni, en kan in geval van niet-naleving bijvoorbeeld een bindende aanwijzing geven of een last onder bestuursdwang opleggen. Alle vitale aanbieders kunnen rekenen op bijstand van het NCSC in het geval van een incident of dreiging. Voor een aantal sectoren geldt dat naast of op onderdelen in plaats van de Wbni in sectorale wetgeving verplichtingen aan vitale aanbieders worden gesteld.

Krachtens de Wbni gelden daarnaast ook verplichtingen voor de categorie digitale dienstverleners (online marktplaatsen, zoekmachines, cloudaanbieders). Voor deze categorie geldt een zorgplicht en een meldplicht bij de toezichthouder en het CSIRT voor digitale diensten. Het CSIRT voor digitale diensten kan bijstand verlenen in het geval van een incident.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet herkent de aanleidingen die de Commissie schetst voor de herziening van de NIB-richtlijn. In het Cybersecuritybeeld Nederland 2020 wordt onder andere gewezen op de permanent geworden dreiging van statelijke actoren, de verwevenheid van de digitale ruimte en de toegenomen afhankelijkheid van digitale middelen als gevolg van COVID-19.[12] Daarnaast onderkent het kabinet de noodzaak van stevige Europese samenwerking op het gebied van digitale veiligheid en crisisbeheersing. Het kabinet verwelkomt het voorstel van de Commissie, maar plaatst daarbij wel enkele kritische kanttekeningen, die hieronder nader worden toegelicht.

Het kabinet is van mening dat cybersecurity binnen de EU in samenhang moet worden bekeken. Daarom acht het kabinet het belangrijk dat EU-wetgeving op het gebied van cybersecurity en de bescherming van vitale processen goed op elkaar aansluit. Het kabinet zal onder meer oog blijven houden voor de samenhang tussen de NIB-Richtlijn, de CER-Richtlijn en sectorale wetgeving zoals het voorstel voor Digital Operational Resilience Act (DORA)[13] en de European Electronic

[11] Bepaalde processen zijn zo belangrijk voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur. Binnen deze processen zijn een of meerdere organisaties belangrijk voor de continuïteit en weerbaarheid van het proces. Deze organisaties worden aangeduid als vitale aanbieders.

[12] Kamerstukken II 2019-2020, 26643, nr. 695

[13] COM (2020) 595

Communications Code (EECC).[14] In dit verband merkt het kabinet op dat verplichtingen voor aanbieders van openbare elektronische communicatienetwerken of -diensten, evenals aanbieders van vertrouwensdiensten, uit de respectievelijke sectorale regelgeving[15] zijn verschoven naar de onderhavige richtlijn, maar niet dezelfde formulering hebben als in de sectorale wetgeving. Het kabinet vraagt zich af wat de toegevoegde waarde is van deze verschuiving en ziet daarin het risico dat daarmee de bredere werking van sectorale waarborgen, anders dan gericht op netwerk- en informatiesystemen, die van cruciaal belang zijn voor de betrouwbaarheid van de diensten onderbelicht of verloren raken. Het kabinet kan hier niet zonder meer mee akkoord gaan en zal hier daarover nadere verduidelijking bij de Commissie over vragen, ook waarom niet gebruik is gemaakt van de mogelijkheid van lex specialis, waar de richtlijn ook in voorziet.

Reikwijdte van de richtlijn
Bij de implementatie van de huidige NIB-richtlijn heeft Nederland ervoor gekozen om bij de aanwijzing van AED's de als vitale aanbieder aangewezen partijen als uitgangspunt te nemen. Dit nieuwe voorstel regelt via centrale aanwijzing welke entiteiten binnen de reikwijdte van de richtlijn vallen, en hiermee wordt aan lidstaten de mogelijkheid ontnomen om zelf te bepalen welke entiteiten essentieel of belangrijk zijn. Dat betekent dat hierdoor in elk geval entiteiten als essentieel of belangrijk zullen worden aangewezen, die in Nederland niet als vitaal zijn beoordeeld. In het geval van essentiële entiteiten staat centrale aanwijzing bovendien op gespannen voet met de uitsluitende verantwoordelijkheid van lidstaten met betrekking tot de bescherming van nationale veiligheid. Tegelijkertijd onderkent het kabinet het belang van een gelijk speelveld voor aanbieders binnen de eengemaakte markt. Het centraal aanwijzen van organisaties die binnen de reikwijdte van de richtlijn vallen draagt hieraan bij. Deze centrale aanwijzing is een belangrijke en complexe afweging, die het kabinet eerst aan de orde wil stellen in het overleg met andere lidstaten. Daarnaast zal het kabinet in de onderhandelingen ook letten op plannen die op gespannen voet staan met de verdragsrechtelijke afspraken betreffende de uitsluitende verantwoordelijkheid van lidstaten op het gebied van nationale veiligheid.

Het kabinet zal verder in de onderhandelingen aandacht vragen voor de proportionaliteit van het voorstel, in het bijzonder met betrekking tot de grote uitbreiding van het aantal aanbieders dat direct onder toepassingsbereik van de richtlijn wordt gebracht. Het kabinet is niet principieel tegen uitbreiding van de reikwijdte met nieuwe sectoren, maar regulering van extra diensten en aanbieders dient pas plaats te vinden na een grondige risicoanalyse, waarin wordt vastgesteld dat het opleggen van verplichtingen noodzakelijk is. Deze verplichtingen dienen ook proportioneel te zijn aan het risico. Het kabinet zal de discussie over de toevoeging van bijlage II met categorieën belangrijke entiteiten die centraal onder de richtlijn worden gebracht dan ook kritisch volgen. Ook zal het kabinet vragen om verdere verduidelijking van de definities in de bijlage, om te kunnen bepalen welke entiteiten onder de reikwijdte van de richtlijn geacht moeten worden te vallen. Niet duidelijk is bijvoorbeeld of universiteiten of onderzoeksinstellingen die hun eigen DNS-diensten beheren ook worden geacht onder het toepassingsbereik van de richtlijn te vallen.

[14] Richtlijn (EU) 2018/1972
[15] Richtlijn (EU) 2018/1972 en Verordening (EU) 910/2014

Verplichtingen van aanbieders

Het kabinet staat overwegend positief tegenover een verdere centrale invulling van de zorgplicht. Een nadere invulling van de zorgplicht draagt bij aan het verhogen van het niveau van digitale veiligheid en een meer gelijkwaardige aanpak binnen de EU. Tegelijkertijd is het van belang dat lidstaten ruimte houden om specifieke maatregelen op te leggen op basis van een risicoanalyse, waar nationale en sectorale omstandigheden in worden meegewogen. Het kabinet is in dit verband van mening dat de Commissie niet zonder instemming van de lidstaten en betrokkenheid van relevante EU-agentschappen extra maatregelen in het kader van de zorgplicht moet kunnen opleggen via gedelegeerde handelingen. Daarnaast vindt het kabinet het aansprakelijk stellen van bestuurders en een bestuursverbod vergaande maatregelen, die juridische bezwaren en bezwaren met betrekking tot proportionaliteit oproepen en waarbij het kabinet sterke twijfels heeft. Ten aanzien van de meldplicht acht het kabinet het van belang dat de uitvoerbaarheid wordt onderzocht, en hoe administratieve lasten hierdoor voor aanbieders zoveel mogelijk kunnen worden beperkt. Tot slot staat het kabinet positief tegenover het aanmoedigen van het melden van incidenten aan opsporingsdiensten indien een vermoeden van zware criminele activiteit bestaat. Een mogelijke rol van Europol en ENISA daarbij moet zorgvuldig worden vormgegeven.

Toezicht

Het kabinet hecht er belang aan dat het toezicht op en handhaving van de naleving van de verplichtingen uit de NIB-richtlijn aansluit bij de Nederlandse regelgeving en toezichtkaders. Toezicht op naleving van de wettelijke verplichtingen dient te voldoen aan de beginselen van goed toezicht en omkleed te zijn met rechtswaarborgen. Bovendien acht het kabinet het van belang dat het toezicht aansluit bij het uitgangspunt dat iedere private en publieke organisatie zelf primair verantwoordelijk is voor zijn eigen digitale beveiliging en in belangrijke mate zelf invulling moet kunnen geven aan de concrete invulling van de vereiste beveiligingsmaatregelen. De regeling in de artikelen 29 tot en met 31 over toezicht en handhaving betreft een tamelijk verstrekkende invulling van de wijze waarop lidstaten in wetgeving de invulling van het toezicht en de handhaving zouden moeten regelen. Daarnaast geldt dat met name bij de in de genoemde artikelen genoemde handhavingsmaatregelen verschillende maatregelen staan opgesomd, die op dit moment niet als zodanig in Nederlandse wetgeving zijn opgenomen en/of vragen oproepen over de precieze betekenis of toegevoegde waarde hiervan. Gelet hierop is het kabinet in algemene zin van oordeel dat de artikelen omtrent toezicht en handhaving in het voorstel te ver gaan, en de invulling van de wettelijke regeling in veel grotere mate aan de nationale wetgever dient te worden overgelaten. Daarnaast acht het kabinet het van belang dat voor verschillende van de nu nog in genoemde artikelen opgenomen bepalingen eerst nader wordt onderbouwd waarom aanvulling hiermee van de regeling in de huidige richtlijn noodzakelijk is.

Het kabinet zal nadere verduidelijking vragen over de wijze waarop het voorstel bepaalt dat de lidstaten verplichtingen moeten opleggen aan organisaties, daarop toezicht moeten houden en de naleving hiervan moeten handhaven. Tevens vraagt het kabinet in relatie tot artikel 24 aandacht voor risico’s die samenhangen met het voorstel dat bepaalde soorten aanbieders onder de

jurisdictie van één lidstaat vallen, in het bijzonder de risico's van *forum shopping* evenals risico's dat de toezichthouder in de betreffende lidstaat een incident mogelijk een lagere prioriteit toekent wanneer de effecten zich grotendeels buiten de eigen lidstaat manifesteren.

Samenwerking tussen autoriteiten
Het kabinet hecht aan een goede samenwerking tussen autoriteiten binnen de EU op het gebied van cybersecurity. Het kabinet verwelkomt dan ook het opnemen van CyCLONe in het voorstel tot herziening van de richtlijn. Het kabinet hecht aan grensoverschrijdende samenwerking tussen toezichthouders en zal in dat verband aandacht vragen voor het belang van een samenwerkingsplatform voor toezichthouders. Daarnaast verwelkomt het kabinet het initiatief om CVD binnen de EU te stimuleren, waar Nederland zich reeds tijdens het EU-voorzitterschap in 2016 voor heeft ingezet. Aangezien er al (internationaal toegankelijke) registers zijn waarin kwetsbaarheden worden geregistreerd, zal het kabinet tijdens de onderhandelingen aangeven te willen waken voor mogelijke versnippering van registratie op verschillende plekken. Het kabinet verwelkomt ook de mogelijkheid tot het opstellen van gecoördineerde sectorale risicobeoordelingen van toeleveringsketens, in lijn met de moties van de leden Van den Berg en Moorlag.[16] Daarnaast onderschrijft het kabinet het belang van het uitwisselen van ervaringen met cybersecuritybeleid (bijv. via peer reviews), maar zal het tijdens de onderhandelingen kritisch zijn op de uitwerking hiervan. Tijdens de onderhandelingen zal het kabinet pleiten voor een structuur van kennisuitwisseling waar leren voorop staat. Tot slot constateert het kabinet dat het voorstel een aantal nieuwe en uitgebreide rapportageverplichtingen bevat voor nationale autoriteiten (zoals de verplichting om ENISA maandelijks te informeren over ontvangen meldingen), en zal het tijdens de onderhandelingen ervoor waken dat er geen onnodige verplichtingen worden opgelegd. Bij het uitwisselen van informatie is het voor het kabinet bovendien van groot belang dat in het kader van de verstrekking van informatie door lidstaten de vertrouwelijkheid van bijvoorbeeld bedrijfsgevoelige informatie zo veel als mogelijk gewaarborgd blijft.

c) Eerste inschatting van krachtenveld
Naar verwachting zullen lidstaten onder meer aandacht vragen voor de samenhang met andere EU-wetgeving, de proportionaliteit en de uitsluitende verantwoordelijkheid van lidstaten op het gebied van nationale veiligheid. Het Europees Parlement zal naar verwachting onder meer aandacht vragen voor de privacyaspecten van het voorstel. Het lid Bart Groothuis is als rapporteur aangewezen door het Europees Parlement.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid
Het kabinet oordeelt ten aanzien van veel onderdelen van de richtlijn positief over de bevoegdheid van de EU om op te treden. De voorgestelde rechtsbasis van het voorstel is artikel 114 VWEU. Op grond van dit artikel kunnen het Europees Parlement en de Raad maatregelen vaststellen inzake de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die

[16] Kamerstukken II 2018-2019, 24 095, nr. 487 en Kamerstukken II 2019-2020, 24 095, nr. 504

de instelling en de werking van de interne markt betreffen. Aangezien het voorstel grotendeels betrekking heeft op de werking van de interne markt, kan het kabinet zich voor deze onderdelen vinden in de voorgestelde rechtsbasis.

Echter wordt de bevoegdheid van de EU voor enkele onderdelen niet zonder meer onderschreven, omdat deze onderdelen op gespannen voet staan met de uitsluitende verantwoordelijkheid van de lidstaten op het gebied van de nationale veiligheid (artikel 4, lid 2, VEU) of omdat niet op voorhand kan worden geconcludeerd dat de bevoegdheid hiervoor in artikel 114 VWEU kan worden gevonden. Dat eerste geldt voor artikel 2 van de richtlijn, meer in het bijzonder de daarin opgenomen vervanging van de aanwijzing van essentiële aanbieders door lidstaten door een centrale aanwijzing van dergelijke aanbieders, waardoor de verplichtingen in de richtlijn direct van toepassing zijn op hen. Van belang is in dat verband dat lidstaten in beginsel zelf kunnen blijven bepalen ten aanzien van welke organisaties geldt dat zij deel uitmaken van de vitale infrastructuur van hun land en dat met het oog daarop aan hen in het kader van de bescherming van de nationale veiligheid maatregelen ter verhoging van hun digitale weerbaarheid worden voorgeschreven. Dezelfde spanning geldt ook voor de in artikel 7 verplicht gestelde elementen van een nationaal crisismanagementplan en de verplichting tot aanwijzing van een of meer nationale autoriteiten voor "management" van crises. Daarnaast geldt specifiek voor het noemen van de categorie overheidsdiensten in de eerste bijlage, en het als gevolg daarvan op hen van toepassing zijn van de verplichtingen in de richtlijn, dat daarvoor niet zomaar een koppeling met het bevorderen van de werking van de interne markt kan worden gemaakt en daarom niet op voorhand kan worden geconcludeerd dat voor deze regeling bevoegdheid bestaat op grond van artikel 114 VWEU. Het kabinet ziet dit laatste daarom graag eerst nader toegelicht. Het kabinet zal deze punten aan de orde stellen tijdens de onderhandelingen.

b) Subsidiariteit

Het kabinet heeft een positief oordeel, met kanttekening over de subsidiariteit. Vanwege de hoge mate van verwevenheid van digitale processen binnen de EU, en de grensoverschrijdende gevolgen van incidenten is een gemeenschappelijke benadering voor een hoog gezamenlijk niveau van cyberbeveiliging noodzakelijk. Deze doelstelling kan onvoldoende worden bereikt door afzonderlijk optreden van de lidstaten, waardoor optreden op EU-niveau gerechtvaardigd is. Bovendien kan een wijziging of intrekking van bestaande EU-regelgeving slechts op EU-niveau plaatsvinden. Wel is het kabinet van mening dat voor de artikelen 29 tot en met 31 geldt dat de richtlijn hiermee in te vergaande mate toezicht en handhaving regelt, en dat de invulling van de wettelijke regeling hiervan in veel grotere mate dan nu wordt toegestaan, aan de nationale wetgever dient te worden overgelaten.

c) Proportionaliteit

Het kabinet heeft een deels positief, deels negatief oordeel over de proportionaliteit. Het kabinet acht de onderdelen van het voorstel die zien op het verbeteren van de samenwerking tussen autoriteiten proportioneel aan het beoogde doel van het voorstel, zoals het verbeteren van de samenwerking tussen lidstaten tijdens een crisis via de oprichting van CyCLONe.

Het kabinet oordeelt negatief over de uitbreiding van de reikwijdte van de richtlijn naar een grote hoeveelheid nieuwe sectoren en aanbieders, de zwaarte van bepaalde verplichtingen (bv. de nadere invulling van zorg- en meldplicht), het toezicht daarop en handhaving daarvan, het aansprakelijk stellen van bestuurders en het opleggen van een bestuursverbod, omdat deze bepalingen in beginsel verder gaan dan noodzakelijk en onvoldoende ruimte laten aan de lidstaten. Voor het uitbreiden van de verplichtingen uit de richtlijn zou uit een grondige analyse moeten blijken dat dit noodzakelijk is, en dat verschillen in nationale regelgeving tot oneerlijke concurrentievoordelen zouden leiden. Voor wat betreft het centraal aanwijzen van, en het als gevolg daarvan automatisch van toepassing laten zijn van de in de richtlijn bedoelde verplichtingen ten aanzien van belangrijke entiteiten in de nieuw toegevoegde sectoren in de tweede bijlage, geldt onder meer dat nog niet uit een evaluatie is gebleken dat meer uniformiteit in het op deze aanbieders van toepassing verklaren van wettelijke verplichtingen noodzakelijk is. Daarnaast is het kabinet van mening dat lidstaten ruimte moeten houden om gedetailleerde invulling te geven aan de zorgplicht, de meldplicht en het aanwijzen van extra aanbieders, om zo rekening te kunnen houden met nationale omstandigheden. Mocht ondanks het onder 4b. hierover gemelde toch tot een verstrekkende regeling van toezicht en handhaving op EU-niveau worden besloten, dan geldt voor het kabinet dat voor verschillende bepalingen in de artikelen over toezicht en handhaving nog in onvoldoende mate vaststaat dat regeling daarvan noodzakelijk is en dat daarom eerst een nadere onderbouwing hiervan gewenst is alvorens hiermee eventueel in te stemmen. Ook is het kabinet in dit verband zeer kritisch over de noodzaak en juridische haalbaarheid van de vergaande bepalingen in de richtlijn over het aansprakelijk stellen van bestuurders en een bestuursverbod. Voor bovengenoemde elementen geldt dat het kabinet om meer verduidelijking van de Commissie zal vragen en hier niet zonder meer mee zal instemmen.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) Consequenties EU-begroting

Naar het oordeel van de Commissie zal het voorstel leiden tot extra uitgaven voor de Commissie en ENISA, ten hoogte van 1,23 miljoen euro per jaar voor de periode 2021-2027. 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 2021-2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting.

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

De financiële gevolgen van het voorstel voor de rijksoverheid zijn op dit moment nog niet te specificeren, maar zijn naar verwachting substantieel. Door de uitbreiding van het aantal organisaties dat onder de richtlijn valt (en daarmee binnen de doelgroep van een CSIRT en onder toezicht van een toezichthouder), en de uitbreiding van de taken van nationale autoriteiten en rapportageverplichtingen, zal dit voorstel financiële consequenties hebben voor verschillende overheidsorganisaties, waaronder het NCSC en toezichthouders. Daarnaast is het mogelijk dat (decentrale) overheidsorganisaties door de uitbreiding van de sectoren in de annex zelf onder de richtlijn komen te vallen. Op basis van het impact assessment schat de Commissie een toename van 20-30% overheidsinvesteringen, bovenop de huidige investeringen in cybersecurity in het

kader van de NIB-richtlijn. Vanwege de relatief lage hoeveelheid aanbieders die in Nederland als AED zijn aangewezen krachtens de Wbni zal dit voor Nederland naar verwachting een relatief grote toename zijn. Eventuele budgettaire gevolgen voor de Rijksbegroting worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

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

In het impact assessment geeft de Commissie aan te rekenen op een initiële verhoging van maximaal 22% van het ICT-budget verwacht in de eerste periode (3-4 jaar) voor bedrijven die nog niet onder de NIB-richtlijn vallen. Voor bedrijven die wel al onder de huidige NIB-richtlijn vallen schat de Commissie in dat dit 12% zal zijn.

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

Het voorstel zal leiden tot een verhoging van administratieve lasten voor Rijksoverheid, decentrale overheden en het bedrijfsleven. Deze administratieve lasten bestaan uit het opleggen van verplichtingen via de zorg- en meldplicht voor organisaties die onder de richtlijn vallen (zowel publiek als privaat). Deze verplichtingen worden met dit voorstel groter, en zullen daarnaast aan meer organisaties worden opgelegd. Voor nationale autoriteiten geldt er een toename van het aantal rapportageverplichtingen.

e) Gevolgen voor concurrentiekracht

Vanwege de harmonisatie van maatregelen leidt het voorstel naar verwachting van de Commissie tot een gelijker speelveld voor bedrijven binnen de EU. Organisaties die onder de richtlijn vallen krijgen naar verwachting wel te maken met toegenomen ICT-investeringen. De inschatting van de Commissie is dat dit opweegt tegen de concurrentievoordelen als gevolg van de positieve effecten van een hoger niveau van cyberbeveiliging.

6. Implicaties juridisch

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

Het voorstel vergt een grondige aanpassing van nationale wetgeving (in de eerste plaats de Wbni) en heeft daarvoor dus grote consequenties.

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan

Het kabinet staat in beginsel positief tegenover het voorstel van de Commissie om aan de Commissie in een aantal artikelen (nl. artikel 12, zevende lid; artikel 18, vijfde lid; artikel 20, elfde lid, eerste volzin) de bevoegdheid te verlenen om uitvoeringshandelingen vast te stellen ter nadere uitwerking van de richtlijn. In artikel 12, zevende lid, krijgt de Commissie de bevoegdheid door middel van uitvoeringshandelingen een procedurele regeling vast te stellen over het functioneren van de NIB Samenwerkingsgroep. Dit betreft een niet-essentieel onderdeel van de regeling, maar een procedurele regeling ter vergemakkelijking van het functioneren van de NIB

Samenwerkingsgroep. De keuze voor een uitvoeringshandeling ligt hierbij juridisch dan ook voor de hand, omdat deze handelingen waarborgen dat de richtlijn in alle lidstaten volgens eenvormige voorwaarden wordt uitgevoerd. Ook ligt de keuze voor de onderzoeksprocedure in de zin van artikel 5 van Verordening (EU) nr. 182/2011 voor de hand, omdat het de vaststelling van uitvoeringshandelingen van algemene strekking betreft in de zin van artikel 2, lid 2, sub a van Verordening (EU) nr. 182/2011. Hiermee kan dan ook vastgesteld worden dat Verordening (EU) nr. 182/2011 goed wordt nageleefd. Deze overwegingen zijn eveneens van toepassing op artikel 18, vijfde lid, waarin de Commissie de bevoegdheid krijgt om door middel van uitvoeringshandelingen technische en methodologische specificaties vast te stellen met betrekking betreffende de maatregelen genoemd onder lid 2, evenals artikel 20, elfde lid, eerste volzin, waarin de Commissie de bevoegdheid krijgt om door middel van uitvoeringshandelingen het soort informatie, het format en de procedure van een incidentennotificatie met significante impact vast te stellen.

Daarnaast wordt in het voorstel de Commissie de bevoegdheid toegekend om via uitvoeringshandelingen de gevallen waarin een incident als significant en daarmee meldplichtig wordt beschouwd nader te specificeren (artikel 20, lid 11, tweede volzin), via gedelegeerde handelingen aanvullingen vast te stellen op de maatregelen die in het kader van de zorgplicht genomen dienen te worden(artikel 18, lid 6) en handelingen vast te stellen waarin wordt bepaald welke categorieën van essentiële entiteiten verplicht zijn een cyberbeveiligingscertificaat te verkrijgen (artikel 21, lid 2). Toekenning van bevoegdheden aan de Commissie is juridisch niet mogelijk als het gaat om essentiële onderdelen van de regelgeving. Deze moeten in de wetgevingshandeling zelf worden uitgewerkt. Het kabinet is daarom kritisch over de bevoegdheidsverlening in de hiervoor genoemde artikelen, aangezien hiermee volgens het kabinet essentiële onderdelen van de richtlijn worden geregeld. Voor de eerste twee van die artikelen geldt namelijk dat de daarin bedoelde nadere regeling door de Commissie betrekking heeft op een uitbreiding van de omvang van de eerder in die artikelen opgenomen belangrijke verplichtingen (zorgplicht, meldplicht) ten aanzien van essentiële en belangrijke entiteiten, die mede vanwege dat verplichtende karakter als essentiële onderdelen van regelgeving dienen te worden aangemerkt en ook als zodanig in de richtlijn zijn opgenomen. Uitbreiding van de materiële reikwijdte van deze verplichtingen is daarmee ook een essentieel onderdeel van regelgeving en dient daarom niet op een lager niveau dan dat van richtlijn plaats te vinden. Het kabinet plaatst daarnaast vraagtekens bij artikel 21, tweede lid, omdat dit strekt tot het voor essentiële entiteiten kunnen vaststellen van verplichte certificering en dit gelet op het zwaarwegende karakter van deze certificering eveneens een essentieel onderdeel van regelgeving lijkt te zijn dat zich niet zonder meer leent voor regeling door de Commissie.

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

De door de Commissie voorgestelde termijn van achttien maanden is voor Nederland, gelet op de benodigde grote wijzigingen van regelgeving, maar ook vanwege de inrichting van bijvoorbeeld toezicht op nieuwe categorieën aanbieders, niet haalbaar. Mede gelet op de met de implementatie

van de huidige richtlijn nodig gebleken tijdsperiode wordt in plaats hiervan aangedrongen op een termijn van ten minste vierentwintig maanden.

d) Wenselijkheid evaluatie-/horizonbepaling
De Commissie evalueert de werking van deze richtlijn periodiek en brengt daarover verslag uit aan het Europees Parlement en de Raad (artikel 35). Het kabinet is positief over het voornemen om de werking van de richtlijn periodiek te evalueren.

e) Constitutionele toets
Vooralsnog geen opmerkingen

7. Implicaties voor uitvoering en/of handhaving

a) Uitvoerbaarheid
Het kabinet verwacht, gezien de uitbreiding van het aantal sectoren en van organisaties in zowel oude als nieuwe sectoren die onder het toepassingsbereik van de richtlijn vallen, een significante toename van het aantal organisaties waarvoor een CSIRT dient te worden aangewezen. Zonder evenredige toename van capaciteit bij CSIRTs betekent dit dat er verder geprioriteerd moet worden binnen het verlenen van CSIRT-diensten.

Het NCSC voert de CSIRT-taken uit de huidige NIB-richtlijn uit voor AED's; het CSIRT voor digitale diensten doet dit voor DSP's. De categorie DSPs verdwijnt als afzonderlijke categorie, maar de aanbieders daarbinnen blijven binnen de reikwijdte van de richtlijn en worden verdeeld worden over de categorieën essentieel en belangrijk. Voor essentiële en belangrijke entiteiten zal een CSIRT moeten worden aangewezen, die de taken uit de richtlijn voor deze entiteiten zal uitvoeren. Het melden van incidenten waarbij het vermoeden bestaat van zware criminele activiteit kan tot een toename van opsporingsonderzoeken leiden.

In het voorstel worden essentiële en belangrijke entiteiten (met uitzondering van kleine en micro-ondernemingen) centraal als zodanig aangemerkt. Krachtens de huidige richtlijn is een aanwijzing als AED door de lidstaten zelf vereist, waarbij aanbieders op de hoogte worden gesteld van hun aanwijzing. Nationale autoriteiten zullen op basis van de omschrijving van de entiteiten in de bijlagen én de uitzondering voor kleine en micro-ondernemingen (omzet en aantal werknemers) moeten bepalen welke aanbieders onder het toepassingsbereik van de richtlijn worden geacht te vallen, wat mogelijk risico's oplevert voor de uitvoerbaarheid. Daarnaast kunnen bovengenoemde indicatoren ook fluctueren, en moet er dus periodiek een nieuwe inschatting worden gemaakt. Ook aanbieders zelf zullen telkens zelf de inschatting moeten maken of de verplichtingen in de richtlijn op hen van toepassing zijn.

b) Handhaafbaarheid
De hierboven geconstateerde gevolgen voor de capaciteiten van nationale autoriteiten en de uitvoerbaarheid van de richtlijn als gevolg van de wijziging van de manier van aanwijzing en de toename van het aantal organisaties dat onder de richtlijn valt, heeft ook gevolgen voor de

capaciteit van toezichthouders en de handhaarbaarheid. Met betrekking tot het toezicht is een verschil aangebracht in toezicht en handhaving van essentiële en belangrijke entiteiten, waarbij op de eerste categorie proactief (ex-ante) en de laatste reactief (ex-post) toezicht wordt uitgeoefend. Het is de verwachting dat door dit verschil de toezichtslast op belangrijke entiteiten van beperktere omvang zal zijn. Het kabinet zal aandacht vragen voor het belang van een risico- en informatiegestuurde aanpak in het toezicht alsmede het belang voor het delen en afstemmen van toezichtsbeleid tussen toezichthouders in de verschillende lidstaten.

8. Implicaties voor ontwikkelingslanden

Geen implicaties voor ontwikkelingslanden.