Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

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

Nr. 2705 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 oktober 2018

Overeenkomstig de bestaande afspraken ontvangt u hierbij 10 fiches, die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC).

Fiche: Verordening tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra
Fiche: Verordening ter voorkoming van de verspreiding van online terroristische inhoud (Kamerstuk 22 112, nr. 2706)
Fiche: Mededeling voorstel uitbreiding bevoegdheden EOM (Kamerstuk 22 112, nr. 2707)
Fiche: Pakket vrije en eerlijke verkiezingen (Kamerstuk 22 112, nr. 2708)
Fiche: Richtlijn betreffende het einde van de omschakeling tussen winter- en zomertijd (Kamerstuk 22 112, nr. 2709)
Fiche: Mededeling Versterking van het Uniekader voor prudentieel en antiwitwastoezicht voor financiële instellingen (Kamerstuk 22 112, nr. 2710)
Fiche: Gewijzigd voorstel tot aanpassing van de verordeningen m.b.t. de Europese Toezichthoudende Autoriteiten en tot wijziging van de vierde anti-witwasrichtlijn (Kamerstuk 22 112, nr. 2711)
Fiche: Mededeling nieuwe Afrikaans-Europese alliantie voor duurzame investeringen en banen (Kamerstuk 22 112, nr. 2712)
Fiche: Mededeling Naar een doeltreffendere financiële architectuur voor investeringen buiten de EU (Kamerstuk 22 112, nr. 2713)
Fiche: Mededeling over efficiëntere besluitvorming in het GBVB (Kamerstuk 22 112, nr. 2714)

De Minister van Buitenlandse Zaken,
S.A. Blok

kst-22112-2705
ISSN 0921 - 7371
's-Gravenhage 2018

Fiche: Verordening voor oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra.

1. Algemene gegevens

a) *Titel voorstel*
Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra.
b) *Datum ontvangst Commissiedocument*
12 september 2018
c) *Nr. Commissiedocument*
COM (2018)630
d) *Eur-Lex*
https://eurlex.Europa.eu/search.html?qid=1537345045676&PROC_NUM=0328&DB_INTER_CODE_TYPE=OLP&type=advanced&PROC_ANN=2018&lang=nl
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
SWD (2018) 403
f) *Behandelingstraject Raad*
Telecomraad
g) *Eerstverantwoordelijk ministerie*
Ministerie van Economische Zaken in nauwe samenwerking met Justitie & Veiligheid
h) *Rechtsbasis*
Artikel 173 (3) VWEU en Artikel 188 (1) VWEU
i) *Besluitvormingsprocedure Raad*
Gekwalificeerde meerderheid
j) *Rol Europees Parlement*
Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Het voorstel heeft als doel om meer coördinatie, efficiëntie en schaalvoordelen te bewerkstelligen in investeringen gedaan binnen de EU en EU Lidstaten op het gebied van cybersecuritykennis en – innovatie. Zo moet worden bereikt dat de Europese cybersecurityindustrie en kennis versterkt wordt en wereldwijd competitief, en dat Europa minder afhankelijk wordt van niet-EU-producten en diensten. Er wordt voorgesteld dit te doen door het creëren van één EU Cybersecurity Competence Centre (EUCCC), dat verantwoordelijk wordt voor het coördineren en stroomlijnen van de EU inzet op cybersecurity. Ook wordt dit de centrale plek in de EU via welke EU-fondsen geoormerkt voor cybersecurity zullen worden toegekend. Dit gaat in bijzonder over de gelden uit het Digital Europe programma en het nieuwe Horizon Europe programma. Het EUCCC wordt voorgesteld als een Europees Partnerschap, waardoor gezamenlijke investeringen van de Unie, Lidstaten en de industrie worden gefaciliteerd. In het voorstel wordt voor het EUCCC ook een rol gezien wat betreft advisering van overheden en bedrijven over (inkoop van) cybersecurity oplossingen.

In het voorstel worden de Lidstaten verplicht om een «Nationaal Coördinatie Centrum» voor te dragen. Dit centrum moet op nationaal niveau banden aanhalen tussen de publieke en private sector wat betreft onderzoek, innovatie en kennisontwikkeling. Ook hebben de nationale

centra een rol in het uitzetten en monitoren van EU-projectgelden. De nationale centra worden geacht op basis van contractuele afspraken samen te werken met het EUCCC. Een van de taken van de EUCCC zal ook zijn om synergie te zoeken tussen civiele en militaire technologieën en toepassingen, evenals in voorkomend geval optreden als manager voor projecten, die gefinancierd worden vanuit het Europese Defensie Fonds.

Als laatste beoogt het voorstel om een Cybersecurity Competence Community te creëren. De leden hiervan (publiek, privaat en wetenschap) worden geacht de opbrengsten en kennis uit cybersecurityonderzoek en -projecten uit te dragen. Lidmaatschap zal worden verleend op basis van accreditatie. De gelden die men via de nieuwe structuur wil besteden zullen voor de helft uit EU-fondsen komen. Voor de andere helft vraagt de Commissie om een vrijwillige bijdrage van de Lidstaten. De Commissie stelt voor om de EU bijdragen vooral te laten komen uit de nieuwe Digital Europe en Horizon Europe programma's.

b) Impact assessment Commissie

In haar impact analyse gaat de Commissie nader in op de verschillende opties om de huidige problemen op het gebied van cybersecurity binnen de Unie aan te pakken. Er is gekozen om een Cybersecurity Netwerk te creëren met in het hart van het netwerk een EU Cybersecurity Competence Centre (EUCCC) om zowel de Europese industrie als onderzoek en innovatie te stimuleren. Deze aanpak kwam van de drie onderzochte opties als meest geschikt naar voren om de door de EC genoemde problemen op het gebied cybersecurityonderzoek en innovatie in Europa aan te pakken.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Het kabinet zet samen met zijn internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering de economie en samenleving biedt worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd. De concrete uitwerking van deze visie is vastgelegd in de Nederlandse Digitaliseringsstrategie, die aansluit bij de Digitale interne marktstrategie en de Nederlandse Cyber Security Agenda. Om kennis op het gebied van cybersecurity te ontwikkelen en te versterken, is samen met de overheid, bedrijfsleven en kennisinstellingen onder coördinatie van het platform Dcypher een derde editie van de Nationale Cyber Security Agenda gepubliceerd (op 5 juni jl.), met als doel te komen tot een gezamenlijk meerjarige onderzoekagenda op het gebied van cybersecurity in Nederland.
Op nationaal niveau wordt momenteel een verkenning verricht in opdracht van het Ministerie van EZK. Er wordt verkend hoe verschillende initiatieven, trajecten en instrumenten met betrekking tot cybersecurityonderzoek beter op elkaar aan kunnen sluiten.

b) beoordeling + inzet ten aanzien van dit voorstel

Het voorstel is aangekondigd in de Mededeling van de Commissie uit september 2017, dat een aantal maatregelen op het gebied van cybersecurity bevat. Nederland was in brede zin positief over dit cybersecuritypakket, omdat Nederland de daarin door de Commissie gesignaleerde dreigingen en risico's kan onderschrijven. Een aantal daarvan kan het best op EU-niveau worden opgepakt.

De noodzaak voor meer EU-capaciteit, kennis en kunde op cybersecurity-gebied wordt ook door Nederland onderschreven. Het doel van het voorstel om middelen te prioriteren ten behoeve van cybersecurity past daarmee bij de Nederlandse prioriteiten. Nederland is het met de Commissie eens dat er economische en maatschappelijke voordelen kunnen worden gehaald als over cybersecurity-investeringen meer en beter wordt afgestemd tussen de EU en EU Lidstaten en tussen publiek, privaat en wetenschap (triple helix).

Nederland zal er daarbij wel op letten dat er geen overbodige overhead, bureaucratie en structuren in het leven worden geroepen, maar zal vooral inzetten op het benutten en verbeteren van bestaande structuren om zo de gewenste versterking van het beleid op het gebied van cybersecurity te bereiken. Allereerst is hier de relatie met de NAVO van belang, in het bijzonder een Cyber Center of Excellence van de NAVO in Tallinn, Estland. Daarnaast zal Nederland het gesprek aangaan met de Commissie en in de Raad over de voor- en nadelen van de voorgestelde nieuwe structuur en het nieuwe centrum, ook in relatie tot bestaande organisaties zoals het Joint Research Centre van de Commissie. Voor wat betreft het nationale niveau, is het kabinet er tevreden over dat de Verordening de Lidstaten in staat stelt om een al bestaande instelling hiervoor aan te wijzen.
Ook is het van belang dat Lidstaten, en ook de private sector en wetenschap, hun eigen ruimte houden qua ontwikkeling van eigen economie, innovatie en arbeidsmarkt en daarbij rekening houdend met de verschillende expertisegebieden die bij kennisinstellingen bestaan. De activiteiten van het EUCCC zullen daarom vooral complementair dienen te zijn aan de activiteiten en faciliteiten, die in de lidstaten al bestaan.

Het EUCCC zal worden aangestuurd door een Governing Board. In artikel 15, lid 3 stelt de Commissie dat beslissingen zullen worden genomen door 75% van de stemgerechtigden, maar tevens dienen zij 75% van de financiële bijdragen te representeren. Daarmee worden grote financiers in een wezenlijk andere positie gezet dan kleinere. De Commissie dient dit mechanisme verder te verduidelijken. De Nederlandse inzet wat betreft de lopende MFK-onderhandelingen zullen ook bij de verdere bespreking van dit voorstel als leidraad dienen. Nederland zal in het kader van de komende onderhandelingen specifiek meer uitleg vragen over het voorgestelde mechanisme van vrijwillige financiering van de Lidstaten, en wat de Commissie voorziet als die bijdrages niet voldoen aan de verwachtingen en onvoldoende zijn om het beoogde Competence Centre te financieren.

In relatie tot de lopende MFK-onderhandelingen zal de inhoudelijke en, mogelijk, financiële relatie tussen het EUCCC en Horizon Europe worden benadrukt. Een inclusieve en veilige maatschappij is een van de vijf mondiale uitdagingen binnen de tweede pijler van Horizon Europe. In het BNC-fiche Horizon Europe heeft Nederland de zorgen uitgesproken over de breedte aan onderwerpen die de Commissie voorstelt voor deze, in financiële termen, kleinste mondiale uitdaging. Deze zorgen betreffen zowel de drie onderwerpen waarin veiligheid centraal staat (bijvoorbeeld cybersecurity) als de drie onderwerpen waarin inclusie centraal staat (bijvoorbeeld democratie). Een eventuele financiële bijdrage van Horizon Europe aan onderzoek dat door EUCCC wordt geprogrammeerd, dient proportioneel te zijn, volledig in overeenstemming te zijn met de doelstellingen van Horizon Europe (met name excellentie en impact) en dient niet ten koste te gaan van het budget voor onderzoek naar een inclusieve maatschappij.

c) Eerste inschatting van krachtenveld

In lijn met de Nederlandse positie bestuderen de EU-lidstaten het voorstel. Er lijkt steun voor de doelen van dit voorstel wat betreft het belang van meer onderzoek naar cybersecurity-innovatie en -kennisontwikkeling. Daarnaast zijn er wel vragen over de manier waarop de Commissie voorstelt dit doel te bereiken. De voorgestelde structuur en het bijbehorende stemmechanisme worden als (onnodig) complex ervaren. Ook de cofinanciering zoals die wordt voorgesteld door de Commissie roept vragen bij de Lidstaten op.

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

De voorgestelde rechtsgrondslag wordt gevormd door de artikelen artikel 173 lid 3 en artikel 187 VWEU. Op basis van artikel 173 lid 3, VWEU is de EU bevoegd om maatregelen te nemen op het terrein van de versterking van het concurrentievermogen van de Europese industrie en op basis van artikel 187 is de EU bevoegd om voorstellen ten aanzien van onderzoek en innovatie.
Het kabinet kan zich, gezien de specifieke verschillende doelstellingen van het kenniscentrum vinden in de keuze voor deze dubbele rechtsgrondslag. De voorziene activiteiten van het kenniscentrum zien enerzijds op onderzoek en ontwikkeling en anderzijds op het ondersteunen van de marktintroductie van cyberbeveiligingsproducten en het helpen versterken van het concurrentievermogen en het marktaandeel van de Europese cyberbeveiligingsbranche.

b) Subsidiariteit

Het Kabinet beoordeelt de subsidiariteit als positief. Gezien de aard en de omvang van de technologische uitdagingen op het gebied van cyberbeveiliging, en aangezien de inspanningen in het bedrijfsleven, de overheidssector en de onderzoekgemeenschappen, alsook tussen deze sectoren onderling, onvoldoende worden gecoördineerd, moet de EU de coördinatie-inspanningen verder ondersteunen, zowel om een kritische massa aan middelen bijeen te brengen als om een beter beheer van kennis en activa te garanderen. Nederland tekent hierbij aan dat EU-beleid en EU-investeringen in onderzoek en innovatie nog altijd een aanvulling zijn op, en geen vervanging voor, nationaal beleid en publieke en private investeringen door de lidstaten.

c) Proportionaliteit

De Nederlandse beoordeling van de proportionaliteit is positief met een kanttekening, omdat de oprichting van een EUCCC en het bijbehorende Netwerk van Nationale Centra een goed mechanisme kan zijn om effectief coördinatie te realiseren. Wel dient de Commissie een aantal zaken te verduidelijken, zoals de voorgestelde aansturing van het programma en hoe het voorstel aansluit op bestaande structuren op Europees niveau en in de lidstaten. Hierbij dient onder andere de relatie met Horizon Europe te worden verduidelijkt. Ook dienen de reikwijdte en verantwoordelijkheden van het EU Cybersecurity Competence Centre voldoende duidelijk en afgebakend te zijn op kennisontwikkeling en innovatie. Indien aan deze voorwaarden niet wordt voldaan dan is het voorgestelde EUCCC naar de mening van het Kabinet niet het geschikte middel om de gestelde doelen te bereiken.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) Consequenties EU-begroting

De financiële middelen die nodig zijn in het kader van het voorstel zullen voornamelijk komen vanuit de nieuwe programma's Digital Europe en Horizon Europe met looptijd van 2021–2027.
In het voorstel zelf is opgenomen dat uit het programma Digital Europe ruim 2 miljard EUR voor dit voorstel wordt bestemd. Daarnaast zou budget uit het Horizon Europe programma kunnen worden toegevoegd, c.q. zou het EUCCC invloed kunnen hebben op de programmering van het security-onderzoek in Horizon Europe maar dit is op dit moment in het voorstel nog opengelaten. Op dit punt dient de Commissie duidelijkheid te verschaffen over het voorstel. Het Horizon Europe voorstel gaat uit van 2,8 miljard EUR voor een zestal onderwerpen voor onderzoek en innovatie om de uitdaging van een inclusieve en veilige maatschappij aan te pakken. Bij drie onderwerpen ligt de nadruk op inclusie; bij drie onderwerpen ligt de nadruk op veiligheid. In de discussies over Horizon Europe ligt de optie op tafel om het cluster inclusieve en veilige maatschappij inhoudelijk en financieel te splitsen.

Zoals vastgelegd in de Kamerbrief van 1 juni 2018 over de Kabinetsappreciatie van het Commissie MFK-voorstel, maken de onderhandelingen over de toekomst van Digital Europe en Horizon Europe voor wat betreft de financiële aspecten, integraal onderdeel uit van de onderhandelingen over het Meerjarig Financieel Kader (MFK) 2021–2027. Nederland hecht eraan dat besprekingen over Digital Europe en Horizon Europe niet vooruitlopen op de integrale besluitvorming betreffende het MFK. De beleidsmatige inzet van Nederland bij de Digital Europe en Horizon Europe zal ondersteunend moeten zijn aan de Nederlandse inzet in de MFK-onderhandelingen zoals hierboven toegelicht, te weten een ambitieus gemoderniseerd en financieel houdbaar MFK. Dit vraagt scherpe keuzes, én bezuinigingen. Om het vertrek van het Verenigd Koninkrijk op te kunnen vangen en nieuwe prioriteiten te kunnen financieren moeten substantiële bezuinigingen worden doorgevoerd. Binnen dit kader blijft vanzelfsprekend de ruimte bestaan om op de inhoud actief in te spelen op het verloop van de onderhandelingen.

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

Aangezien de Commissie uitgaat van cofinanciering door de Lidstaten (artikel 22 lid1) kunnen de lidstaten gezamenlijk een vergelijkbare bijdrage leveren als de Unie in de operationele en administratieve kosten van het EUCCC. Conform artikel 23 lid 3 zullen deze middelen komen uit financiële contributies of in voorkomend geval in bijdragen in-kind. De budgettaire gevolgen worden ingepast op de begroting van het/de beleidsverantwoordelijk (e) departement(en), conform de regels van de budgetdiscipline.

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

Vermoedelijk kunnen bedrijven en burgers financieel voordeel hebben van producten en diensten op het gebied van cybersecurity, die minder kosten dan zonder de Europese samenwerking.

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

Vooralsnog geen gevolgen voor regeldruk/administratieve lasten. Indien het EUCCC wordt opgericht dient dit nader te worden bezien.

e) Gevolgen voor concurrentiekracht

Positief. Het is de bedoeling dat met het voorstel de ontwikkeling van een Europese cybersecurityindustrie wordt bevorderd. Dit is een industrie, die op wereldschaal snel groeit. Ook de Nederlandse industrie kan hiervan profiteren.

6. Implicaties juridisch

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

Vooralsnog valt niet te verwachten dat dit gevolgen zal hebben voor nationale of decentrale regelgeving. Dit kan echter pas met zekerheid worden bezien, zodra meer bekend is over de activiteiten die uit EUCCC en Nationale Coördinatie Centra voortvloeien. Met de verordening worden de oprichting van een EUCCC en Nationale Coördinatie Centra voorzien. Deze Centra zijn als gevolg van het voorstel bevoegd financiële steun aan derden te verlenen/door te geven. Bij de uitwerking zal moeten worden bezien in hoeverre dit onderdeel raakt aan het Nederlandse subsidie- en bestuursrecht.

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

Niet van toepassing

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

Voorzien is dat de Verordening per 1 januari 2021 in werking treedt. Voor die tijd zal in Nederland een Nationaal Coördinatie Centrum voor cybersecurity moeten worden aangewezen. Aangezien er in Nederland middels de eerdergenoemde verkenning al wordt gewerkt aan betere coördinatie tussen de verschillende betrokken partijen zou dat haalbaar moeten zijn.

d) Wenselijkheid evaluatie-/horizonbepaling

Artikel 38 van het voorstel bevat de monitoring, evaluatie en review van het voorstel. Artikel 46, lid 1 bepaald de looptijd van het EUCCC van 1 januari 2021 tot en met 31 december 2029. Tenzij op basis van een review anders wordt besloten (artikel 46, lid 2).

7. Implicaties voor uitvoering en/of handhaving

Er zal in Nederland een Nationaal Coördinatie Centrum moeten worden aangewezen, die zich met de uitvoering zal bezighouden.

8. Implicaties voor ontwikkelingslanden

Geen gevolgen voor ontwikkelingslanden