Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

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

Nr. 2854 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal»

Den Haag, 6 maart 2020

Overeenkomstig de bestaande afspraken ontvangt u hierbij 1 fiche dat werd opgesteld door de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC).

Fiche: Mededeling implementatie EU 5G toolbox

De Minister van Buitenlandse Zaken,
S.A. Blok

kst-22112-2854
ISSN 0921 - 7371
's-Gravenhage 2020

Fiche: Mededeling implementatie EU 5G toolbox

1. Algemene gegevens

a) *Titel voorstel:*
Mededeling uitrol van beveiligde 5G in de EU – uitvoering van de EU-toolbox
b) *Datum ontvangst Commissiedocument:*
29 januari 2020
c) *Nr. Commissiedocument:*
COM(2020) 50
d) *EUR-Lex:*
https://eur-lex.europa.eu/legal- content/EN/TXT/?qid=1581335197295&uri=CELEX:52020DC0050
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing:*
Niet opgesteld
f) *Behandelingstraject Raad*
Raad vervoer, telecommunicatie en energie (telecom)
g) *Eerstverantwoordelijk ministerie*
Ministerie van Economische Zaken en Klimaat, Ministerie van Justitie en Veiligheid

2. Essentie voorstel

De mededeling geeft nadere invulling aan de uitvoering van de EU toolbox voor 5G cybersecurity. Zowel de mededeling als de toolbox zijn op 29 januari 2020 gepubliceerd.

In de eerdere aanbeveling Cyberbeveiliging van 5G-netwerken van 26 maart 2019[1] werd een proces aangekondigd ten behoeve van de toolbox, waaronder het uitvoeren van nationale risicobeoordelingen. Op basis van deze risicobeoordelingen betreffende de cyberbeveiliging van 5G netwerken is een gecoördineerde EU-risicobeoordeling opgesteld, die op 9 oktober 2019 is gepubliceerd. De toolbox vloeit voort uit deze gecoördineerde EU-risicobeoordeling. Deze toolbox is ontwikkeld door de Samenwerkingsgroep voor Netwerk- en Informatiebeveiliging (NIB Samenwerkingsgroep). In de NIB Samenwerkingsgroep zitten vertegenwoordigers van de lidstaten samen met de Commissie en het Europese Agentschap voor Netwerk- en Informatiebeveiliging (Enisa).[2]

De mededeling bevat een overzicht van de inhoud van zowel de eerder gepubliceerde gecoördineerde EU-risicobeoordeling en van de conclusies van de toolbox. De Commissie steunt in deze mededeling de conclusies van de toolbox. Daarnaast roept de Commissie de lidstaten op tot snelle invoering van een doeltreffende en passende risicobeperkende aanpak die in lijn is met deze toolbox. Hierbij dient rekening te worden gehouden met nationale omstandigheden. Ook roept de Commissie op om alle noodzakelijke verdere stappen te ondernemen om de coördinatie op EU-niveau te waarborgen.

De Commissie verzoekt in dat kader de lidstaten om uiterlijk 30 april 2020 concrete en meetbare stappen te zetten om de in de conclusies van de toolbox aanbevolen reeks kernmaatregelen te nemen. Ook vraagt de Commissie de lidstaten om op uiterlijk 30 juni 2020 in de

[1] COM (2019) 2335
[2] De gecoördineerde risicobeoordeling en de toolbox zijn ten tijde van publicatie aan u aangeboden: Kamerbrief EU 5G risicobeoordeling (Kamerstuk 21 501-33, nr. 781) en Kamerbrief over 5G (Kamerstukken 24 095 en 30 821, nr. 495)

NIB-Samenwerkingsgroep een verslag op te stellen van de nationale uitvoering van deze kernmaatregelen in elke lidstaat.

De toolbox geeft een reeks strategische en technische maatregelen, alsmede ondersteunende acties ter versterking van de doeltreffendheid, die de vastgestelde risico's van 5G kunnen beperken. In de conclusies van de toolbox wordt aanbevolen dat alle lidstaten moeten zorgen dat zij over maatregelen beschikken (waaronder ook bevoegdheden voor nationale autoriteiten) om op passende wijze en proportioneel te reageren op bekende en toekomstige risico's. De lidstaten moeten er met name voor zorgen dat zij de levering, uitrol en exploitatie van 5G-netwerkapparatuur kunnen beperken, verbieden en/of er specifieke eisen of voorwaarden aan kunnen verbinden. Dit moet aan de hand van een risico gebaseerde benadering en op grond van een reeks veiligheid gerelateerde redenen.

Ook wordt in deze conclusies aanbevolen dat alle lidstaten moeten zorgen voor aangescherpte beveiligingseisen voor exploitanten van mobiele netwerken. Er wordt aanbevolen dat de lidstaten relevante beperkingen vaststellen voor leveranciers die mogelijk een hoog risico vormen voor essentiële activa, die als kritiek en gevoelig zijn gedefinieerd in de gecoördineerde risicobeoordeling. Tot slot wordt aanbevolen dat lidstaten zorgen dat exploitanten een passende bedrijfsstrategie opstellen om verregaande afhankelijkheid van individuele leveranciers te voorkomen of te beperken en afhankelijkheid van leveranciers die mogelijk een hoog risico vormen, te vermijden.

De Commissie schetst in deze mededeling daarnaast een aantal risicobeperkende maatregelen uit de toolbox die onder de bevoegdheid van de Unie vallen. Dit zijn maatregelen waarop de Commissie reeds actie onderneemt of nog zal gaan ondernemen. Doel van deze maatregelen is bij te dragen aan de technologische soevereiniteit van de EU en het leiderschap van de EU op het gebied van netwerk- en cyberbeveiligingstechnologie. Het gaat hier onder meer om acties zoals verdere samenwerking voor cyberbeveiliging, mogelijk aanvullende telecom- en cyberbeveiligingsregels, certificering, screening van buitenlandse directe investeringen, handelsbeschermingsinstrumenten, crisisrespons en -beheersing en een kader voor diplomatieke respons op kwaadwillige cyberactiviteiten.

3. Nederlandse positie ten aanzien van de mededeling/aanbeveling

a) Essentie Nederlands beleid op dit terrein

De Nederlandse Cyber Security Agenda uit 2018[3] zet de beleidsprioriteiten voor cybersecurity uiteen. Gezien het inherente grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging staan Europese en internationale samenwerking in de Nederlandse aanpak centraal. Binnen de EU zet Nederland zich met betrekking tot cybersecurity onder meer in op uitwisseling van informatie in de NIB-samenwerkingsgroep.

Zoals ook in de Kamerbrief van 1 juli 2019[4] is vermeld, is onder leiding van de Nationaal Coördinator Terrorismebestrijding en Veiligheid een interdepartementale Taskforce Economische Veiligheid opgericht. Deze Taskforce heeft met medewerking van de drie grote telecomaanbieders in

[3] Aanbiedingsbrief Nederlandse Cyber Security Agenda (Kamerstuk 26 643, nr. 536)
[4] Maatregelen bescherming telecomnetwerken en 5G, brief van de Minister van Justitie en Veiligheid en de Staatssecretaris van Economische Zaken en Klimaat van 1 juli 2019 aan de Tweede Kamer (Kamerstuk 30 821, nr. 92)

Nederland (KPN, T-Mobile en VodafoneZiggo) een nationale risicoanalyse uitgevoerd naar de kwetsbaarheid van telecommunicatienetwerken voor misbruik van leveranciers van technologie voor deze netwerken en geadviseerd welke aanvullende maatregelen nodig zijn om risico's voor de veiligheid en integriteit van de netwerken te beheersen.

De basis voor de beveiligingsmaatregelen, zoals die naar aanleiding van de rapportage van de Taskforce zijn aangekondigd in bovengenoemde brief van 1 juli 2019, wordt inmiddels gevormd door het Besluit veiligheid en integriteit telecommunicatie dat op 5 december 2019 is gepubliceerd. Uw Kamer heb ik eerder over deze publicatie geïnformeerd[5]. Ook richt het kabinet in samenwerking met de telecomaanbieders een structureel proces in. Dit gebeurt onder aansturing van de Taskforce Economische Veiligheid. Uw Kamer wordt voor de zomer geïnformeerd over de voortgang van het inrichten van dit proces[6].

b) Beoordeling + inzet ten aanzien van dit voorstel

Conform de moties Weverling en Van den Berg[7] heeft het kabinet gepleit voor meer Europese samenwerking op het gebied van de veiligheid van 5G-telecommunicatienetwerken. Het kabinet stond daarom ook positief tegenover de Europese aanbeveling van 26 maart 2019. Het kabinet steunt ook de verdere doorontwikkeling van de Europese aanpak via de toolbox. Het Nederlandse beleid sluit nauw aan bij de in de toolbox geschetste maatregelen en de Raadsconclusies[8] die in de Telecomraad van 3 december 2019 zijn aangenomen. Evenzeer zal het kabinet, onder meer via de NIB-Samenwerkingsgroep, een actieve bijdrage blijven leveren aan de vervolgstappen, zoals door de Commissie geschetst in deze mededeling.

Het kabinet zal in het komende traject met de andere lidstaten en de Commissie scherp zijn op specifieke stappen die strijdig zijn met de verdragsrechtelijke bepalingen betreffende de bevoegdheid van lidstaten op het gebied van nationale veiligheid (artikel 4, lid 2, VEU). Ook zal het kabinet nadrukkelijk aandacht vragen voor de zorgvuldige behandeling van vertrouwelijke informatie mocht deze door lidstaten worden gedeeld. Daarnaast blijft het uiteindelijk aan de lidstaten zelf om te bepalen of en in welke mate informatie uiteindelijk wordt gedeeld met andere lidstaten en de Commissie. In alle gevallen geldt dat gerubriceerde of vertrouwelijke informatie in elk geval geen onderdeel zal uitmaken van deze informatie-uitwisseling, vanwege risico's voor de nationale veiligheid, vanwege bedrijfsvertrouwelijkheid of omdat deze betrekking heeft op de concurrentiepositie van de telecomaanbieders en de beveiliging van hun netwerken.

Voor de bredere strategische trajecten die ook onder de bevoegdheid van de Unie vallen, zoals geschetst in de mededeling, heeft het kabinet uw Kamer geïnformeerd over de al lopende trajecten. Zo heeft het kabinet zich in Brussel hard gemaakt voor de op 9 april 2019 door de Raad aangenomen Cyberbeveiligingsverordening, die een Europees cybersecurity certificeringskader creëert.[9] Conform de motie van het lid Paternotte c.s.[10], heeft het kabinet zich daarbij ingezet voor verplichte cybersecuritycertificering. De Commissie zal uiterlijk eind 2023 aangeven voor

---

[5] Kamerstuk 24 095, nr. 492
[6] Kamerstukken 24 095 en 30 821, nr. 495
[7] Motie van het lid Weverling c.s. (Kamerstuk 21 501–33, nr. 734) en motie van het lid Van den Berg c.s. (Kamerstuk 21 501–33, nr. 747)
[8] https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.
[9] Kamerstuk 22 112, nr. 2437
[10] Kamerstuk 21 501–30, nr. 422

welke ICT-producten, -diensten en -processen waarvoor een cybersecurity certificeringsschema bestaat, een certificeringsschema verplicht zal worden gesteld.
Ook wordt de geschetste inzet op de blauwdruk voor incident response en crisismanagement door het kabinet gesteund. Een gecoördineerde respons op grootschalige cyberincidenten en -crises is een nationale verantwoordelijkheid en moet volgens het kabinet binnen bestaande werkgroepen en crisisstructuren plaatsvinden.[11] In dat kader organiseert Nederland in 2020 de oefening Blue OLEx waarbij binnen de NIB-Samenwerkingsgroep wordt nagedacht hoe efficiënt kan worden omgegaan met een cybercrisis die de EU-lidstaten treft.

c) Eerste inschatting van krachtenveld

De noodzaak voor samenwerking en het uitwisselen van informatie en ervaringen rondom cyberbeveiliging en 5G wordt door het merendeel van de lidstaten onderschreven. De ontwikkeling van de gezamenlijke EU-risicobeoordeling en de EU-toolbox door de lidstaten in samenwerking met de Commissie laten dit ook zien. Deze mededeling, die zich baseert op die documenten, is daarmee in lijn met wat de lidstaten reeds hebben geadviseerd, waardoor deze naar verwachting op steun kan rekenen. Daarbij zien veel lidstaten, net als Nederland, (potentiële) raakvlakken met nationale veiligheid en geven aan dat de voorgestelde acties geen afbreuk mogen doen aan de nationale bevoegdheid van de lidstaten. Het Europees Parlement heeft nog geen positie ingenomen op het brede onderwerp van 5G.

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

a) Bevoegdheid

Het kabinet heeft een positieve grondhouding ten aanzien van de bevoegdheid van de Commissie voor wat deze mededeling betreft. Deze mededeling van de Commissie strekt met name ter bescherming van de Europese Unie tegen digitale aanvallen in het kader van het 5G-netwerk en passen op hoofdlijnen binnen de bevoegdheden van de EU op het terrein van de interne markt. Op dat terrein heeft de EU een gedeelde bevoegdheid met de lidstaten (artikel 4, lid 2, onder a, VWEU).

Wel bevindt een aantal van de aangekondigde acties en plannen zich dicht tegen of op het terrein van nationale veiligheid. Op grond van artikel 4, lid 2, VEU dient de EU de essentiële staatsfuncties, zoals de bescherming van de nationale veiligheid te eerbiedigen. Met name de nationale veiligheid blijft de uitsluitende verantwoordelijkheid van elke lidstaat. Nederland zal er ook in het komende traject op toezien dat de verdragsrechtelijke bepalingen worden gerespecteerd.

b) Subsidiariteit

Het kabinet heeft een positieve grondhouding ten aanzien van de subsidiariteit. Gelet op het grensoverschrijdende karakter van cyberbeveiliging, cyberdreiging en het wettelijke telecomkader, kunnen de gestelde doelstellingen volgens het kabinet beter worden verwezenlijkt op niveau van de Unie.

[11] Kamerstuk 22 112, nr. 2407

c) Proportionaliteit

De grondhouding van het kabinet ten aanzien van de proportionaliteit van maatregelen die worden aangekondigd in de mededeling is positief, omdat zij de cyberveiligheid van Europa op een geschikte en evenredige wijze naar een hoger niveau brengen. De mededeling zoals nu gesteld, verzoekt de lidstaten de toolbox uit te voeren, door middel van het nemen van stappen op basis van de maatregelen, zoals gesteld in de EU-toolbox en de stand van de uitvoering te monitoren. Deze maatregelen zijn vooral ook bedoeld om de gedachten- en beleidsvorming op nationaal niveau bij de lidstaten verder te helpen, door van elkaars expertise en ervaring gebruik te kunnen maken ledere lidstaat kan op basis van eigen geschatte risico's bepaalde maatregelen nemen, waardoor de mededeling toeziet op een evenredige uitvoering van de EU-toolbox.

d) Financiële gevolgen

Er wordt geen concrete informatie gegeven over eventueel verwachte financiële impact op de hoogte van de EU-begroting. 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. De kabinetsinzet voor het volgende Meerjarig Financieel Kader (MFK) is leidend voor een integrale afweging van middelen voor de periode na 2020; Nederland wil niet vooruitlopen op de besluitvorming over het volgende MFK. Indien er sprake is van budgettaire gevolgen voor Nederland, dan zullen deze worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels van de budgetdiscipline.

e) Gevolgen voor regeldruk, administratieve lasten en concurrentiekracht

De mededeling zelf bevat geen nieuwe wettelijke maatregelen en geeft daarmee geen aanleiding om gevolgen te verwachten op regeldruk en administratieve lasten, voor de overheid, bedrijfsleven of burgers. De bovengenoemde maatregelen, die inmiddels op nationaal niveau worden genomen, zijn in lijn met de in de toolbox aanbevolen maatregelen. Deze vloeien uit reeds bestaande nationale bevoegdheden, en zijn derhalve geen extra regeldruk voortvloeiend uit deze mededeling. Gedurende het traject dat de mededeling schetst, zal het kabinet nadrukkelijk in de gaten houden of er gevolgen zijn voor de regeldruk en administratieve lasten en u hierover informeren indien nodig. Indien de Commissie in de nabije toekomst aanvullende maatregelen of eisen aankondigt zal Nederland erop aandringen dat deze zo lastenluw mogelijk worden ingericht.