Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

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

Nr. 2816 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 1 juli 2019

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

Fiche: Aanbeveling Cyberbeveiliging van 5G-netwerken

De Minister van Buitenlandse Zaken,
S.A. Blok

kst-22112-2816
ISSN 0921 - 7371
's-Gravenhage 2019

Fiche: Aanbeveling Cyberbeveiliging van 5G-netwerken

1. Algemene gegevens

a) *Titel voorstel*
Cyberbeveiliging van 5G-netwerken
b) *Datum ontvangst Commissiedocument*
26 maart 2019
c) *Nr. Commissiedocument*
C (2019) 2335
d) *EUR-Lex*
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1559130502446&uri=CELEX:32019H0534
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
Niet opgesteld
f) *Behandelingstraject Raad*
Telecommunicatieraad
g) *Eerstverantwoordelijk ministerie*
Ministerie van Justitie en Veiligheid, Ministerie van Economische Zaken en Klimaat

2. Essentie voorstel

5G-netwerken[1], de volgende, vijfde generatie mobiele netwerken, zijn van essentieel belang voor de ontwikkeling van toekomstige digitale diensten, de goede werking van de interne markt en voor tal van vitale processen zoals energie, vervoer en het bankwezen alsmede andere economische en maatschappelijke activiteiten. Mobiele providers treffen voorbereidingen om 5G-netwerken grootschalig uit te kunnen rollen zodra aan hen gebruiksrechten voor radiofrequenties voor mobiele communicatie zijn toegekend. Frequenties vormen een essentiële bouwsteen voor het aanbieden van draadloze en mobiele communicatie.
Lidstaten en de Europese Commissie zijn bezorgd over mogelijke veiligheidsrisico's die verband houden met 5G-netwerken. Het is cruciaal de veiligheid en integriteit van 5G-netwerken te waarborgen. Daarom voorziet deze aanbeveling in maatregelen om een hoog gemeenschappelijk niveau van beveiliging van 5G-netwerken te realiseren. In de aanbeveling staat dat deze daarbij geen afbreuk doet aan bijvoorbeeld de bevoegdheden van de lidstaten met betrekking tot nationale veiligheid.

De Commissie stelt de volgende maatregelen voor:
1) *Lidstaten zouden hun cyberrisico's voor 5G-netwerken op nationaal niveau moeten beoordelen en de nodige beveiligingsmaatregelen treffen;*
Daartoe zouden lidstaten een risicobeoordeling van de infrastructuur van het 5G-netwerk moeten uitvoeren, uiterlijk op 30 juni 2019. Het gaat hierbij eveneens om het evalueren van de vigerende beveiligingsvereisten en risicobeheermethoden, rekening houdend met technische factoren en andere factoren, zoals wetgeving en beleid die gelden voor leveranciers van apparatuur in derde landen. Lidstaten sturen uiterlijk op 15 juli 2019 hun risicobeoordelingen aan de Commissie en ENISA.

[1] 5G is de term voor de volgende, vijfde generatie mobiele communicatietechnologie. Het onderscheidt zich van 4G doordat het zeer snelle, betrouwbare mobiele connectiviteit met pieksnelheden tot 20 gigabits per seconde kan leveren en reactietijden (latency) van enkele milliseconden. Het kan tevens een belangrijke bijdrage leveren aan het opvangen van het groeiende dataverkeer en het mogelijk maken van allerlei nieuwe toepassingen, zoals smart mobility.

Op basis van deze risicobeoordeling en -evaluatie zouden de lidstaten hun nationale beveiligingsvereisten en risicobeheermethoden ook moeten actualiseren om de risico's te beperken. Er zijn meerdere Europeesrechtelijke kaders op grond waarvan dergelijke beveiligingseisen (kunnen) worden gesteld, zoals de Kaderrichtlijn (Richtlijn2002/21/EG[2]) de Machtigingsrichtlijn (Richtlijn 2002/20/EG[3]) en de Verordening agentschap ENISA en Europees kader voor Cyberbeveiligingscertificering (kortweg de «Cyberbeveiligingsverordening»)[4].

2) *Het ontwikkelen van een gecoördineerde risicobeoordeling op het niveau van de Unie die voortbouwt op deze nationale risicobeoordelingen;*
Uiterlijk op 1 oktober 2019 zouden lidstaten – samen met de Commissie en ENISA – een gezamenlijke evaluatie moeten hebben uitgevoerd ten aanzien van de risico's die zijn verbonden met infrastructuur die ten grondslag ligt aan het digitale ecosysteem, in het bijzonder met 5G-netwerken (risico's die van toepassing zijn op de bijzonder gevoelige of kwetsbare kernonderdelen).

3) *Voor de Samenwerkingsgroep[5] heeft de Commissie de ambitie om uiterlijk 31 december 2019 een gemeenschappelijk instrumentarium («tool box») overeen te komen met betrekking tot de beste mitigerende maatregelen om de risico's te beheersen.*
Het kan hierbij gaan om het delen van op nationaal niveau geïdentificeerde *best practices*, het maken van een inventaris van de risico's (bijvoorbeeld in de toeleveringsketen of bij software) en maatregelen zoals testen en conformiteitscontroles van hardware en software. Specifiek worden lidstaten opgeroepen om EU-schema's voor certificering op dit thema, voortvloeiend uit de nieuwe cyberbeveiligingsverordening nationaal verplicht te stellen. Deze maatregelen vloeien voort uit de geïdentificeerde risico's. Onderdeel van de activiteiten van de Samenwerkingsgroep is ook het adviseren van de Commissie over EU-brede minimumbeveiligingseisen met betrekking tot 5G waarmee een hoog niveau van cybersecurity van 5G-netwerken kan worden gewaarborgd.

Uiterlijk 1 oktober 2020 moeten de effecten die voortkomen uit deze aanbeveling zijn geëvalueerd.

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

---

[2] Richtlijn 2002/21/EG van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische communicatienetwerken en -diensten (Kaderrichtlijn).

[3] Richtlijn 2002/20/EG van 7 maart 2002 betreffende de machtiging voor elektronische communicatienetwerken en -diensten.

[4] Verordening inzake ENISA, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (de «cyberbeveiligingsverordening»).

[5] De Samenwerkingsgroep is opgericht in het kader van de Richtlijn 2016/1148 inzake maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIB); hierin participeren de lidstaten, de Commissie en ENISA.

De concrete uitwerking van deze visie op het gebied van digitale veiligheid is vastgelegd in de Nederlandse Cyber Security Agenda uit 2018.[6] Gezien het inherent grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging staat Europese en internationale samenwerking in de Nederlandse aanpak centraal.

Zoals ook in de Kamerbrief[7] van 15 april is vermeld, is onder leiding van de Nationaal Coördinator Terrorismebestrijding en Veiligheid een interdepartementale Taskforce opgericht. De Taskforce voert met medewerking van de drie grote telecomaanbieders (KPN, T-Mobile en Vodafone Ziggo) een risicoanalyse uit naar de kwetsbaarheid van 5G-telecommunicatienetwerken voor misbruik van leveranciers van technologie voor deze netwerken en welke maatregelen nodig zijn om risico's te beheersen. De Taskforce is voor wat betreft samenstelling en activiteiten zo opgezet dat evenwichtige besluitvorming kan plaatsvinden waarbij zowel veiligheidsbelangen, waaronder het aspect van nationale veiligheid bij de uitrol van 5G, als economische belangen worden geborgd. Nederland spant zich daarbij ook in voor informatie-uitwisseling en gedeelde risicoafweging in EU-verband en met bondgenoten buiten de EU. De Kamer zal (vertrouwelijk) over de uitkomsten van de Taskforce worden geïnformeerd conform de moties van de leden Weverling en Van den Berg.[8]

De Kaderrichtlijn schrijft voor dat lidstaten ervoor moeten zorgen dat aanbieders van openbare elektronische communicatienetwerken- en diensten de veiligheid en integriteit van hun netwerken en diensten moeten waarborgen. Deze verplichting is geïmplementeerd in de Telecommunicatiewet (Tw). De Telecommunicatiewet biedt de Nederlandse overheid hiermee een basis voor nationale voorschriften met betrekking tot de veiligheid en integriteit van openbare elektronische communicatienetwerken en -diensten, waaronder het gebruik van netwerkapparatuur. Zo bepaalt artikel 11a.1 Tw dat aanbieders van openbare elektronische communicatienetwerken en -diensten de verplichting hebben passende technische en organisatorische maatregelen te nemen om de risico's voor de veiligheid en integriteit van hun netwerken en diensten te beheersen. Met betrekking tot deze maatregelen kunnen bij of krachtens algemene maatregel van bestuur (amvb) nadere regels worden gesteld[9] of rechtstreekse verplichtingen aan de aanbieders worden opgelegd.

Binnen de EU zet Nederland zich met betrekking tot cybersecurity onder meer in via de Samenwerkingsgroep vanuit de Richtlijn voor Netwerk- en Informatiebeveiliging (NIB-richtlijn). Het uitwisselen van beleidsmatige ervaringen en kwetsbaarheden binnen de sectoren die zijn geïdentificeerd in de NIB-richtlijn is een beleidsprioriteit voor Nederland. Ook heeft Nederland zich in Brussel hard gemaakt voor de op 9 april door de Raad aangenomen Cyberbeveiligingsverordening, die een Europees cybersecurity certificeringskader creëert. Conform de motie van het lid Paternotte c.s.[10] heeft Nederland zich ingezet voor verplichte cybersecuritycertificering. De Europese Commissie zal uiterlijk eind 2023 aangeven voor welke ICT-producten, -diensten en -processen waarvoor een cybersecurity

---

[6] Aanbiedingsbrief Nederlandse Cyber Security Agenda, Kamerstuk 26 643, nr. 536.

[7] «Reactie op bericht KPN gaat in zee met Huawei voor aanleg 5G», brief van de Staatssecretaris van Economische Zaken en Klimaat en de Minister van Justitie en Veiligheid van 1 april 2019 aan de Tweede Kamer, Kamerstuk 24 095, nr. 465.

[8] 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).

[9] Dat zou een uitbreiding van het huidige Besluit continuïteit openbare elektronische communicatienetwerken en -diensten betekenen.

[10] Motie van het lid Paternotte c.s. (Kamerstuk 21 501-30, nr. 422).

certificeringsschema bestaat, een certificeringsschema verplicht zal worden gesteld. Verder heeft Nederland een positieve houding ten opzichte van de momenteel in onderhandeling zijnde Verordening tot oprichting van het Europese kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra, dat kan bijdragen aan de ontwikkeling van nieuwe veilige digitale technologieën in Europa.

b) Beoordeling + inzet ten aanzien van dit voorstel

Conform de moties van de leden Weverling en Van den Berg[11] heeft het kabinet gepleit voor meer Europese samenwerking op het gebied van 5G-veiligheid. Het kabinet juicht toe dat in het verlengde daarvan de Europese Commissie dit onderwerp actief oppakt. Nederland steunt in algemene zin dan ook een gezamenlijke Europese aanpak die via deze aanbeveling vorm krijgt. Nederland zal hieraan een actieve bijdrage leveren. Er wordt daarbij vooral toegevoegde waarde gezien in het uitwisselen van risicoanalyses en het delen van oplossingsrichtingen tussen lidstaten, uiteraard dient dit wel op vrijwillige basis te gebeuren (zoals verderop beschreven). Daarbij zal het kabinet er ook op letten dat zaken zoveel mogelijk efficiënt en in gezamenlijkheid met de relevante al bestaande groepen wordt opgepakt, in plaats van parallel aan elkaar.

Nederland zal in het lopende traject scherp zijn op specifieke voornemens die strijdig zijn met de verdragsrechtelijke bepalingen betreffende de bevoegdheid van lidstaten op het gebied van nationale veiligheid (artikel 4, lid 2, VEU). Dit geldt ook voor de verwachtingen en vragen vanuit de Commissie rondom (het delen van) de nationale risicobeoordeling, en de verwerking daarvan door ENISA in een Europese risicobeoordeling. In dat kader zal Nederland ook nadrukkelijk aandacht vragen voor de zorgvuldige behandeling van (bedrijfs)vertrouwelijke informatie mocht deze door lidstaten worden gedeeld. Daarnaast blijft het uiteindelijk aan de lidstaten zelf om te bepalen welke informatie uiteindelijk wordt gedeeld met ENISA en andere lidstaten. In alle gevallen geldt dat gerubriceerde informatie van de Nederlandse inlichtingen- en veiligheidsdiensten geen onderdeel zal uitmaken van deze informatie-uitwisseling, omdat dit de nationale veiligheid betreft danwel informatie die bedrijfsvertrouwelijk is en betrekking heeft op de concurrentiepositie van de telecomaanbieders en de beveiliging van hun netwerken. Voor wat betreft de rol van ENISA zal Nederland in het traject benadrukken dat deze vooral moet dienen ter ondersteuning en facilitering van de lidstaten en van het proces, en specifiek op cybersecurity-gerelateerde onderwerpen gericht dient te zijn.

De Europese Commissie geeft in de aanbeveling aan dat prioriteit wordt toegekend aan de ontwikkeling van certificeringschema's voor 5G-netwerken. Voorts beveelt de Europese Commissie aan dat deze schema's op nationaal niveau verplicht zouden moeten worden gesteld. Gezien de Europese interne digitale markt en het grensoverschrijdend karakter van digitale veiligheidsvraagstukken, zet Nederland zich in algemene zin in voor verplichte cybersecuritycertificering op EU-niveau. De cyberbeveiligingsverordening zelf gaat overigens uit van vrijwillige certificering. Wat betreft de certificering op EU-niveau zal Nederland erop letten dat deze niet in de weg gaan staan aan het eigenstandig stellen van additionele nationale eisen aan 5G netwerken, met name vanuit het oogpunt van nationale veiligheid.

[11] 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).

De aanbeveling roept de lidstaten op hun nationale beveiligingsmaatregelen te evalueren en te actualiseren. Het is belangrijk om eventuele nationale beveiligingsmaatregelen bekend te maken vóórdat de vergunningen voor 5G worden geveild. Het gaat hierbij vooral om beveiligingsmaatregelen waar mogelijk hoge financiële kosten mee verbonden kunnen zijn. Om het veilingproces zorgvuldig te laten verlopen, is het namelijk belangrijk dat er zo min mogelijk onzekerheden boven de markt hangen en dat er voor de deelnemers zo veel mogelijk duidelijkheid is over de factoren die van invloed zijn op hun investeringsbeslissingen. Gegeven de planning om eind 2019 de formele aanvraag- en veilingprocedure te starten voor de 700, 1400 en 2100 MHz banden, is het gewenst dat dan eveneens duidelijkheid wordt gegeven over ingrijpende nationale beveiligingsmaatregelen.

c) Eerste inschatting van krachtenveld

De noodzaak voor samenwerking en het uitwisselen van informatie en ervaringen rondom cybersecurity en 5G wordt door het grote merendeel van de lidstaten onderschreven. De aanbeveling en het pakket aan voorgestelde maatregelen daarin, wordt daarmee over het algemeen positief ontvangen. Daarbij zien veel lidstaten, net als Nederland, (potentiële) raakvlakken met nationale veiligheid en geven aan dat de voorgestelde acties hier niet aan kunnen raken.

4. 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 voor deze aanbeveling. De aanbevelingen van de Commissie strekken met name ter bescherming van de Europese Unie tegen digitale aanvallen in het kader van het 5G-netwerk en zien 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). Op grond van artikel 292 VWEU is de Commissie bevoegd om aanbevelingen vast te stellen op de gebieden waarvoor de Unie bevoegd is.

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 bij de concretisering en uitwerking van de plannen nauwgezet op toezien dat de verdragsrechtelijke bepalingen worden gerespecteerd.

b) Subsidiariteit

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

c) Proportionaliteit

De grondhouding van het kabinet ten aanzien van de proportionaliteit van maatregelen die worden aangekondigd in de aanbeveling is positief, omdat zij de cyberveiligheid van Europa op een geschikte en evenredige wijze naar een hoger niveau brengen. De maatregelen zoals nu voorgesteld 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.

d) Financiële gevolgen

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 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.

Er wordt geen concrete informatie gegeven over eventueel verwachte financiële impact op de hoogte van de EU-begroting. Eventuele budgettaire gevolgen voor de Nederlandse begroting komen voort uit reeds bestaande nationale bevoegdheden en juridische kaders en niet uit deze aanbeveling.

e) Gevolgen voor regeldruk en administratieve lasten

De aanbeveling zelf bevat geen nieuwe wettelijke maatregelen en geeft daarmee geen aanleiding gevolgen te verwachten voor regeldruk en administratieve lasten, voor de overheid, bedrijfsleven of burgers. Gedurende het traject zoals geschetst in de aanbeveling zal een aantal voorstellen worden geconcretiseerd, bijvoorbeeld met betrekking tot veiligheidsvoorschriften. Hierbij zal het kabinet nadrukkelijk in de gaten houden of er gevolgen zijn voor de regeldruk en administratieve lasten en u hierover informeren indien nodig.