AANBEVELINGEN

AANBEVELING VAN DE COMMISSIE (EU) 2019/534

van 26 maart 2019

Cyberbeveiliging van 5G-netwerken

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 292,

Overwegende hetgeen volgt:

(1) De Commissie heeft de ontplooiing van netwerktechnologieën van de vijfde generatie (5G) erkend als een belangrijke factor in de ontwikkeling van toekomstige digitale diensten en als een prioriteit binnen de strategie voor een digitale eengemaakte markt. Het 5G-actieplan is door de Commissie goedgekeurd om ervoor te zorgen dat de Unie beschikt over de connectiviteitsinfrastructuur die nodig is voor haar digitale transformatie vanaf 2020 ([1]).

(2) De 5G-netwerken zullen voortbouwen op de huidige netwerktechnologieën van de vierde generatie (4G) door nieuwe mogelijkheden te bieden voor diensten en de centrale infrastructuur en motor te worden van grote delen van de economie van de Unie. Wanneer de 5G-netwerken uitgerold worden, zullen zij als ruggengraat dienen voor een brede waaier aan diensten die essentieel zijn voor de goede werking van de interne markt en de instandhouding en werking van vitale maatschappelijke en economische functies zoals energie, vervoer, het bankwezen, de gezondheidszorg, evenals industriële besturingssystemen. Bij de organisatie van democratische processen, zoals verkiezingen, zullen digitale infrastructuur en 5G-netwerken ook een steeds grotere rol spelen.

(3) Wanneer veel essentiële diensten afhankelijk worden van 5G-netwerken, zouden wijdverspreide systemische storingen bijzonder ernstige gevolgen kunnen hebben. Als gevolg daarvan is het voor de Unie van strategisch belang de cyberbeveiliging van 5G-netwerken te waarborgen, in tijden van toenemende cyberaanvallen die complexer dan ooit zijn.

(4) De onderlinge verwevenheid en grensoverschrijdende aard van de infrastructuur aan de basis van het digitale ecosysteem, en de grensoverschrijdende aard van de dreigingen in kwestie, betekenen dat elk significant zwak punt en/of elk met 5G-netwerken verband houdend cyberincident in één bepaalde lidstaat gevolgen zou hebben voor de Unie als geheel. Daarom moet worden voorzien in maatregelen om een hoog gemeenschappelijk niveau van cyberbeveiliging van 5G-netwerken te schragen.

(5) De behoefte aan actie op Unieniveau is door de lidstaten bevestigd. In zijn conclusies van 21 maart 2019 zag de Europese Raad uit naar een aanbeveling van de Commissie over een gezamenlijke aanpak voor de veiligheid van 5G-netwerken ([2]).

(6) Het waarborgen van de Europese soevereiniteit moet een hoofddoelstelling zijn, onder volledige inachtneming van de Europese waarden van openheid en tolerantie ([3]). Buitenlandse investeringen in strategische sectoren, verwerving van kritieke activa, technologie en infrastructuur in de Unie en levering van kritieke uitrusting kunnen ook potentiële risico's voor de veiligheid van de Unie vormen.

(7) De cyberbeveiliging van 5G-netwerken is van cruciaal belang om de strategische autonomie van de Unie te waarborgen, zoals is erkend in de Gezamenlijke mededeling „EU-China — Een strategische visie" ([4]).

(8) In de resolutie van het Europees Parlement over de veiligheidsdreigingen in verband met de toenemende technologische aanwezigheid van China in de EU worden de Commissie en de lidstaten ook opgeroepen om actie te ondernemen op het niveau van de Unie ([5]).

(9) Deze aanbeveling stelt cyberbeveiligingsrisico's in 5G-netwerken aan de orde door richtsnoeren vast te stellen voor passende risicoanalyse en -beheersmaatregelen op nationaal niveau, de ontwikkeling van een gecoördineerde risicobeoordeling op Europees niveau en de bepaling van een procedure om een gemeenschappelijk instrumentarium van de beste risicobeheersmaatregelen samen te stellen.

(10) De Unie beschikt over een sterk wetgevingskader om elektronische-communicatienetwerken te beschermen.

([1]) COM(2016) 588 final.
([2]) Conclusies van de Europese Raad van 21 en 22 maart 2019.
([3]) Staat van de Unie 2018 — De tijd is gekomen voor Europese soevereiniteit, 12 september 2018.
([4]) JOIN(2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//NL

(11) Het Uniekader op het gebied van elektronische communicatie ([6]) bevordert de mededinging, de interne markt en de belangen van de eindgebruiker, en streeft met het Europees wetboek voor elektronische communicatie ([7]) een aanvullende connectiviteitsdoelstelling na, uitgedrukt in resultaten: brede toegang tot en invoering van vaste en mobiele netwerken met zeer hoge capaciteit voor alle burgers en bedrijven van de Unie, waarbij de belangen van de burgers worden beschermd. Richtlijn 2002/21/EG schrijft voor dat de lidstaten de integriteit en de veiligheid van de openbare communicatienetwerken moeten waarborgen en verplicht zijn ervoor te zorgen dat ondernemingen die openbare communicatienetwerken of openbaar beschikbare elektronische-communicatiediensten aanbieden technische en organisatorische maatregelen nemen om de risico's voor de veiligheid van hun netwerken of diensten goed te beheersen. De richtlijn bepaalt ook de bevoegdheden van nationale regelgevende instanties, waaronder de bevoegdheid om bindende instructies te geven om te verzekeren dat die verplichtingen worden nageleefd.

(12) Voorts staat Richtlijn 2002/20/EG van het Europees Parlement en de Raad ([8]) de lidstaten toe voorwaarden aan de algemene machtiging te verbinden betreffende de beveiliging van publieke netwerken tegen ongeoorloofde toegang, met als doel het vertrouwelijke karakter van communicatie te beschermen overeenkomstig Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([9]).

(13) Om de nakoming van die verplichtingen te vergemakkelijken, heeft de Unie een aantal samenwerkingsorganen opgezet. Het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa), de Commissie, de lidstaten en nationale regelgevende instanties hebben technische richtsnoeren voor nationale regelgevende instanties opgesteld met betrekking tot incidentrapportage, beveiligingsmaatregelen en dreigingen en voorzieningen ([10]). De samenwerkingsgroep die bij Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ([11]) is opgericht („de samenwerkingsgroep") brengt bevoegde autoriteiten bij elkaar om samenwerking te schragen en te faciliteren, in het bijzonder door strategische richtsnoeren te verstrekken voor de activiteiten van het netwerk van Computer Security Incident Response Teams, dat op technisch niveau operationele samenwerking bevordert.

(14) Het toekomstige Europese kader voor cyberbeveiligingscertificering ([12]) is bedoeld als essentieel ondersteunend instrument ter bevordering van consistente beveiligingsniveaus. Het moet de ontwikkeling van regelingen voor cyberbeveiligingscertificering mogelijk maken waarmee kan worden ingespeeld op de behoeften van de gebruikers van 5G-apparatuur en -software. Door het cruciale belang van deze infrastructuur moet onmiddellijk prioriteit worden toegekend aan de ontwikkeling van die relevante Europese regelingen voor cyberbeveiligingscertificering van producten, diensten of processen in de informatie- en communicatietechnologie die worden gebruikt voor 5G-netwerken. De lidstaten en marktdeelnemers moeten zich actief inzetten voor de ontwikkeling van zulke certificeringsregelingen, en ondersteuning bieden bij het definiëren van specifieke beveiligingsprofielen voor 5G-netwerken.

(15) In gevallen waarin geharmoniseerd recht van de Unie ontbreekt, kunnen de lidstaten een Europese regeling voor cyberbeveiligingcertificering verplicht maken, door middel van nationale technische voorschriften die overeenkomstig het recht van de Unie zijn vastgesteld. De lidstaten kunnen ook gebruikmaken van regelingen voor cyberbeveiligingscertificering in het kader van openbare aanbestedingen en van Richtlijn 2014/24/EU van het Europees Parlement en de Raad ([13]), en kunnen de ontwikkeling ondersteunen van mechanismen voor bijstand — zoals een assistentiehub — voor de aankoop van cyberbeveiligingsoplossingen door overheidsafnemers.

(16) Een hoog niveau van gegevensbescherming en privacy is belangrijk voor de beveiliging van 5G-netwerken. Er zijn op het niveau van de Unie ook regels vastgesteld die de beveiliging bij de verwerking van persoonsgegevens waarborgen, waaronder in elektronische communicatie. De algemene verordening gegevensbescherming ([14]) maakt het verplicht persoonsgegevens zodanig te verwerken dat de beveiliging ervan wordt gewaarborgd, onder meer om ongeoorloofde toegang tot of gebruik van persoonsgegevens en de apparatuur voor de verwerking

([6]) Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en diensten (Kaderrichtlijn) (PB L 108 van 24.4.2002, blz. 33) en de bijzondere richtlijnen.

([7]) Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (PB L 321 van 17.12.2018, blz. 36).

([8]) Richtlijn 2002/20/EG van het Europees Parlement en de Raad van 7 maart 2002 betreffende de machtiging voor elektronische-communicatienetwerken en -diensten (Machtigingsrichtlijn) (PB L 108 van 24.4.2002, blz. 21).

([9]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

([10]) https://resilience.enisa.europa.eu/article-13

([11]) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

([12]) Voorstel voor een Verordening van het Europees Parlement en de Raad 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") (COM(2017) 477 final — 2017/0225 (COD)).

([13]) Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65).

([14]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

ervan, te voorkomen. In de richtlijn betreffende privacy en elektronische communicatie zijn specifieke voorschriften vastgelegd inzake de bescherming van het vertrouwelijke karakter van communicatie en van de eindapparatuur van eindgebruikers. Ook verplicht de richtlijn aanbieders van diensten ertoe passende technische en organisatorische maatregelen te nemen om de veiligheid van hun diensten te garanderen.

(17) De Unie heeft eveneens een instrument vastgesteld ter bescherming van kritieke infrastructuur en technologie, zoals die welke worden gebruikt bij communicatie, door de lidstaten buitenlandse directe investeringen te laten screenen om redenen van veiligheid of openbare orde en door een samenwerkingsmechanisme op te zetten waarmee de lidstaten en de Commissie informatie kunnen uitwisselen en bezorgdheid kunnen uiten over specifieke investeringen ([15]).

(18) De lidstaten en exploitanten zetten momenteel belangrijke voorbereidende stappen om de grootschalige uitrol van 5G-netwerken mogelijk te maken. Verscheidene lidstaten hebben hun bezorgdheid geuit over mogelijke met 5G-netwerken verband houdende veiligheidsrisico's in het kader van de uitvoering van procedures voor de toekenning van gebruiksrechten voor radiospectrumbanden bestemd voor 5G-netwerken ([16]) en hebben maatregelen genomen om deze risico's het hoofd te bieden.

(19) Bij de aanpak van cyberbeveiligingsrisico's in 5G-netwerken moet rekening worden gehouden met zowel technische als andere factoren. Technische factoren kunnen onder andere zwakke punten in de cyberbeveiliging zijn. Die kunnen worden uitgebuit om ongeoorloofde toegang tot informatie te krijgen (cyberspionage om economische of politieke redenen) of voor andere kwaadaardige bedoelingen (cyberaanvallen die gericht zijn op het verstoren of vernietigen van systemen en gegevens). Hierbij is het belangrijk rekening te houden met de noodzaak om netwerken gedurende hun gehele levenscyclus te beschermen en alle betrokken apparatuur in aanmerking te nemen, onder meer tijdens het ontwerp, de ontwikkeling, de aankoop, de uitrol, de exploitatie en het onderhoud van 5G-netwerken.

(20) Andere factoren kunnen wettelijke of andere vereisten omvatten die opgelegd worden aan leveranciers van apparatuur voor informatie- en communicatietechnologie. Bij een beoordeling van het belang van dergelijke factoren moet onder meer rekening worden gehouden met het algemene risico op beïnvloeding door een derde land, met name wat betreft het bestuursmodel in kwestie, het ontbreken van samenwerkingsovereenkomsten op het gebied van veiligheid of soortgelijke regelingen inzake gegevensbescherming, zoals adequaatheidsbesluiten, tussen de Unie en het derde land in kwestie, en met het feit of het land partij is bij multilaterale, internationale of bilaterale overeenkomsten inzake cyberbeveiliging, de bestrijding van cybercriminaliteit of gegevensbescherming.

(21) Als een belangrijke stap op de weg naar cyberbeveiliging van 5G-netwerken op het niveau van de Unie moet op nationaal niveau een risicobeoordeling worden uitgevoerd en afgerond. Die beoordelingen zouden de lidstaten kunnen helpen om op basis ervan hun nationale maatregelen voor beveiligingsvereisten en risicobeheer aan te passen.

(22) Om de doeltreffendheid te garanderen van de op deze cyberdreigingen gerichte maatregelen, die essentieel zijn voor de goede werking van de interne markt en de bescherming van persoonsgegevens en de persoonlijke levenssfeer, moet coördinatie worden ontwikkeld.

(23) De nationale risicobeoordelingen moeten de basis vormen voor een gecoördineerde risicobeoordeling van de Unie, bestaand uit een inventarisatie van de dreigingen en een gezamenlijke evaluatie door de lidstaten, met de steun van de Commissie en samen met het Europese Agentschap voor cyberbeveiliging (Enisa).

(24) Rekening houdend met de risicobeoordelingen op nationaal en op Unieniveau, moet de samenwerkingsgroep een instrumentarium samenstellen tot vaststelling van soorten cyberbeveiligingsrisico's en van mogelijke maatregelen die de risico's op gebieden zoals certificering, tests en toegangscontroles verkleinen. De samenwerkingsgroep moet ook mogelijke specifieke maatregelen identificeren waarmee de door een of meer lidstaten vastgestelde risico's kunnen worden aangepakt. De samenwerkingsgroep moet gebruikmaken van de steun van het Enisa, Europol, het Orgaan van Europese regelgevende instanties voor elektronische communicatie (Berec) en het Inlichtingen- en situatiecentrum van de EU. Dit instrumentarium moet als advies dienen voor de Commissie bij de ontwikkeling van gemeenschappelijke minimumeisen die blijven instaan voor een hoog niveau van cyberbeveiliging van 5G-netwerken in de hele Unie.

(25) Wanneer maatregelen tegen cyberbeveiligingsrisico's worden genomen, moet bij de opbouw van om het even welk netwerk rekening worden gehouden met de bevordering van cyberbeveiliging door met meerdere leveranciers te werken.

([15]) Verordening (EU) 2019/452 van het Europees Parlement en de Raad van 19 maart 2019 tot vaststelling van een kader voor de screening van buitenlandse directe investeringen in de Unie (PB L 79I van 21.3.2019, blz. 1).

([16]) De veilingprocedure voor ten minste één spectrumband staat voor 2019 gepland in elf lidstaten: België, Tsjechië, Duitsland, Ierland, Griekenland, Frankrijk, Litouwen, Hongarije, Nederland, Oostenrijk en Portugal. In 2020 staan nog zes veilingen op de agenda in Spanje, Litouwen (andere frequenties), Malta, Polen, Slowakije en het Verenigd Koninkrijk. *Bron:* http://5gobservatory.eu/observatory-overview/observatory-reports/

(26) Deze aanbeveling doet geen afbreuk aan de bevoegdheden van de lidstaten met betrekking tot activiteiten op het gebied van openbare beveiliging, defensie, staatsveiligheid en activiteiten van de staat op het gebied van het strafrecht, met inbegrip van het recht van de lidstaten om dienstverleners of leveranciers van hun markten te weren om redenen van nationale veiligheid,

HEEFT DE VOLGENDE AANBEVELING VASTGESTELD:

I. **DOELSTELLINGEN**

(1) Met het oog op de ontwikkeling van een aanpak op het niveau van de Unie die de cyberbeveiliging van 5G-netwerken waarborgt, wijst deze aanbeveling maatregelen aan die zouden moeten worden genomen die:

a) de lidstaten in staat stellen de cyberbeveiligingsrisico's voor 5G-netwerken op nationaal niveau te beoordelen en de nodige beveiligingsmaatregelen te nemen;

b) de lidstaten en de relevante instellingen, agentschappen en andere organen van de Unie in staat stellen samen een gecoördineerde risicobeoordeling op het niveau van de Unie te ontwikkelen die voortbouwt op de nationale risicobeoordeling;

c) de krachtens Richtlijn (EU) 2016/1148 opgerichte samenwerkingsgroep in staat stellen een mogelijke gemeenschappelijke reeks maatregelen te bepalen ter beperking van cyberbeveiligingsrisico's die verbonden zijn met de infrastructuur aan de basis van het digitale ecosysteem, in het bijzonder met 5G-netwerken.

II. **DEFINITIES**

(2) Voor de toepassing van deze aanbeveling wordt verstaan onder:

a) „5G-netwerk": een reeks van alle relevante infrastructuurelementen voor mobiele en draadloze communicatietechnologie, die wordt gebruikt voor connectiviteit en diensten met toegevoegde waarde met geavanceerde prestatiekenmerken, zoals zeer hoge transmissiesnelheden en -capaciteit, een lage latentie, een zeer hoge betrouwbaarheid, of voor de ondersteuning van een groot aantal aangesloten apparaten. Dat kunnen onder meer legacy-netwerkelementen zijn die gebaseerd zijn op vorige generaties van mobiele en draadloze communicatietechnologie zoals 4G of 3G. De term „5G-netwerk" moeten worden geacht alle relevante delen van het netwerk te omvatten;

b) „infrastructuur aan de basis van het digitale ecosysteem": de infrastructuur die digitalisering in een breed scala van belangrijke toepassingen voor de economie en de samenleving mogelijk maakt.

III. **ACTIE OP NATIONAAL NIVEAU**

(3) Uiterlijk op 30 juni 2019 zouden de lidstaten een risicobeoordeling van de infrastructuur van het 5G-netwerk moeten uitvoeren, en daarbij de meest kwetsbare elementen moeten identificeren die aanzienlijke negatieve gevolgen zouden ondervinden van beveiligingsincidenten. Uiterlijk op dezelfde datum zouden de lidstaten eveneens de op nationaal niveau van toepassing zijnde beveiligingsvereisten en risicobeheermethoden moeten evalueren, rekening houdend met cyberdreigingen die het gevolg kunnen zijn van i) technische factoren, zoals de specifieke technische kenmerken van 5G-netwerken, en ii) andere factoren zoals het wetgevings- en beleidskader dat mogelijk geldt voor leveranciers van apparatuur voor informatie- en communicatietechnologie in derde landen.

(4) Op basis van deze nationale risicobeoordeling en -evaluatie en rekening houdend met de lopende gecoördineerde actie op het niveau van de Unie, zouden de lidstaten het volgende moeten doen:

a) de met betrekking tot 5G-netwerken toegepaste beveiligingsvereisten en risicobeheermethoden actualiseren;

b) de relevante verplichtingen die gelden voor ondernemingen die openbare communicatienetwerken of openbaar beschikbare elektronische-communicatiediensten aanbieden uit hoofde van de artikelen 13 bis en 13 ter van Richtlijn 2002/21/EG actualiseren;

c) voorwaarden aan de algemene machtiging verbinden betreffende de beveiliging van publieke netwerken tegen ongeoorloofde toegang en verbintenissen verlangen van de ondernemingen die deelnemen aan aanstaande procedures voor de toekenning van gebruiksrechten voor radiofrequenties in 5G-banden met betrekking tot de naleving van beveiligingsvereisten voor netwerken uit hoofde van Richtlijn 2002/20/EG;

d) andere preventieve maatregelen nemen om potentiële cyberbeveiligingsrisico's te beperken.

(5) De in punt 4 bedoelde maatregelen zouden strengere verplichtingen moeten inhouden voor leveranciers en exploitanten om de beveiliging van gevoelige onderdelen van het netwerk te garanderen, evenals andere verplichtingen in voorkomend geval, zoals de verplichting relevante informatie aan de bevoegde nationale autoriteiten te verstrekken betreffende geplande wijzigingen in elektronische-communicatienetwerken en de verplichting specifieke IT-componenten en -systemen vooraf te laten testen door nationale controle-instanties of certificatielaboratoria met het oog op veiligheid en integriteit.

(6) Gezamenlijke beveiligingsevaluaties zouden moeten worden uitgevoerd door twee of meer lidstaten die beschikken over de passende technische deskundigheid en voorzieningen met betrekking tot de infrastructuur aan de basis van het digitale ecosysteem en van 5G-netwerken, bijvoorbeeld wanneer dezelfde onderneming netwerkinfrastructuur exploiteert of bouwt in meer dan één lidstaat of wanneer de netwerkconfiguraties van die lidstaten grote gelijkenissen vertonen. Het Europese Agentschap voor cyberbeveiliging (Enisa), Europol en het Orgaan van Europese regelgevende instanties voor elektronische communicatie (Berec) zouden prioriteit moeten toekennen aan steunverzoeken van lidstaten op dit gebied. De resultaten van deze evaluaties zouden moeten worden doorgegeven aan de samenwerkingsgroep en het netwerk van Computer Security Incident Response Teams.

IV. GECOÖRDINEERDE ACTIE OP UNIENIVEAU

(7) Teneinde een gemeenschappelijke aanpak tegen cyberbeveiligingsrisico's met betrekking tot 5G-netwerken te ontwikkelen, zouden de lidstaten uiterlijk op 30 april 2019 werkzaamheden moeten aanvangen binnen een specifieke actielijn in de samenwerkingsgroep. Waar passend zouden de lidstaten de betrokken autoriteiten moeten uitnodigen om deel te nemen aan de werkzaamheden van de samenwerkingsgroep.

Gecoördineerde risicobeoordeling op Europees niveau

(8) De lidstaten zouden met elkaar en met de betrokken organen van de Unie informatie moeten uitwisselen met als doel een gedeeld besef te krijgen van de bestaande en mogelijke cyberbeveiligingsrisico's die aan 5G-netwerken verbonden zijn.

(9) De lidstaten zouden hun nationale risicobeoordelingen uiterlijk op 15 juli 2019 moeten overmaken aan de Commissie en het Enisa.

(10) Het Enisa zou een specifieke inventarisatie van de dreigingen voor 5G-netwerken moeten uitvoeren. De samenwerkingsgroep en het netwerk van Computer Security Incident Response Teams die krachtens Richtlijn (EU) 2016/1148 zijn opgericht, zouden daarbij ondersteuning moeten bieden.

(11) Rekening houdend met al deze elementen zouden de lidstaten met de steun van de Commissie en samen met het Enisa uiterlijk op 1 oktober 2019 een gezamenlijke evaluatie moeten voltooien van de Uniebrede blootstelling aan risico's die verbonden zijn met de infrastructuur aan de basis van het digitale ecosysteem, in het bijzonder met 5G-netwerken.

(12) Bij die gezamenlijke evaluatie moet prioriteit worden gegeven aan een analyse van de risico's die van toepassing zijn op bijzonder gevoelige of kwetsbare kernonderdelen van de 5G-netwerken, het Operations and Maintenance Centre en de 5G-toegangsnetwerkelementen die gebruikt worden voor industriële toepassingen.

(13) Vervolgens zou deze gezamenlijke evaluatie moeten worden uitgebreid naar andere strategische elementen van de digitale waardeketen.

Een gemeenschappelijk Uniebreed instrumentarium om de risico's te beperken

(14) De samenwerkingsgroep zou moeten bepalen welke op nationaal niveau toegepaste maatregelen van het in punt 4 bedoelde type de beste praktijken zijn. Op basis van die nationale beste praktijken zou uiterlijk op 31 december 2019 overeenstemming moeten worden bereikt over een instrumentarium van mogelijke passende, doeltreffende en evenredige risicobeheersmaatregelen om de geïdentificeerde cyberbeveiligingsrisico's op nationaal niveau en Unieniveau te beperken, om de Commissie te adviseren over de ontwikkeling van gemeenschappelijke minimumvereisten waarmee in de hele Unie een hoog niveau van cyberbeveiliging van 5G-netwerken kan worden gewaarborgd.

(15) Dat instrumentarium zou het volgende moeten omvatten:

a) een inventaris van de soorten risico's die gevolgen kunnen hebben voor de cyberbeveiliging van 5G-netwerken (bv. risico's in de toeleveringsketen, door kwetsbaarheid van software, bij toegangscontrole, en risico's die voortvloeien uit het wetgevings- en beleidskader dat mogelijk geldt voor leveranciers van apparatuur voor informatie- en communicatietechnologie in derde landen), en

b) een reeks mogelijke risicobeperkende maatregelen (bv. certificering door een derde partij van hardware, software of diensten; formele tests of conformiteitscontroles van hardware en software; procedures om te waarborgen dat toegangscontroles bestaan en worden gehandhaafd; identificatie van producten, diensten of leveranciers die als potentieel onveilig kunnen worden beschouwd enz.) Deze maatregelen zouden gericht moeten zijn op alle soorten beveiligingsrisico's die in één of meer lidstaten worden vastgesteld aan de hand van de risicobeoordeling.

(16) Zodra er Europese regelingen voor cyberbeveiligingscertificering met betrekking tot 5G-netwerken zijn ontwikkeld, zouden de lidstaten overeenkomstig het recht van de Unie nationale technische voorschriften moeten vaststellen die de certificering van de onder deze regelingen vallende producten, diensten of systemen in de informatie- en communicatietechnologie verplicht maken.

(17) De lidstaten zouden samen met de Commissie de voorwaarden moeten bepalen betreffende de beveiliging van publieke netwerken tegen ongeoorloofde toegang die aan de algemene machtiging moeten worden verbonden, evenals de beveiligingsvereisten voor netwerken, met als doel verbintenissen te verlangen van de ondernemingen die deelnemen aan procedures voor de toekenning van gebruiksrechten voor spectrum in 5G-banden uit hoofde van Richtlijn 2002/20/EG. Indien mogelijk zouden deze vereisten tot uitdrukking moeten komen in de in punt 4, onder c), vermelde maatregelen.

(18) De lidstaten zouden met de Commissie moeten samenwerken om specifieke beveiligingsvereisten te ontwikkelen die van toepassing kunnen zijn in het kader van met 5G-netwerken verband houdende openbare aanbestedingen. Die vereisten zouden ook de verplichting moeten omvatten om regelingen voor cyberbeveiligingscertificering in te voeren bij openbare aanbestedingen, voor zover zulke regelingen nog niet bindend zijn voor alle leveranciers en exploitanten.

V. **TOETSING**

(19) De lidstaten zouden met de Commissie moeten samenwerken om de effecten van deze aanbeveling uiterlijk op 1 oktober 2020 te beoordelen, teneinde uit te maken wat de juiste weg vooruit is. Bij deze beoordeling zou rekening moeten worden gehouden met de resultaten van de gecoördineerde risicobeoordeling op het niveau van de Unie en met het Uniebrede instrumentarium.

Gedaan te Straatsburg, 26 maart 2019.

Voor de Commissie
Julian KING
Lid van de Commissie