EUROPESE
COMMISSIE

Brussel, 29.1.2020
COM(2020) 50 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Uitrol van beveiligde 5G in de EU – uitvoering van de EU-toolbox

1. Inleiding

De vijfde generatie (5G) telecommunicatienetwerken is startklaar om een essentiële rol te spelen in de ontwikkeling van de Europese samenleving en economie. Deze netwerken zullen naar verwachting enorme economische kansen bieden en een belangrijke basis vormen voor de digitale en groene transformatie op gebieden als vervoer, energie, de maakindustrie, gezondheid, landbouw en media.

5G zou dus gevolgen kunnen hebben voor alle aspecten van het leven van de EU-burgers. De cyberbeveiliging van 5G-netwerken is daarom niet alleen essentieel voor de bescherming van onze economieën, samenlevingen en democratische processen, maar ook voor een betrouwbare digitale transformatie waarbij alle EU-burgers baat hebben.

Aangezien veel kritieke diensten afhankelijk zijn van 5G-netwerken, zouden de gevolgen van een systemische en wijdverbreide verstoring bijzonder ernstig zijn. Gezien de verwevenheid van de digitale ecosystemen zou zo'n verstoring een aanzienlijke impact over nationale grenzen heen kunnen hebben. Het waarborgen van de cyberbeveiliging van 5G-netwerken is dan ook een kwestie van strategisch belang voor de Unie, in een tijd waarin cyberaanvallen steeds vaker voorkomen, steeds geraffineerder worden en afkomstig zijn van zeer uiteenlopende dreigingsactoren, en met name van actoren van buiten de EU of van door staten gesteunde actoren. Wat betreft de beveiliging van kritieke infrastructuur, waaronder die van 5G, is ervoor gekozen om voor het eerst tot een gemeenschappelijke Europese benadering te komen. Bij deze benadering wordt ten volle rekening gehouden met de openheid van de interne markt van de EU, zolang de risicoafhankelijke EU-beveiligingseisen in acht wordt genomen.

De Europese Raad heeft op 22 maart 2019 opgeroepen tot een gezamenlijke aanpak van de veiligheid van 5G-netwerken. Op 26 maart 2019 heeft de Commissie Aanbeveling (EU) 2019/534 inzake de cyberbeveiliging van 5G-netwerken goedgekeurd[1]. In de aanbeveling werden de lidstaten opgeroepen om de nationale risicobeoordelingen af te ronden en nationale maatregelen te evalueren, om op EU-niveau samen te werken aan een gecoördineerde risicobeoordeling en een toolbox van mogelijke risicobeperkende maatregelen voor te bereiden. Deze mededeling is een integrerend deel van de alomvattende Europese digitale strategie van de Commissie, waartoe de Europese Raad heeft opgeroepen.

2. Uitrol van 5G in de EU

De invoering van 5G-netwerkinfrastructuur in Europa is van groot belang voor de industriële strategie en het concurrentievermogen van Europa. De Commissie heeft de invoering van 5G-netwerktechnologieën erkend als belangrijke factor in de ontwikkeling van toekomstige digitale diensten. In 2016 heeft de Commissie het 5G-actieplan goedgekeurd om ervoor te zorgen dat de Unie vanaf 2020 beschikt over de connectiviteitsinfrastructuur die nodig is voor de digitale transformatie en voor de alomvattende invoering van 5G in stedelijke gebieden en op belangrijke transportroutes tegen 2025[2]. In de mededeling over de gigabitmaatschappij

[1] Aanbeveling (EU) 2019/534 inzake de cyberbeveiliging van 5G-netwerken (PB L 88 van 29.3.2019, blz. 42).
[2] COM(2016) 588 final van 14.9.2016: "5G voor Europa: een actieplan".

wordt tot doel gesteld overal toegang tot mobiele gegevensverbindingen te verschaffen[3], ook in landelijke en afgelegen gebieden.

Wat de toewijzing van frequenties betreft, hebben de lidstaten 16 % van de 5G-pionierbanden toegewezen[4]. Met het oog op de wettelijke verplichting om het gebruik van alle 5G-pionierbanden tegen het einde van het jaar toe te staan, worden de komende maanden raadplegingen over een aantal toewijzingsprocedures verwacht.

Europa is een van de meest geavanceerde regio's ter wereld wat de commerciële lancering van 5G-diensten betreft[5]. De eerste 5G-diensten zullen naar verwachting eind 2020 in 138 Europese steden beschikbaar zijn. Vroege 5G-netwerken bouwen voort op de huidige vierde generatie netwerktechnologieën (4G) en 5G-diensten zijn hoofdzakelijk bestemd voor het grote publiek, hetzij als een verbetering van de capaciteit en snelheid van 4G, hetzij als een kosteneffectief draadloos alternatief voor vaste netwerken[6].

Wat de mogelijkheden voor nieuwe business-to-businessdiensten betreft, bijvoorbeeld in de sectoren energie, voedsel en landbouw, gezondheidszorg, de maakindustrie en vervoer, heeft Europa aanzienlijke vooruitgang geboekt: de investeringen bedragen ongeveer 1 miljard EUR, waarvan 300 miljoen EUR aan EU-financiering in het kader van het publiek-private partnerschap voor 5G dat onder Horizon 2020 valt. Deze investering gaat naar meer dan 160 specifieke grootschalige 5G-proeven in Europa, waaronder tien grensoverschrijdende snelwegcorridors voor het grootschalig testen van op 5G gebaseerde geconnecteerde en geautomatiseerde mobiliteitsdiensten. Er worden onder meer op 5G werkende toepassingen getest op uiteenlopende gebieden, variërend van duurzame gezondheidszorg, geautomatiseerde mobiliteit en hulpbronnenefficiënte landbouw tot slimme elektriciteitsnetten en industrie 4.0. Daarnaast heeft de EIB, ondersteund door het Europees Fonds voor strategische investeringen, leningen verstrekt om het onderzoek naar en de ontwikkeling van 5G-technologie te versnellen.

Het Europees wetboek voor elektronische communicatie[7] dat met ingang van 21 december 2020 van toepassing is, is een belangrijke basis voor het scheppen van een investeringsvriendelijk klimaat voor 5G-netwerken en netwerken van de volgende generaties. Voorts zullen overheidsfinancieringsprogramma's, zoals de Connecting Europe Facility[8] en de Europese structuur- en investeringsfondsen, essentieel zijn voor de ondersteuning van de toekomstige invoering van 5G-netwerken, met name doordat gemeenschappen, zoals scholen, ziekenhuizen, steden en lokale overheden, worden verbonden met diensten die gebruikmaken van 5G.

---

[3] COM(2016) 587 final: "Connectiviteit voor een competitieve digitale eengemaakte markt – Naar een Europese gigabitmaatschappij".

[4] http://www.5GObservatory.eu

[5] http://www.5GObservatory.eu

[6] Sommige nieuwe functionaliteiten van 5G zullen gefaseerd worden ingevoerd. In de eerste fase (op zeer korte of korte termijn) zal de invoering van 5G voornamelijk bestaan uit "niet-standalone" netwerken, waarbij alleen het radiotoegangsnetwerk wordt opgewaardeerd tot 5G-technologie en voor het overige nog steeds gebruik wordt gemaakt van de bestaande 4G-kernnetwerken, wat betere mobiele-breedbandprestaties voor de eindgebruikers zal opleveren. Tijdens de volgende fasen (korte en middellange tot lange termijn) zal voor de invoering van standalone 5G-netwerken, met inbegrip van 5G-kernnetwerkfuncties, een veel ingrijpender wijziging van de netwerkarchitectuur nodig zijn.

[7] Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking).

[8] COM(2018) 438 final van 6.6.2018, Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van de Connecting Europe Facility en tot intrekking van Verordeningen (EU) nr. 1316/2013 en (EU) nr. 283/2014.

Gezien de strategische mogelijkheden in 5G-diensten die Europa voor diverse sectoren te bieden heeft, zal het van het grootste belang zijn dat exploitanten en dienstverleners investeren in geavanceerde oplossingen voor 5G-netwerken en -diensten. Daarvoor zijn niet alleen nieuwe 5G-radionetwerken nodig, maar ook nieuwe zogenaamde „standalone" 5G-netwerken, teneinde geavanceerde 5G-functionaliteiten te bieden, zoals networkslicing[9] en edgecomputing[10].

De Commissie blijft de succesvolle uitrol van 5G in de EU volledig ondersteunen, onder meer door met de lidstaten en belanghebbenden samen te werken teneinde de kansen van 5G te benutten. Er zal, uitgaande van het voorzorgsbeginsel[11], naar behoren rekening worden gehouden met relevante gezondheidsaspecten, waarbij wordt samengewerkt met de desbetreffende internationale organisaties en de wetenschappelijke wereld.

3. De gecoördineerde EU-risicobeoordeling betreffende cyberbeveiliging in 5G-netwerken

Elke lidstaat heeft binnen de NIS-samenwerkingsgroep[12] zijn eigen nationale risicobeoordeling van zijn 5G-netwerkinfrastructuurvoorzieningen voltooid en de resultaten daarvan begin juli 2019 ingediend bij de Commissie en het Enisa, het Agentschap van de Europese Unie voor cyberbeveiliging.

Op basis van deze nationale risicobeoordelingen hebben de NIS-samenwerkingsgroep, bestaande uit vertegenwoordigers van de lidstaten, de Commissie en het Enisa, op 9 oktober 2019 een verslag gepubliceerd over de gecoördineerde EU-risicobeoordeling betreffende de cyberbeveiliging van 5G-netwerken[13]. In het verslag worden de belangrijkste dreigingen en dreigingsactoren, de meest kwetsbare activa en de belangrijkste zwakke punten van 5G-netwerken (onder meer op technisch gebied) in kaart gebracht. Het verslag bevat op basis hiervan ook een aantal categorieën van risico's die van strategisch belang zijn voor de EU en die worden geïllustreerd aan de hand van concrete risicoscenario's met relevante combinaties van de verschillende parameters (zwakke punten, dreigingen en dreigingsactoren) met betrekking tot de verschillende activa (zie bijlage).

Als aanvulling op dit verslag en als verdere input voor de toolbox heeft het Enisa een specifieke inventarisatie van het dreigingsbeeld verricht[14], bestaande uit een gedetailleerde analyse van bepaalde technische aspecten, waarbij met name werd ingegaan op de identificatie van netwerkactiva en van bedreigingen die hierop van invloed zijn.

In het gecoördineerde EU-risicobeoordelingsverslag komen aspecten aan bod die van belang zijn voor 5G-netwerken. Het gaat specifiek om de volgende aspecten:

---

[9] 5G-networkslicing maakt een hoge mate van scheiding tussen verschillende dienstenlagen op hetzelfde fysieke netwerk mogelijk, waardoor de mogelijkheden voor het aanbieden van gedifferentieerde diensten over het hele netwerk toenemen.

[10] Edgecomputing is een paradigma voor distributed computing waarbij computerprocessen en gegevensopslag dichter bij de locatie worden gebracht waar deze nodig zijn, teneinde de responstijd te verbeteren en de vereiste bandbreedte te beperken.

[11] Aanbeveling 1999/519/EG van de Raad van 12 juli 1999 betreffende de beperking van blootstelling van de bevolking aan elektromagnetische velden van 0 Hz – 300 GHz.

[12] 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 (NIS-richtlijn). De NIS-samenwerkingsgroep is opgericht bij de NIS-richtlijn om te zorgen voor strategische samenwerking en de uitwisseling van informatie tussen de EU-lidstaten op het gebied van cyberbeveiliging.

[13] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[14] ENISA Threat landscape for 5G networks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

a) Door de technologische veranderingen die voortvloeien uit 5G zal het totale aanvalsoppervlak groter worden en het aantal potentiële toegangspunten voor aanvallers toenemen:

- Door verbeterde functionaliteit aan de rand van het netwerk en een minder gecentraliseerde architectuur dan in vorige generaties mobiele netwerken kunnen sommige functies van de kernnetwerken worden geïntegreerd in andere delen van de netwerken, waardoor de desbetreffende apparatuur kwetsbaarder wordt (bv. basisstations of MANO-functies);

- Software speelt een grotere rol in 5G-apparatuur, waardoor de risico's in verband met de ontwikkeling en het bijwerken van software toenemen, nieuwe risico's op configuratiefouten ontstaan en de keuzes van de exploitanten van mobiele netwerken tijdens de uitrolfase van het netwerk van groter belang worden voor de beveiligingsanalyse;

b) Door deze nieuwe technologische kenmerken wordt de mate waarin exploitanten van mobiele netwerken afhankelijk zijn van derde leveranciers belangrijker, alsook hun rol in de 5G-toeleveringsketen.

Het gevolg is dat er aanvalspaden ontstaan die dreigingsactoren kunnen benutten, en met name actoren van buiten de EU of door staten gesteunde actoren, aangezien zij beschikken over capaciteiten (opzet en middelen) om telecommunicatienetwerken van EU-lidstaten aan te vallen, en dat de gevolgen van dergelijke aanvallen potentieel ernstiger worden.

Door de toegenomen blootstelling aan aanvallen die worden gefaciliteerd door derde leveranciers, zal het individuele risicoprofiel van de leveranciers bijzonder belangrijk worden, met name wanneer een leverancier sterk aanwezig is in bepaalde netwerken of gebieden.

c) Indien een leverancier in zeer grote mate afhankelijk is van één enkele leverancier, neemt de blootstelling toe en worden de gevolgen van een mogelijk verzuim van de leverancier ernstiger. Daarnaast kunnen zwakke punten zwaardere consequenties hebben die door dreigingsactoren kunnen worden benut, met name wanneer men afhankelijk is van een leverancier die een hoog risico vormt.

d) Zodra een aantal nieuwe gebruikssituaties voor 5G tot wasdom komen, zullen 5G-netwerken een belangrijk onderdeel vormen van de toeleveringsketen voor veel kritieke IT-toepassingen. Dat heeft gevolgen voor vereisten inzake vertrouwelijkheid en privacy. Verder zullen de integriteit en beschikbaarheid van deze netwerken belangrijke punten van zorg worden op het vlak van de nationale veiligheid en een belangrijke beveiligingsuitdaging op EU-niveau.

Bron: gecoördineerde EU-risicobeoordeling

In het gecoördineerde EU-risicobeoordelingsverslag wordt verder geconcludeerd dat deze uitdagingen een nieuw beveiligingsparadigma tot gevolg hebben, waardoor het noodzakelijk is het huidige beleids- en beveiligingskader voor de 5G-sector en het bijbehorende ecosysteem opnieuw te beoordelen en het voor de lidstaten van essentieel belang is de nodige risicobeperkende maatregelen te nemen.

Om de vastgestelde risico's doeltreffend aan te pakken en de beveiliging en weerbaarheid van 5G-netwerken te versterken, is een alomvattende aanpak vereist. Dat betekent dat er een reeks essentiële maatregelen en daarmee samenhangende ondersteunende acties moet worden ondernomen waarmee de risico's gelijktijdig worden aangepakt. Op basis van de gecoördineerde EU-risicobeoordeling werd bepaald welke risicobeperkende maatregelen op nationaal en Europees niveau kunnen worden toegepast.

In de conclusies van de Raad van 3 december 2019 werden de bevindingen van de gecoördineerde risicobeoordeling gesteund en nadruk gelegd op „het belang van een gecoördineerde aanpak en een doeltreffende uitvoering van de aanbeveling om versnippering in de eengemaakte markt te voorkomen"[15]. Daartoe riep de Raad de lidstaten, de Commissie en het Enisa op om „binnen hun bevoegdheidsgebieden alle nodige maatregelen te nemen om de beveiliging en integriteit van elektronische communicatienetwerken, met name 5G-netwerken, te waarborgen en verder te werken aan de consolidatie van een gecoördineerde aanpak om de beveiligingsproblemen in verband met 5G-technologieën aan te pakken."

4. De EU-toolbox inzake 5G-cyberbeveiliging

Op 29 januari 2020 heeft de NIS-samenwerkingsgroep de EU-toolbox voor risicobeperkende maatregelen gepubliceerd[16]. Daarin wordt ingegaan op alle risico's die in het gecoördineerde risicobeoordelingsverslag zijn vastgesteld.

In de EU-toolbox wordt een reeks strategische en technische maatregelen vastgesteld en beschreven alsmede bijbehorende ondersteunende acties ter versterking van de doeltreffendheid ervan, die kunnen worden ingevoerd om de vastgestelde risico's te beperken. Tot de **strategische maatregelen** behoren maatregelen voor meer regelgevende bevoegdheden op basis waarvan autoriteiten de aanschaf en uitrol van netwerken kunnen controleren, specifieke maatregelen voor het aanpakken van risico's in verband met niet-technische kwetsbaarheden alsmede mogelijke initiatieven ter bevordering van een duurzame en diverse leverings- en waardeketen voor 5G om systemische langetermijnrisico's op afhankelijkheid te vermijden. Tot de **technische maatregelen** behoren maatregelen om de beveiliging van 5G-netwerken en -apparatuur te versterken door de risico's als gevolg van technologieën en processen, maar ook menselijke en fysieke factoren aan te pakken. Bovendien voorziet de toolbox voor elk van de risicogebieden die in de gecoördineerde EU-risicobeoordeling zijn vastgesteld in **risicobeperkingsplannen** op basis van de meest doeltreffende maatregelen.

Verder wordt in de conclusies van de EU-toolbox, als overeengekomen door de NIS-samenwerkingsgroep, een reeks **belangrijke maatregelen** aanbevolen die door alle lidstaten en de Commissie moeten worden getroffen:

[15] Conclusies van de Raad over het belang van 5G voor de Europese economie en de noodzaak om de veiligheidsrisico's in verband met 5G te beperken. 3 december, 2019 14517/19 https://data.consilium.europa.eu/doc/document/ST-14517-2019-INIT/nl/pdf.

[16] Cyberbeveiliging van 5G-netwerken – EU-toolbox voor risicobeperkende maatregelen, 29 januari 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

Conclusies van de EU-toolbox

De EU-toolbox bevat een reeks maatregelen en acties die, wanneer ze juist worden gecombineerd en doeltreffend worden uitgevoerd, de basis vormen voor een gecoördineerde aanpak op dit gebied. Aangezien bij de gecoördineerde EU-risicobeoordeling uiteenlopende risicogebieden in kaart zijn gebracht, die bovendien verschillend van aard zijn, zal geen enkel type maatregel op zichzelf toereikend zijn en zullen in plaats daarvan verschillende maatregelen passend moeten worden gecombineerd om alle belangrijke risicogebieden aan te pakken.

Mogelijke risicobeperkingsplannen werden beoordeeld en er werd vastgesteld welke maatregelen het doeltreffendst zouden zijn, en op basis daarvan beveelt deze toolbox het volgende aan:

1. Alle lidstaten moeten ervoor 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, en zij 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 volgens een risicogebaseerde benadering en op grond van een reeks veiligheidsgerelateerde redenen.

Zij moeten met name:

- *de **beveiligingseisen** voor exploitanten van mobiele netwerken aanscherpen (bv. strenge toegangscontroles, regels voor veilige exploitatie en monitoring, beperkingen op het uitbesteden van specifieke functies enz.);*

- *het risicoprofiel van leveranciers beoordelen; en dus **relevante beperkingen toepassen voor leveranciers die worden geacht een hoog risico te vormen — met inbegrip van de nodige uitsluitingen om de risico's effectief te beperken — voor essentiële activa** die als kritiek en gevoelig worden gedefinieerd in de gecoördineerde EU-risicobeoordeling (bv. functies van het kernnetwerk, netwerkbeheers- en orkestratiefuncties, en toegangsnetwerkfuncties);*

- *ervoor zorgen dat elke exploitant een passende multivendor-strategie heeft om **verregaande afhankelijkheid** van individuele leveranciers (of leveranciers met een vergelijkbaar risicoprofiel) **te voorkomen of te beperken**, een passend evenwicht van leveranciers op nationaal niveau te garanderen en **afhankelijkheid van leveranciers die worden geacht een hoog risico te vormen te vermijden**; dit betekent ook dat een lock-in door bepaalde leveranciers moet worden voorkomen, onder andere door een grotere interoperabiliteit van apparatuur te bevorderen.*

2. De Europese Commissie moet samen met de lidstaten bijdragen aan:

- *de instandhouding van een **diverse en duurzame 5G-toeleveringsketen** om afhankelijkheid op langere termijn te vermijden, door*

  - *o ten volle gebruik te maken van de bestaande EU-instrumenten, met name door potentiële **buitenlandse directe investeringen** (BDI's) te screenen die betrekking hebben op essentiële 5G-activa, en **verstoringen** op de 5G-markt als gevolg van potentiële dumping of subsidies te voorkomen; en*

  - *o de **EU-capaciteiten op het gebied van 5G- en post-5G-technologieën** verder te versterken door middel van de relevante EU-programma's en -financiering;*

- *de coördinatie tussen de lidstaten op het gebied van **normalisatie** te vergemakkelijken zodat specifieke veiligheidsdoelstellingen worden verwezenlijkt, en **passende certificeringsregelingen voor de hele EU** te ontwikkelen ter bevordering van veiligere producten en processen.*

3. Om ervoor te zorgen dat deze gecoördineerde aanpak de tijd trotseert, moet het mandaat van de actielijn van de NIS-samenwerkingsgroep worden verlengd, evenals de samenwerking met andere betrokken instanties en entiteiten, met name om:

- ***de nationale en Europese risicobeoordelingen*** *inzake de beveiliging van 5G- en post-5G-netwerken periodiek te evalueren – met steun van de Commissie en het Enisa – waarbij de gevolgde beoordelingsmethode nader wordt uitgewerkt en aangepast naarmate de 5G-technologie zich ontwikkelt;*

- ***de tenuitvoerlegging van de toolbox diepgaand en periodiek te monitoren en te evalueren*** *op basis van een gestructureerde verslaglegging door de lidstaten;*

- *de uitvoering van* ***ondersteunende acties*** *die samenwerking op EU-niveau vereisen, te coördineren en te ondersteunen, met name voor de opstelling van richtsnoeren en de uitwisseling van beste praktijken inzake de verschillende maatregelen;*

- *verdere coördinatie op EU-niveau, waar passend, te ondersteunen, met name om de* ***technische en organisatorische beveiligingseisen voor netwerkexploitanten*** *meer gelijklopend te maken.*

Bron: EU-toolbox.

De conclusies van de toolbox duiden erop dat de lidstaten vastbesloten zijn gezamenlijk te reageren op de beveiligingsuitdagingen in verband met 5G-netwerken. Dit is van fundamenteel belang voor de veiligheid in de lidstaten en in de hele EU, voor de nationale economieën en voor de interne markt van de EU, en voor de technologische soevereiniteit van Europa. Zowel uit de gecoördineerde EU-risicobeoordeling als uit de EU-toolbox blijkt dat er zeer waardevol collectief werk is verricht in de NIS-samenwerkingsgroep, met intensieve samenwerking tussen vertegenwoordigers van alle lidstaten, de Commissie en het Enisa.

De toolbox maakt een gemeenschappelijke EU-aanpak van 5G-cyberbeveiliging mogelijk, zorgt door middel van EU-beleid en -coördinatie voor samenhang binnen de interne markt en steunt de lidstaten in de uitoefening van hun bevoegdheden, met name op het gebied van de nationale veiligheid. Aan de hand van de risicobeperkende maatregelen en risicobeperkingsplannen in de toolbox kan de EU de gemeenschappelijke uitdagingen op het gebied van 5G-cyberbeveiliging passend, doeltreffend en evenredig beantwoorden.

De Commissie is tevreden met de publicatie van de EU-toolbox inzake 5G-cyberbeveiliging en steunt ten volle alle bovenstaande conclusies.

De Commissie roept de lidstaten en de betrokken instellingen, agentschappen en andere organen van de Unie op om:

i) te zorgen voor een snelle invoering van doeltreffende en passende risicobeperkende strategieën in de hele EU, in overeenstemming met de EU-toolbox, en

ii) alle noodzakelijke verdere stappen te ondernemen om de coördinatie op het niveau van de Unie te waarborgen, onder meer door de werkzaamheden in de NIS-samenwerkingsgroep voort te zetten en een robuust mechanisme op te zetten waarmee toezicht wordt gehouden op de uitvoering van de EU-toolbox, zodat de doeltreffendheid van de maatregelen en de soepele werking van de interne markt worden gewaarborgd.

5. Uitvoering van de toolbox

Voor een geloofwaardige en succesvolle Europese aanpak van 5G-beveiliging is het cruciaal dat de lidstaten vastbesloten zijn om de toolbox ten volle te benutten. Hoewel de lidstaten rekening houdend met nationale omstandigheden zullen beslissen of een bepaalde maatregel geschikt is, is het absoluut noodzakelijk dat een **reeks belangrijke maatregelen, zoals aanbevolen door de NIS-samenwerkingsgroep (zie bovenstaande conclusies van de toolbox), in elke lidstaat wordt ingevoerd en dat bepaalde maatregelen op EU-niveau worden ingevoerd** zodat de gesignaleerde risico's worden aangepakt.

De Commissie staat klaar om ook in de volgende fasen haar volledige steun te verlenen en verzoekt de lidstaten om:

- **uiterlijk tegen 30 april 2020** concrete en meetbare stappen te zetten om de in de conclusies van de EU-toolbox aanbevolen reeks kernmaatregelen te nemen;

- **uiterlijk tegen 30 juni 2020** een verslag van de NIS-samenwerkingsgroep op te stellen over de stand van de uitvoering van deze belangrijke maatregelen in elke lidstaat, op basis van de regelmatige verslaglegging en monitoring, met name binnen de NIS-samenwerkingsgroep, met de steun van de Commissie en het Enisa.

5.1. Een op risico's gebaseerde, gecoördineerde aanpak voor 5G-leveranciers

Aangezien het uiteindelijke doel is om de beveiliging, weerbaarheid en duurzaamheid van de 5G-netwerken te waarborgen, zijn de lidstaten het erover eens dat het risicoprofiel van individuele leveranciers moet worden beoordeeld en dat er, als gevolg daarvan, met betrekking tot essentiële activa relevante beperkingen moeten worden toegepast voor leveranciers die worden geacht een hoog risico te vormen, met inbegrip van de nodige uitsluitingen om de risico's effectief te beperken, zoals aangegeven in de toolbox. De Commissie staat klaar om de lidstaten bij de uitvoering van deze maatregelen te ondersteunen.

Hiertoe bieden ook de gecoördineerde EU-risicobeoordeling en de EU-toolbox richtsnoeren voor de beoordeling van 1) het risicoprofiel van leveranciers[17] en 2) de gevoeligheid van netwerkelementen en -functies[18] alsook van andere activa. Zowel met de gecoördineerde EU-risicobeoordeling als de maatregelen in de toolbox worden de risico's afgedekt die verband houden met de leveranciers van 5G-netwerkapparatuur en -netwerkdiensten. Geen van beide heeft betrekking op de andere producten of diensten die deze of andere leveranciers kunnen verlenen.

Zoals bepaald in paragraaf 2.37 van de gecoördineerde EU-risicobeoordeling kunnen de risicoprofielen van individuele leveranciers worden beoordeeld op basis van verschillende factoren.

De beoordeling van de risicoprofielen van leveranciers moet uitsluitend om veiligheidsredenen en op basis van objectieve criteria worden uitgevoerd. Om een

[17] Paragraaf 2.37 van de gecoördineerde EU-risicobeoordeling.

[18] Paragraaf 2.21 van de gecoördineerde EU-risicobeoordeling bevat de belangrijkste categorieën elementen en functies en hun algemene gevoeligheidsgraad, en bevat voor elke categorie een lijst met essentiële elementen die door de lidstaten zijn vastgesteld. In paragrafen 2.28 en 2.29 staan een aantal andere soorten gevoelige activa of gebieden (bijvoorbeeld specifieke entiteiten of geografische gebieden).

gecoördineerde aanpak van de uitvoering van deze maatregelen te vergemakkelijken, wordt in de toolbox aanbevolen dat de lidstaten informatie uitwisselen over nationale benaderingen en beste praktijken. Voorts is de Commissie van mening dat deze actie een van de eerste prioriteiten moet zijn in de volgende fase van de werkzaamheden die binnen de NIS-samenwerkingsgroep worden uitgevoerd samen met de Commissie en het Enisa.

Het is belangrijk dat beperkende maatregelen ten aanzien van leveranciers die worden geacht een hoog risico te vormen, met inbegrip van de nodige uitsluitingen om de risico's effectief te beperken, alsook maatregelen om afhankelijkheid van deze leveranciers te voorkomen, tijdig worden genomen. Als dit in een zo vroeg mogelijk stadium gebeurt – waar mogelijk ook met betrekking tot vergunningsprocessen voor 5G-frequenties – biedt dit de marktdeelnemers meer voorspelbaarheid, wat bijdraagt aan een snelle uitrol van 5G-netwerken, en worden de langetermijnbeveiliging van 5G-netwerken en de weerbaarheid van de 5G-toeleveringsketen gewaarborgd.

Tegelijk kunnen voor de nationale uitvoering van deze maatregelen, indien noodzakelijk en gerechtvaardigd, andere termijnen worden vastgesteld, met name indien er reeds een hoge mate van afhankelijkheid bestaat van apparatuur of diensten van leveranciers die worden geacht een hoog risico te vormen (bijvoorbeeld door rekening te houden met de upgradecycli van apparatuur, met name voor de migratie van "niet-standalone" naar "standalone" 5G-netwerken). De lidstaten zouden kunnen overwegen om uitvoeringsplannen op te stellen, eventueel met passende overgangsperioden voor de betrokken netwerkexploitanten. In dit verband moeten overgangsperioden zodanig worden vastgesteld dat de stimulansen behouden blijven of zelfs worden versterkt om in moderne netwerkapparatuur te investeren, onder meer door de uitrol van volwaardige ("standalone") 5G-kernnetwerken en de vervanging van bestaande 4G-apparatuur in andere delen van de netwerken (bijvoorbeeld in het radiotoegangsnetwerk) te versnellen, overeenkomstig de doelstellingen van het 5G-actieplan[19].

Bovendien zou het kunnen dat telecomexploitanten vanwege de complexiteit van de op software gebaseerde 5G-netwerken in toenemende mate beroep zullen doen op derde partijen, niet alleen voor de levering van netwerkapparatuur, maar ook voor de uitvoering van bepaalde taken, zoals het onderhoud en de upgrade van 5G-netwerken en -software, en andere uitbestede diensten. Zoals beschreven in de gecoördineerde EU-risicobeoordeling is dit een ernstig veiligheidsrisico. Daarom moet hier bijzondere aandacht aan worden besteed. Het is van essentieel belang dat ook het risicoprofiel van de leveranciers van dergelijke diensten, met name wanneer deze taken niet in de EU worden uitgevoerd, aan een grondige veiligheidsbeoordeling wordt onderworpen. Om de integriteit van de 5G-infrastructuur op lange termijn te vrijwaren, moeten er passende maatregelen worden genomen, zoals de toepassing van beperkingen op met name gevoelige delen van de 5G-netwerken of de noodzakelijke uitsluiting van entiteiten met een hoog risico, in overeenstemming met de risicobeperkende maatregelen van de toolbox.

5,2. De rol van de Commissie bij de ondersteuning van de uitvoering van de toolbox

De Commissie zal de uitvoering van de EU-aanpak inzake 5G-cyberbeveiliging in het algemeen blijven ondersteunen, en zal specifieke initiatieven nemen met betrekking tot de

[19] COM(2016) 588 final van 14.9.2016 "5G voor Europa: een actieplan"

maatregelen en doelstellingen van de toolbox indien deze een meerwaarde kunnen betekenen. De Commissie zal haar bevoegdheden en relevante instrumenten voor zover nodig ten volle benutten om de vastgestelde veiligheidsoverwegingen aan te pakken. Op die manier, en door samen te werken met de lidstaten en de particuliere sector, streeft de Commissie ernaar strategische maatregelen te ondersteunen die zullen bijdragen aan de technologische soevereiniteit van de EU en het leiderschap van de EU bij de toekomstige ontwikkeling van netwerktechnologieën, op het gebied van cyberbeveiligingstechnologieën en met betrekking tot alle relevante bouwstenen waar onze hele economie en beveiliging van afhangen.

Meer in het bijzonder zal de Commissie, met het oog op de uitvoering van de overeenkomstige risicobeperkende maatregelen in de toolbox die onder haar bevoegdheid vallen, het volgende ondernemen:

Het waarborgen van de cyberbeveiliging van 5G-netwerken en van een gediversifieerde 5G-waardeketen:

- **Samenwerking op het gebied van cyberbeveiliging**: Steun blijven verlenen aan de lidstaten voor de doeltreffende, gecoördineerde en tijdige uitvoering van nationale maatregelen via de NIS-samenwerkingsgroep.

- **Telecom- en cyberbeveiligingsregels**: Steun verlenen voor de uitvoering van toolboxmaatregelen die betrekking hebben op beveiligingseisen, met name als het gaat om relevante bepalingen in het kader van de Europese regels inzake elektronische communicatie, de toegevoegde waarde overwegen van mogelijke uitvoeringshandelingen met gedetailleerde technische en organisatorische beveiligingsmaatregelen tot aanvulling van de nationale regels, en de doeltreffendheid en consistentie van de aan de exploitanten opgelegde beveiligingsmaatregelen vergroten.

- **Normalisatie**: Actie ondernemen om de Europese deelname aan de respectieve normalisatie-instellingen te handhaven en zo nodig te vergroten, teneinde de Europese doelstellingen inzake beveiliging en interoperabiliteit te verwezenlijken. De Commissie zal meer bepaald samen met de lidstaten zorgen voor de beoordeling en bevordering van de technische specificaties en normen die interoperabiliteit mogelijk maken tussen leveranciers van 5G-apparatuur in verschillende delen van het netwerk, met inbegrip van oudere netwerken, zodat er een echte multi-vendoromgeving ontstaat, bijvoorbeeld door middel van open, interoperabele interfaces.

- **Certificering**: De ontwikkeling van 5G-certificeringsregelingen ondersteunen om te voldoen aan de behoeften van 5G-netwerken in het EU-kader voor cyberbeveiligingscertificering.

- **Screening van buitenlandse directe investeringen (BDI's)**: De uitvoering van het EU-screeningkader ondersteunen door de 5G-waardeketen in kaart te brengen, met inbegrip van gevoelige netwerkactiva, en buitenlandse directe investeringen in de waardeketen regelmatig monitoren. In overeenstemming met het tijdschema voor de screening van BDI's (vanaf oktober 2020) zal de Commissie buitenlandse investeringen op het gebied van 5G onderzoeken volgens de richtsnoeren van Verordening (EU) 2019/452, rekening houdend met de gecoördineerde EU-risicobeoordeling en de EU-toolbox.

- **Handelsbeschermingsinstrumenten**: Alle relevante marktontwikkelingen in de EU en in derde landen volgen en EU-actoren op de Europese 5G-markt beschermen met

handelsbeschermende maatregelen tegen mogelijke handelsverstorende praktijken (dumping of subsidiëring), met onder meer de instelling van vooronderzoeken indien nodig.

- **Mededingingsregels:** Toezicht houden op de werking van de markten voor de levering van 5G-hardware en -software om de vrije concurrentie te waarborgen, onder meer ten aanzien van potentiële contractuele of technische lock-ins.

- **EU-financieringsprogramma's**: Ervoor zorgen dat alleen aan EU-financieringsprogramma's op relevante technologiegebieden kan worden deelgenomen als aan beveiligingseisen wordt voldaan, door voluit gebruik te maken van en verdere uitvoering te geven aan beveiligingsvoorwaarden in O&I-programma's, met name in Horizon Europa, het programma Digitaal Europa en Connecting Europe Facility 2, in de Europese structuur- en investeringsfondsen en in andere relevante programma's. Een soortgelijke aanpak moet ook worden gevolgd voor de externe financieringsprogramma's en financiële instrumenten van de EU, onder meer met betrekking tot de financiering die via internationale financiële instellingen wordt verstrekt.

- **Overheidsopdrachten:** Overheidsopdrachten op het gebied van 5G-netwerken gebruiken ter ondersteuning van vastgestelde doelstellingen op het gebied van beveiliging, diversiteit van leveranciers en duurzaamheid op lange termijn van 5G-netwerken; er moet met name naar worden gestreefd dat bij de gunning van overheidsopdrachten in verband met 5G-netwerken terdege rekening wordt gehouden met beveiligingsaspecten, overeenkomstig de EU-regels inzake overheidsopdrachten.

- **Crisisrespons en -beheersing (blauwdruk) en cyberoefeningen**: Ten volle gebruikmaken van de ontwikkeling van de blauwdruk van de EU[20] voor de gecoördineerde respons op grootschalige cyberincidenten. Samen met het Enisa ook de mogelijkheid overwegen om een 5G-cyberoefening uit te voeren zodra de marktrijpheid het toelaat.

En onder de verantwoordelijkheid van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid en vicevoorzitter van de Commissie, en de Raad:

- **Kader voor gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten (instrumentarium voor cyberdiplomatie)[21]**: In het geval van kwaadwillige cyberactiviteiten die de integriteit en veiligheid van de EU bedreigen, worden de lidstaten aangemoedigd om gebruik te maken van de relevante maatregelen op het gebied van het gemeenschappelijk buitenlands en veiligheidsbeleid die deel zijn van het EU-instrumentarium voor cyberdiplomatie (inclusief, indien nodig, beperkende maatregelen), om samenwerking aan te moedigen, de beperking van bedreigingen te vergemakkelijken en het gedrag van potentiële agressors te beïnvloeden.

Bovendien zal een aantal programma's aan het vermijden of beperken van het risico van langdurige afhankelijkheid bijdragen door een gediversifieerde en duurzame 5G-markt te bevorderen, onder meer door de capaciteit van de EU in de 5G-waardeketen te handhaven en in innovatie te investeren, in overeenstemming met de internationale verplichtingen van de EU.

[20] Aanbeveling EU 2017/1584 van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises.
[21] Conclusies van de Raad van 20 november 2017 (9916/17).

Bevordering van innovatie en investeringen in cyberbeveiliging en netwerkinfrastructuurtechnologieën:

- **EU-financieringsprogramma's**: Zorgen voor meer investeringen in onderzoek, innovatie en de uitrol van netwerktechnologieën en relevante onderliggende bouwstenen. De Commissie heeft in het kader van de volgende EU-begroting 2021-2027 voorgesteld om bijna 3 miljard euro te investeren in cyberbeveiligingstechnologieën. Het gaat daarbij onder meer om onderzoek en innovatie in het kader van Horizon Europa en steun voor cyberbeveiligingscapaciteiten in het kader van het programma Digitaal Europa. InvestEU kan ook financiële steun verlenen voor onderzoek en ontwikkeling op het gebied van 5G en de uitrol ervan ondersteunen.

Bovendien heeft de Commissie in het kader van het volgende Horizon Europa-programma[22] voorgesteld een geïnstitutionaliseerd Europees partnerschap voor NGI/6G op te zetten ("Slimme netwerken en diensten"), in samenwerking met het bedrijfsleven en gecoördineerd met de lidstaten om de uitrol van 5G te voltooien en voornamelijk om **voorbereidingen te treffen voor 6G**, de volgende generatie mobiele technologie. Er wordt voorgesteld om meer dan 2,5 miljard euro uit de EU-begroting 2021-2027 te investeren, aangevuld met ten minste 7,5 miljard euro aan particuliere investeringen in dit initiatief.

- **Industriële ontwikkeling en uitrol**: Het evalueren van potentiële marktlacunes of -tekortkomingen in de 5G-waardeketen die gerichte acties in het kader van de volgende langetermijnbegroting of in het kader van mogelijke belangrijke projecten van gemeenschappelijk Europees belang (IPCEI) op het gebied van cyberbeveiliging zouden rechtvaardigen, in overeenstemming met de voorstellen van het IPCEI-forum op hoog niveau. Het besluit om belangrijke projecten van gemeenschappelijk Europees belang te ontwerpen en op te zetten ligt in handen van lidstaten en bedrijven. De EU-regels bieden een gunstig kader en de Commissie staat paraat om de noodzakelijke contacten te faciliteren en richtsnoeren te verstrekken.

[22] Financiering kan ook worden verstrekt uit CEF 2.0 en Digitaal Europa.

6. Conclusie

Van 5G-netwerken wordt verwacht dat zij de Europese burgers, de maatschappij en de economie een hele reeks kansen zullen bieden. Het is daarom van essentieel belang dat de beveiliging en schokbestendigheid van 5G-netwerken wordt gewaarborgd. Tegelijkertijd zijn cyberdreigingen (waaronder het risico van inmenging door actoren van buiten de EU of door staten gesteunde actoren) in voortdurende ontwikkeling en zijn deze een steeds groter probleem door de toegenomen afhankelijkheid van technologie en gegevens. Door onvoldoende aandacht te besteden aan cyberbeveiliging zou het vertrouwen in de ontwikkeling van de digitale economie en samenleving worden ondermijnd en zou de EU niet ten volle van de voordelen ervan profiteren. Dit betekent dat de manier waarop er gereageerd wordt gelijke tred moet houden met de cyberdreigingen.

Een gecoördineerde en consequente aanpak van cyberbeveiliging in de EU met betrekking tot kritieke technologieën en netwerken is van essentieel belang wil de EU haar technologische soevereiniteit waarborgen en de industriële capaciteit in stand houden en ontwikkelen. De Commissie zal de uitvoering van de Europese aanpak van 5G-cyberbeveiliging ten volle ondersteunen en ervoor zorgen dat de EU-markten open blijven voor producten en diensten die voldoen aan de zich ontwikkelende eisen inzake cyberbeveiliging en vertrouwen.

Daartoe is het van belang dat wanneer het om 5G-beveiliging gaat alle belanghebbenden zich vastberaden blijven inzetten en dat de lidstaten, de Commissie en het Enisa blijven samenwerken.

Als eerstvolgende stap roept de Commissie, zoals hierboven uiteengezet, de lidstaten op snel actie te ondernemen om de in het kader van de toolbox overeengekomen maatregelen doeltreffend en objectief ten uitvoer te leggen en om, met de steun van de Commissie en het Enisa, samen te blijven werken aan de coördinatie op EU-niveau. Tegelijkertijd zal de Commissie alle relevante acties lanceren die onder haar bevoegdheid vallen om de uitvoering van de toolbox door de lidstaten te ondersteunen en de impact ervan te versterken.

Aanhangsel: Risicocategorieën (bron: gecoördineerde EU-risicobeoordeling)

	Risicocategorieën
Risicoscenario's in verband met ontoereikende beveiligingsmaatregelen	*R1: Onjuiste configuratie van netwerken*
	R2: Gebrek aan toegangscontroles
Risicoscenario's in verband met de 5G-toeleveringsketen	*R3: Lage productkwaliteit*
	R4: Afhankelijkheid van één enkele leverancier binnen afzonderlijke netwerken of gebrek aan diversiteit op landelijk niveau
Risicoscenario's in verband met de modus operandi van de voornaamste dreigingsactoren	*R5: Staatsinmenging via de 5G-toeleveringsketen*
	R6: Exploitatie van 5G-netwerken door de georganiseerde misdaad of een criminele organisatie, gericht op eindgebruikers
Risicoscenario's in verband met onderlinge afhankelijkheid tussen 5G-netwerken en andere kritieke systemen	*R7: Aanzienlijke verstoring van kritieke infrastructuren of diensten*
	R8: Massale uitval van netwerken als gevolg van een onderbreking van de elektriciteitslevering of andere ondersteunende systemen
Risicoscenario's in verband met eindgebruikersapparatuur	*R9: Misbruik via het internet van de dingen*