NL 2022

03

Speciaal verslag

Uitrol van 5G in de EU:

vertragingen bij de invoering van netwerken, waarbij beveiligingskwesties nog niet zijn opgelost

CURIA RATIONUM

EUROPESE REKENKAMER

Inhoud

Samenvatting

I De “vijfde generatie” telecommunicatiesystemen, ofwel 5G, is een nieuwe wereldwijde draadloze norm die een veel hogere gegevenscapaciteit en transmissiesnelheid biedt. 5G-diensten zijn essentieel voor een breed scala van innovatieve toepassingen die het potentieel hebben om tal van sectoren van onze economieën te transformeren en het dagelijkse leven van burgers te verbeteren. 5G is dan ook van strategisch belang voor de hele eengemaakte markt.

II In haar 5G-actieplan van 2016 heeft de Commissie de doelstelling geformuleerd om tegen 2025 te zorgen voor ononderbroken 5G-dekking in stedelijke gebieden en op belangrijke transportroutes. In maart 2021 heeft zij de doelstelling uitgebreid tot 5G-dekking in alle bevolkte gebieden uiterlijk in 2030.

III Hoewel 5G veel groeimogelijkheden kan bieden, zijn er bepaalde risico’s aan verbonden. In haar aanbeveling van 2019 inzake 5G-cyberbeveiliging waarschuwde de Commissie dat wanneer veel essentiële diensten afhankelijk worden van 5G-netwerken, wijdverspreide storingen bijzonder ernstige gevolgen zouden kunnen hebben. Voorts zou door de grensoverschrijdende aard van de dreigingen in kwestie elk significant zwak punt en/of elk cyberincident in één bepaalde lidstaat gevolgen hebben voor de EU als geheel. Een van de resultaten van de aanbeveling van de Commissie was de EU-toolbox voor 5G-cyberbeveiliging (“toolbox”), die in januari 2020 werd vastgesteld.

IV In de hele EU zouden de totale kosten van de invoering van 5G kunnen oplopen tot 400 miljard EUR. In de periode 2014-2020 heeft de EU financiering ten bedrage van meer dan 4 miljard EUR verstrekt voor 5G-projecten.

V Wij hebben onderzocht of de Commissie de lidstaten doeltreffend heeft ondersteund bij het verwezenlijken van de EU-doelstellingen voor de uitrol van hun 5G-netwerken en bij het op gecoördineerde wijze aanpakken van kwesties inzake de beveiliging van 5G. We beoordeelden aspecten in verband met zowel de implementatie van 5G-netwerken, waarvoor 2020 een cruciaal jaar was, als de beveiliging daarvan. Met dit verslag willen wij inzichten en aanbevelingen verschaffen voor de tijdige invoering van veilige 5G-netwerken in alle EU-landen. Onze controle was toegespitst op de Commissie, maar wij onderzochten ook de rol van nationale overheidsdiensten en andere actoren.

VI Uit onze controle bleek dat er vertragingen zijn bij de uitrol van 5G-netwerken door de lidstaten. Eind 2020 hadden 23 lidstaten commerciële 5G-diensten ingevoerd en hadden zij de tussentijdse doelstelling behaald dat ten minste één grote stad toegang tot 5G heeft. Niet alle lidstaten verwijzen echter naar de doelstellingen van de EU voor 2025 en 2030 in hun nationale 5G-strategieën of breedbandplannen. In verschillende landen is het Europees wetboek voor elektronische communicatie bovendien nog niet in nationaal recht omgezet en heeft de toewijzing van 5G-frequenties vertraging opgelopen. Deze vertragingen bij de toewijzing van de frequenties kunnen worden toegeschreven aan verschillende oorzaken: een geringe vraag van mobiele-netwerkexploitanten, grensoverschrijdende coördinatieproblemen met niet-EU-landen langs de oostgrenzen, de impact van COVID-19 op de geplande veilingen en onzekerheid over de aanpak van beveiligingskwesties. De mate waarin de lidstaten achterlopen bij de implementatie van 5G brengt de verwezenlijking van de EU-doelstellingen in gevaar. De Commissie heeft de lidstaten steun verleend voor de uitvoering van het 5G-actieplan van 2016 door middel van wetgevingsinitiatieven (zowel “hard law” als “soft law”), richtsnoeren en de financiering van 5G-gerelateerd onderzoek. De Commissie heeft echter de verwachte kwaliteit van 5G-diensten niet duidelijk omschreven.

VII In de EU-toolbox voor 5G-cyberbeveiliging wordt een aantal strategische, technische en ondersteunende maatregelen beschreven om bedreigingen voor de veiligheid van het 5G-netwerk aan te pakken en worden de relevante actoren voor elk van deze maatregelen aangewezen. Verscheidene maatregelen hebben betrekking op leveranciers van 5G-apparatuur die een hoog risico inhouden. Deze toolbox werd bekrachtigd door de Commissie en de Europese Raad. De criteria in de toolbox bieden een operationeel kader dat nuttig is om het risicoprofiel van leveranciers in alle lidstaten op gecoördineerde wijze te beoordelen. Tegelijkertijd blijft het uitvoeren van deze beoordeling een nationale verantwoordelijkheid. De toolbox werd in een vroeg stadium van de invoering van 5G vastgesteld, maar een aantal mobiele-netwerkexploitanten had al leveranciers geselecteerd. Sinds de goedkeuring van de toolbox is vooruitgang geboekt met het versterken van de beveiliging van 5G-netwerken, waarbij een meerderheid van de lidstaten beperkingen toepast of zal toepassen op leveranciers met een hoog risico. In de komende jaren kan wetgeving inzake 5G-beveiliging die door de lidstaten wordt vastgesteld op basis van de toolbox, leiden tot meer convergente benaderingen van 5G-leveranciers met een hoog risico. Aangezien geen van de voorgestelde maatregelen juridisch bindend is, is de Commissie echter niet bevoegd deze te handhaven. Daarom blijft het risico bestaan dat de toolbox op zich geen garantie is voor een gecoördineerde aanpak door de lidstaten van de netwerkbeveiligingsaspecten.

VIII De Commissie heeft een aanvang gemaakt met het aanpakken van de kwestie van buitenlandse subsidies aan 5G-leveranciers, waaraan mogelijke gevolgen voor de beveiliging kleven. De Commissie beschikt niet over voldoende informatie over de behandeling door de lidstaten van potentiële vervangingskosten die zouden kunnen ontstaan als mobiele-netwerkexploitanten apparatuur van leveranciers met een hoog risico zonder een overgangsperiode van EU-netwerken zouden moeten verwijderen.

IX Wij bevelen de Commissie aan om:

- de gelijkmatige en tijdige invoering van 5G-netwerken in de EU te bevorderen;
- een gecoördineerde aanpak van de beveiliging van 5G onder de lidstaten te bevorderen, en
- de aanpak van de lidstaten inzake de beveiliging van 5G te monitoren en de impact van verschillen hierbij op de doeltreffende werking van de eengemaakte markt te beoordelen.

Inleiding

Aard en belang van 5G

01 De “vijfde generatie” telecommunicatiesystemen, ofwel 5G, is een nieuwe wereldwijde draadloze norm. In vergelijking met de 3G- en 4G-netwerken biedt 5G een veel hogere gegevenscapaciteit en transmissiesnelheid. 5G omvat een aantal netwerkelementen die zijn gebaseerd op vorige generaties mobiele en draadloze communicatietechnologie, maar vormt geen geleidelijke verdere ontwikkeling van deze netwerken. 5G biedt universele connectiviteit met ultrahoge bandbreedte en een lage latentietijd voor individuele gebruikers en verbonden apparaten.

02 Met 5G zullen meer apparaten dan ooit tevoren met elkaar in verbinding staan in het “internet der dingen”. Eind 2018 waren er wereldwijd naar schatting 22 miljard verbonden apparaten in gebruik. Verwacht wordt dat dit aantal tegen 2030 tot ongeveer 50 miljard zal zijn gestegen[1], waardoor een enorm web van onderling verbonden apparaten zal ontstaan dat alles van smartphones tot keukenapparaten omvat. Het wereldwijde verbruik van data zal naar verwachting een sprong maken van 12 exabytes aan mobiel dataverkeer per maand in 2017[2] tot meer dan 5 000 exabytes in 2030[3].

03 5G-diensten zijn essentieel voor een breed scala van innovatieve toepassingen die het potentieel hebben om tal van sectoren van de EU-economie te transformeren en het dagelijkse leven van burgers te verbeteren (zie ***figuur 1***). Uit een studie uit 2017 die in opdracht van de Commissie is uitgevoerd, blijkt dat de invoering van 5G in vier belangrijke strategische industriële sectoren (de automobielindustrie, gezondheidzorg, vervoer en energie) een profijt van wel 113 miljard EUR per jaar zou kunnen opleveren[4]. In deze studie wordt ook de verwachting uitgesproken dat door de implementatie van 5G 2,3 miljoen banen in de lidstaten zouden kunnen worden

---

1 Statista, Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030.

2 Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017-2022, februari 2019.

3 ITU-R, IMT traffic estimates for the years 2020 to 2030.

4 Identification and quantification of key socio-economic data to support strategic planning for the introduction of 5G in Europe, februari 2017.

gecreëerd. In een studie uit 2021 werd geraamd dat 5G tussen 2021 en 2025 het Europese bruto binnenlands product (bbp) met 1 biljoen EUR zou verhogen voor die periode en dat met 5G in potentie 20 miljoen banen konden worden gecreëerd of getransformeerd in alle sectoren van de economie[5].

Figuur 1 — 5G zal alle aspecten van ons leven bestrijken

Bron: Europese Commissie.

Veiligheidskwesties

04 Hoewel 5G veel groeimogelijkheden kan bieden, zijn er bepaalde risico's aan verbonden (zie ***bijlage I***, waarin de belangrijkste mogelijkheden en risico's van 5G worden uiteengezet). Bedreigingen voor de veiligheid behoren tot die risico's. Telecommunicatiesystemen stonden altijd al bloot aan het risico van cyberaanvallen in (zie ***bijlage II***)[6]. Beveiligingskwesties zijn een bijzonder punt van zorg wat betreft 5G, omdat het meer aanvalsmogelijkheden biedt dan 3G- of 4G-telecommunicatiesystemen vanwege de aard van de technologie en met name de afhankelijkheid ervan van software[7].

---

[5] Accenture Strategy, The Impact of 5G on the European Economy, februari 2021.

[6] Evaluatie nr. 02/2019: Uitdagingen voor een doeltreffend EU-beleid inzake cyberbeveiliging (Briefingdocument); Controlecompendium 2020 van het Contactcomité — Cyberbeveiliging, en Onderzoeksdienst van het Europees Parlement — European Science-Media hub.

[7] NIS-samenwerkingsgroep, EU coordinated risk assessment of the cybersecurity of 5G networks, 9 October 2019. punt 3.4.

05 Aangezien 5G-netwerken naar verwachting de ruggengraat zullen worden van een breed scala van diensten en toepassingen, zal de beschikbaarheid van die netwerken een belangrijke veiligheidsuitdaging worden op nationaal en EU-niveau. Als hackers een 5G-netwerk binnendringen, kunnen zij de kernfuncties ervan compromitteren om diensten te verstoren of de controle te grijpen over kritieke infrastructuur (bijvoorbeeld elektriciteitsnetten), die in de EU vaak een grensoverschrijdende dimensie heeft. In studies wordt geraamd dat de economische impact van cybercriminaliteit wereldwijd kan oplopen tot wel 5 000 miljard EUR per jaar, d.w.z. meer dan 6 % van het wereldwijde bbp in 2020[8].

06 Een andere uitdaging op het gebied van de beveiliging van 5G is de kritieke rol van een beperkt aantal leveranciers bij het bouwen en exploiteren van 5G-netwerken. Dit verhoogt de blootstelling aan potentiële verstoring van de levering wanneer er sprake is van afhankelijkheid van één enkele leverancier — met name als deze leverancier een hoog risico vormt — bijvoorbeeld omdat deze blootstaat aan inmenging van een niet-EU-land. In 2019 heeft de NIS-samenwerkingsgroep (NIS — netwerk- en informatiesystemen), die is samengesteld uit vertegenwoordigers van de lidstaten en van EU-organen, gewezen op het risico dat “vijandige overheidsactoren” gemakkelijk toegang krijgen tot een 5G-netwerk, hetzij via geprivilegieerde toegang, hetzij door druk uit te oefenen op een leverancier of door zich te beroepen op nationale wettelijke voorschriften[9] (zie ***kader 1***). Tegen deze achtergrond is de EU begonnen met het ontwikkelen van initiatieven op het gebied van de beveiliging van 5G.

[8] Wereld Economisch Forum, Wild Wide Web — Consequences of Digital Fragmentation, 2021.

[9] NIS-samenwerkingsgroep, EU coordinated risk assessment of the cybersecurity of 5G networks, 9 October 2019.

Kader 1

Veiligheidskwesties in verband met de samenwerking tussen de EU en China op het gebied van 5G

- In 2015 heeft de EU een gezamenlijke verklaring met China ondertekend over strategische samenwerking op het gebied van 5G, waarin zij zich verbinden tot wederkerigheid en openheid wat betreft de toegang tot financiering voor onderzoek inzake 5G-netwerken en markttoegang[10].

- In 2017 heeft China een nationale inlichtingenwet aangenomen die bepaalt dat alle Chinese organisaties en burgers moeten meewerken aan nationale inlichtingen, en de geheimhouding ervan moeten waarborgen[11]. In reactie daarop hebben de VS in 2018 acties ondernomen ter beperking van de activiteiten van verschillende Chinese bedrijven, waaronder Huawei, een belangrijke 5G-leverancier.

In maart 2019 heeft het Europees Parlement ook zijn bezorgdheid geuit over het feit dat Chinese 5G-leveranciers vanwege de wetgeving van hun land van herkomst een veiligheidsrisico voor de EU zouden kunnen vormen.

07 Ook de vertrouwelijkheid en de privacy kunnen op het spel staan, aangezien telecomexploitanten hun gegevens vaak aan datacentra uitbesteden. Het risico bestaat dat deze gegevens worden opgeslagen op apparatuur van 5G-leveranciers, die zich in niet-EU-landen bevindt met andere niveaus van juridische en gegevensbescherming dan binnen de EU.

5G-initiatieven op EU-niveau

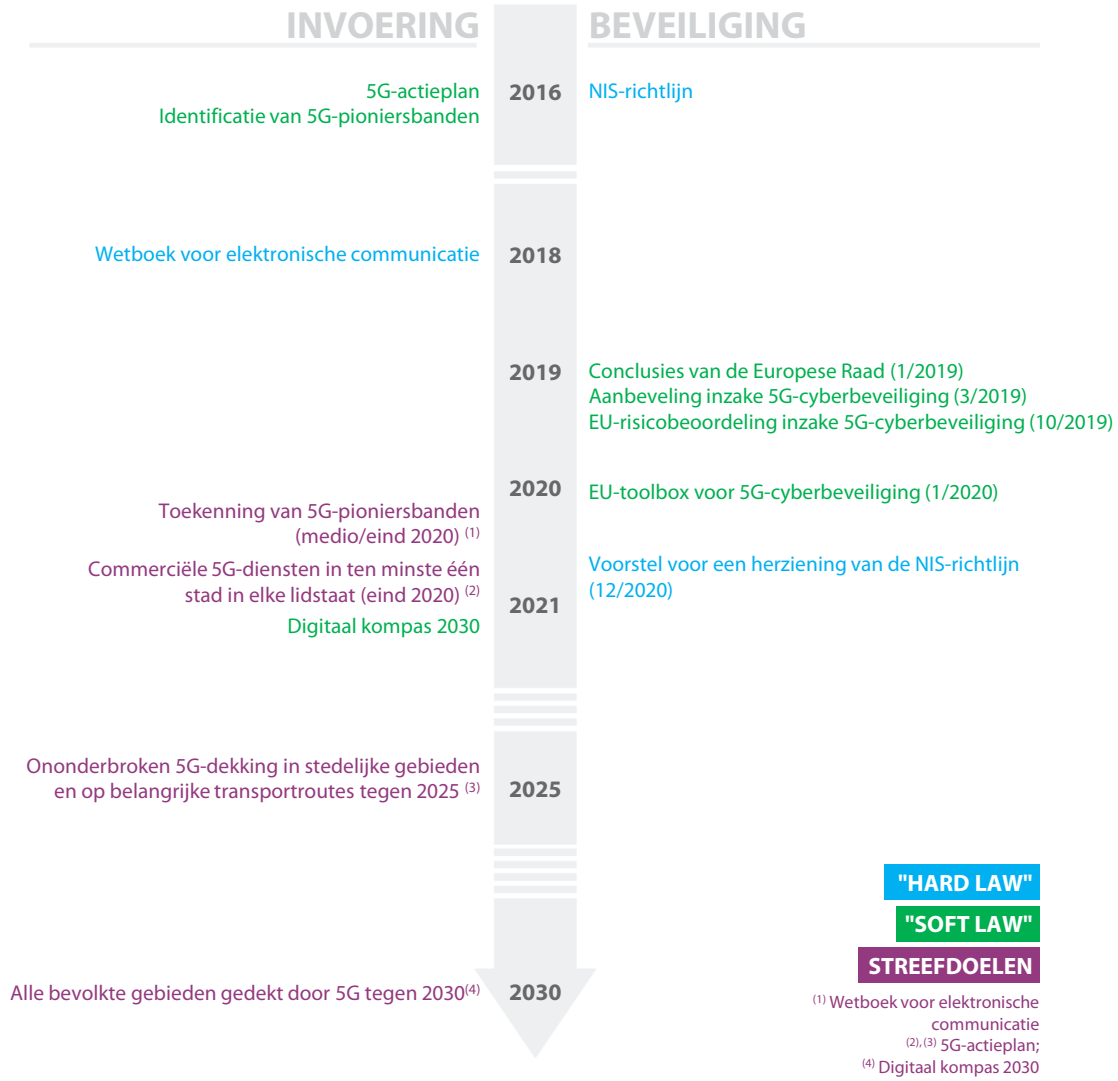
08 Het beleidskader met betrekking tot 5G en de veiligheid van 5G bestaat zowel uit "hard law" die juridisch bindend en afdwingbaar is (bijvoorbeeld verordeningen) als uit niet-bindende "soft law" (bijvoorbeeld mededelingen van de Commissie). ***Bijlage III*** bevat het juridisch en beleidskader. ***Figuur 2*** geeft een overzicht van de belangrijkste beleidsdocumenten, samen met de kerndoelen.

---

[10] https://ec.europa.eu/commission/presscorner/detail/en/IP_15_5715

[11] Resolutie van het Europees Parlement van 12 maart 2019; nationale inlichtingenwet van de Volksrepubliek China, artikel 14. Zie ook de Engelse vertaling op https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

Figuur 2 — Belangrijkste beleidsdocumenten en kerndoelen met betrekking tot de invoering en veiligheid van 5G



Bron: ERK.

Rollen en verantwoordelijkheden

09 Hoewel mobiele-netwerkexploitanten verantwoordelijk zijn voor de veilige uitrol van 5G met apparatuur die afkomstig is van technologieleveranciers, en de lidstaten verantwoordelijk zijn voor de nationale veiligheid, is de beveiliging van 5G-netwerken een kwestie van strategisch belang voor de gehele eengemaakte markt en de technologische soevereiniteit van de EU[12]. Bijgevolg ondersteunen en coördineren de

[12] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_12

Commissie en EU-agentschappen, wat de technische en veiligheidsaspecten van 5G-netwerken betreft, de acties van de lidstaten.

10 In ***tabel 1*** worden de belangrijkste rollen en verantwoordelijkheden op het gebied van 5G-netwerken verder toegelicht.

Tabel 1 — Rollen en verantwoordelijkheden

	Commissie en EU-agentschappen	Autoriteiten van de lidstaten	Mobiele-netwerkexploitanten & 5G-leveranciers
Indeling en toewijzing van 5G-pioniersbanden		✓	
Vaststelling van het 5G-beleid van de EU	✓	✓	
Invoering van 5G-netwerken			✓
Investeringen en financiering	✓	✓	✓
Nationale veiligheid		✓	
Veiligheid van 5G-netwerken		✓	✓
Ondersteuning en coördinatie van acties van de lidstaten	✓		

Bron: ERK.

Kosten van de invoering van 5G en de daarmee samenhangende financiële steun van de EU

De totale kosten van de invoering van 5G in alle lidstaten zouden kunnen oplopen tot 400 miljard EUR

11 In 2021 zijn de totale kosten van de invoering van 5G in alle EU-lidstaten tot 2025 geraamd op 281 miljard EUR tot 391 miljard EUR, gelijkmatig verdeeld over de aanleg van nieuwe 5G-infrastructuur en de modernisering van vaste infrastructuur tot gigabitsnelheden[13]. Het grootste deel van deze investeringen moet door mobiele-netwerkexploitanten worden gefinancierd.

[13] Raming door de Commissie, gebaseerd op gegevens van de EIB, Analysys, GSMA en mededelingen van ondernemingen, alsmede op het document van ETNO – European Telecommunications, Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All, maart 2021.

In de periode 2014-2020 heeft de EU de ontwikkeling van 5G met meer dan 4 miljard EUR gesteund

12 In de periode 2014-2020 heeft de EU de ontwikkeling van 5G met meer dan 4 miljard EUR gesteund, zowel rechtstreeks uit de EU-begroting als via financiering van de Europese Investeringsbank (EIB). Uit de EU-begroting werden projecten gefinancierd die uitsluitend betrekking hadden op onderzoeks, terwijl de EIB steun verleende voor zowel onderzoek als invoering.

13 De EIB is de grootste verstrekker van EU-financiering voor 5G-gerelateerde projecten geweest. Tot augustus 2021 heeft de EIB leningen verstrekt voor een totaalbedrag van 2,5 miljard EUR voor negen 5G-projecten in vijf lidstaten[14]. Voorts werd voor de periode 2014-2020 ongeveer 1,9 miljard EUR uit de EU-begroting beschikbaar gesteld. ***Tabel 2*** geeft een overzicht van de belangrijkste bronnen van financiële steun van de EU voor 5G.

Tabel 2 — EU-financiering voor 5G (2014-2020)

EU-financiering	Bedrag
EIB	2 485 miljard EUR[1]
Europees Fonds voor strategische investeringen (EFSI)	1 miljard EUR[2]
Horizon 2020	755 miljoen EUR[3]
EFRO	Minstens 147 miljoen EUR[4]

1) Lijst van EIB-projecten.
2) Lijst van EFSI-projecten.
3) Horizon 2020-dashboard.
4) Dataset van projecten die door het EFRO zijn gecofinancierd tijdens het meerjarig financieel kader 2014-2020.

Bron: ERK.

14 Het EFSI (dat door de EIB wordt beheerd) heeft steun verleend aan twee projecten die gericht zijn op de uitrol van een dichter netwerk van cellen en ondersteuning van de normalisatie. De totale investeringskosten van deze projecten bedroegen 3,9 miljard EUR, inclusief 1 miljard EUR financiering uit het EFSI (zie ***bijlage IV***).

[14] Lijst van EIB-projecten.

15 Sinds 2014 heeft de Commissie ook meer dan 100 5G-projecten rechtstreeks gecofinancierd via Horizon 2020-financiering en in mindere mate het EFRO. ***Bijlage V*** bevat voorbeelden van dergelijke projecten.

De herstel- en veerkrachtfaciliteit zal de komende jaren extra EU-financiering verstrekken voor de invoering van 5G

16 De herstel- en veerkrachtfaciliteit (Recovery and Resilience Facility, RRF) zal de komende jaren een aanvullende financieringsbron bieden voor de invoering van 5G. Per september 2021 waren 16 lidstaten van plan de invoering van 5G via de RRF te financieren en hadden 10 lidstaten besloten dit niet te doen. Er was nog geen informatie beschikbaar van de laatste lidstaat.

Reikwijdte en aanpak van de controle

17 Bij deze controle hebben we beoordeeld of de Commissie de lidstaten doeltreffend ondersteunt bij:

- het verwezenlijken van de EU-doelstellingen voor 2025 en 2030 voor de invoering en uitrol van hun 5G-netwerken, en
- het op een gecoördineerde manier aanpakken van kwesties inzake de beveiliging van 5G.

Op deze beide gebieden hebben wij ook de maatregelen en activiteiten van de lidstaten onderzocht.

18 Met "beveiliging van 5G" wordt gedoeld op cyberbeveiliging en veiligheid van hardware/software. Wij hebben zowel de veiligheid als de implementatie van 5G-netwerken onderzocht, waarvoor 2020 een cruciaal jaar was (zie ***figuur 2***). Met ons verslag willen wij inzichten en aanbevelingen verschaffen over de tijdige invoering van veilige 5G-netwerken in de EU.

19 Onze controle heeft betrekking op de periode tussen 2016 en mei 2021. Voor zover mogelijk hebben wij verdere actuele informatie opgenomen. In het kader van onze controlewerkzaamheden hebben wij:

- EU-wetgeving, initiatieven van de Commissie en andere relevante documentatie geanalyseerd;
- gesprekken gevoerd met vertegenwoordigers van de Commissie, de EIB, het Orgaan van Europese regulerende instanties voor elektronische communicatie (Berec), het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), telecomverenigingen, mobiele-netwerkexploitanten, leveranciers van 5G en internationale organisaties, alsmede met deskundigen op dit gebied om inzichten te vergaren, en met autoriteiten in Finland, Duitsland, Polen en Spanje. De selectie van de lidstaten was gebaseerd op criteria zoals het bedrag aan EU-middelen dat voor 5G-projecten is uitgetrokken, de stand van de invoering en de inachtneming van een geografisch evenwicht;
- een enquête gehouden onder alle 27 nationale regelgevende telecomautoriteiten in de EU om een breder perspectief te krijgen op de 5G-uitdagingen in de lidstaten, en

- tien door de EU gecofinancierde projecten (EFSI, EFRO en Horizon 2020) met betrekking tot 5G geanalyseerd, die ter illustratie zijn geselecteerd.

20 Wij putten ook uit onze recente analyse van de respons van de EU op de Chinese staatsgestuurde investeringsstrategie[15] en uit andere verslagen over bijvoorbeeld breedband[16], het initiatief voor de digitalisering van het Europese bedrijfsleven[17] en het EU-beleid inzake cyberveiligheid[18].

[15] Analyse nr. 03/2020 “De respons van de EU op de Chinese staatsgestuurde investeringsstrategie".

[16] Speciaal verslag nr. 12/2018 “Breedband in de EU-lidstaten: hoewel er vooruitgang is geboekt, zullen niet alle Europa 2020-streefdoelen worden gehaald".

[17] Speciaal verslag 19/2020 “Digitalisering van het Europese bedrijfsleven: een ambitieus initiatief waarvan het succes afhangt van de voortdurende inzet van de EU, regeringen en ondernemingen".

[18] Analyse nr. 02/2019 “Uitdagingen voor een doeltreffend EU-beleid inzake cyberbeveiliging” (briefingdocument).

Opmerkingen

Vertragingen bij de invoering van 5G-netwerken brengen de verwezenlijking van de doelstellingen van de EU voor 2025 en 2030 in gevaar

21 Wat de tijdige invoering van 5G-netwerken betreft, hebben wij onderzocht of:

- de lidstaten op schema liggen met de invoering van 5G;
- de Commissie de lidstaten passende steun heeft geboden, en
- de lidstaten belangrijke belemmeringen voor de snelle uitrol van 5G-netwerken hebben weggenomen.

De lidstaten lopen achter bij de implementatie van 5G

De Commissie stelde in haar 5G-actieplan van 2016 termijnen vast voor de invoering van 5G-netwerken

22 In haar 5G-actieplan van 2016 heeft de Commissie termijnen voorgesteld voor de invoering van 5G-netwerken in de EU: De lidstaten moesten tegen eind 2018 eerste 5G-netwerken hebben ingevoerd en tegen eind 2020 volledig commerciële 5G-diensten in ten minste één grote stad; tegen 2025 moeten zij zorgen voor ononderbroken 5G-dekking in stedelijke gebieden en op belangrijke transportroutes.

23 In maart 2021 voegde de Commissie een nieuwe termijn toe voor de 5G-dekking van alle bevolkte gebieden tegen 2030[19].

23 lidstaten hadden vóór eind 2020 commerciële 5G-diensten ingevoerd

24 Eind 2020 hadden 23 lidstaten de doelstelling behaald dat ten minste één grote stad toegang had tot 5G-diensten. Alleen Cyprus, Litouwen, Malta en Portugal haalden deze doelstelling niet. Eind oktober 2021 beschikten alleen Litouwen en Portugal nog in geen enkele stad over 5G-diensten.

---

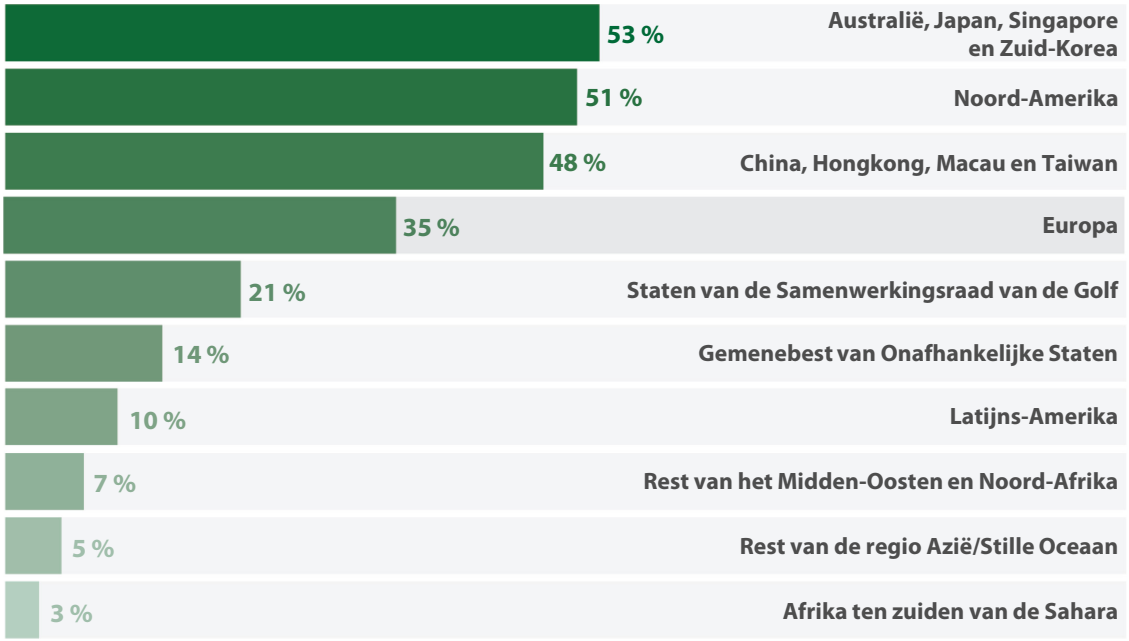
[19] Europese Commissie, Digitaal kompas 2030: de Europese aanpak voor het digitale decennium, COM(2021) 118 final.

Het risico bestaat dat de meeste lidstaten de termijnen van 2025 en 2030 niet zullen halen

25 Volgens een recente studie van de Commissie zullen waarschijnlijk slechts elf lidstaten tegen 2025 een ononderbroken 5G-dekking in al hun stedelijke gebieden en op belangrijke transportroutes over land bereiken[20]. Voor de resterende 16 lidstaten acht de Commissie de kans dat deze doelstelling wordt gehaald middelgroot (Oostenrijk, Tsjechië, Estland, Duitsland, Ierland, Polen, Litouwen en Slovenië) of klein (België, Bulgarije, Kroatië, Cyprus en Griekenland).

26 In 2021 merkte de brancheorganisatie Global System for Mobile Communications Association (GSMA) op dat de invoering van 5G in de EU in een ander tempo verloopt dan in andere delen van de wereld. Zo wordt geschat dat in 2025 51 % van alle mobiele verbindingen in Noord-Amerika op 5G zal zijn gebaseerd, terwijl dit in Europa (waartoe ook niet-EU-landen behoren) naar verwachting slechts 35 % zal zijn (zie ***figuur 3***).

Figuur 3 — 5G-verbindingen als percentage van totale mobiele verbindingen tegen 2025



Bron: GSMA — The Mobile Economy 2021.

[20] Study on National Broadband Plans in the EU-27.

27 In het huidige tempo van invoering is het risico groot dat de termijn van 2025 — en dus ook de termijn van 2030 voor de dekking van alle bevolkte gebieden — door een meerderheid van de lidstaten niet zal worden gehaald. Tegen deze achtergrond hebben wij onderzocht of de Commissie de lidstaten doeltreffend heeft ondersteund om de 5G-doelstellingen van de EU voor 2025 en 2030 voor de invoering en uitrol van hun 5G-netwerken te bereiken.

Enkele tekortkomingen inzake de steun van de Commissie aan de lidstaten

De Commissie heeft de verwachte kwaliteit van de dienstverlening van 5G-netwerken niet omschreven

28 De Commissie heeft tot dusver de verwachte kwaliteit van de dienstverlening van 5G-netwerken niet omschreven, bijvoorbeeld wat betreft minimumsnelheid en maximale latentietijd. In het actieplan van 2016 wordt de lidstaten bovendien gevraagd om tegen eind 2020 “volledig commerciële” 5G-diensten in Europa in te voeren, zonder dat deze kwaliteitsgerelateerde concepten worden omschreven.

29 Door het gebrek aan duidelijkheid over de verwachte kwaliteit van de dienstverlening ontstaat het risico dat deze termen door de lidstaten verschillend worden geïnterpreteerd. Wij hebben voorbeelden gezien van uiteenlopende benaderingen van de lidstaten bij de invoering van 5G (zie ***kader 2***).

Kader 2

Voorbeelden van uiteenlopende benaderingen bij de invoering van 5G

Snelheid en latentietijd zijn twee belangrijke aspecten van de prestaties van diensten die gebruikmaken van 5G. Voor operaties op afstand of industriële automatisering met behulp van 5G zijn bijvoorbeeld zeer hoge snelheden en lage latentietijden vereist. Tot dusver hebben echter slechts twee lidstaten (Duitsland en Griekenland) eisen inzake minimumsnelheid en maximale latentietijd vastgesteld[21].

[21] 5G Observatory Quarterly Report 12, Up to June 2021.

De eis dat ten minste één grote stad tegen eind 2020 toegang heeft tot 5G-diensten is door de lidstaten verschillend geïnterpreteerd. Dit leidt tot een situatie waarin een stad die wordt aangemerkt als stad met toegang tot 5G-diensten, kan variëren van een stad waarvan slechts enkele straten zijn gedekt, zoals Luxemburg, tot een stad waarvan bijna haar hele grondgebied is gedekt, zoals Helsinki. ***Bijlage VI*** geeft voor een aantal steden voorbeelden van de dekking.

30 Als deze situatie voortduurt, zou dit kunnen leiden tot ongelijkheden in de toegang tot en de kwaliteit van 5G-diensten in de EU ("digitale kloof"): mensen in bepaalde delen van de EU zouden beschikken over een betere toegang tot en kwaliteit van 5G-diensten dan mensen in andere delen. Deze digitale kloof kan ook gevolgen hebben voor het potentieel van economische ontwikkeling, aangezien 5G alleen een revolutie teweeg kan brengen in sectoren zoals de gezondheidszorg, het onderwijs en de beroepsbevolking indien deze gepaard gaat met voldoende 5G-prestaties.

31 Duidelijkheid over de verwachte prestaties van 5G-netwerken is ook nodig in het licht van het initiatief van de Commissie om meer transparantie op te leggen met betrekking tot de kwaliteit van de dienstverlening van de mobiele-netwerkexploitanten bij roaming, waarvoor de Commissie onlangs een wetgevingsvoorstel heeft gedaan[22].

De driemaandelijkse verslagen van de Commissie over de uitrol van 5G zijn niet altijd betrouwbaar

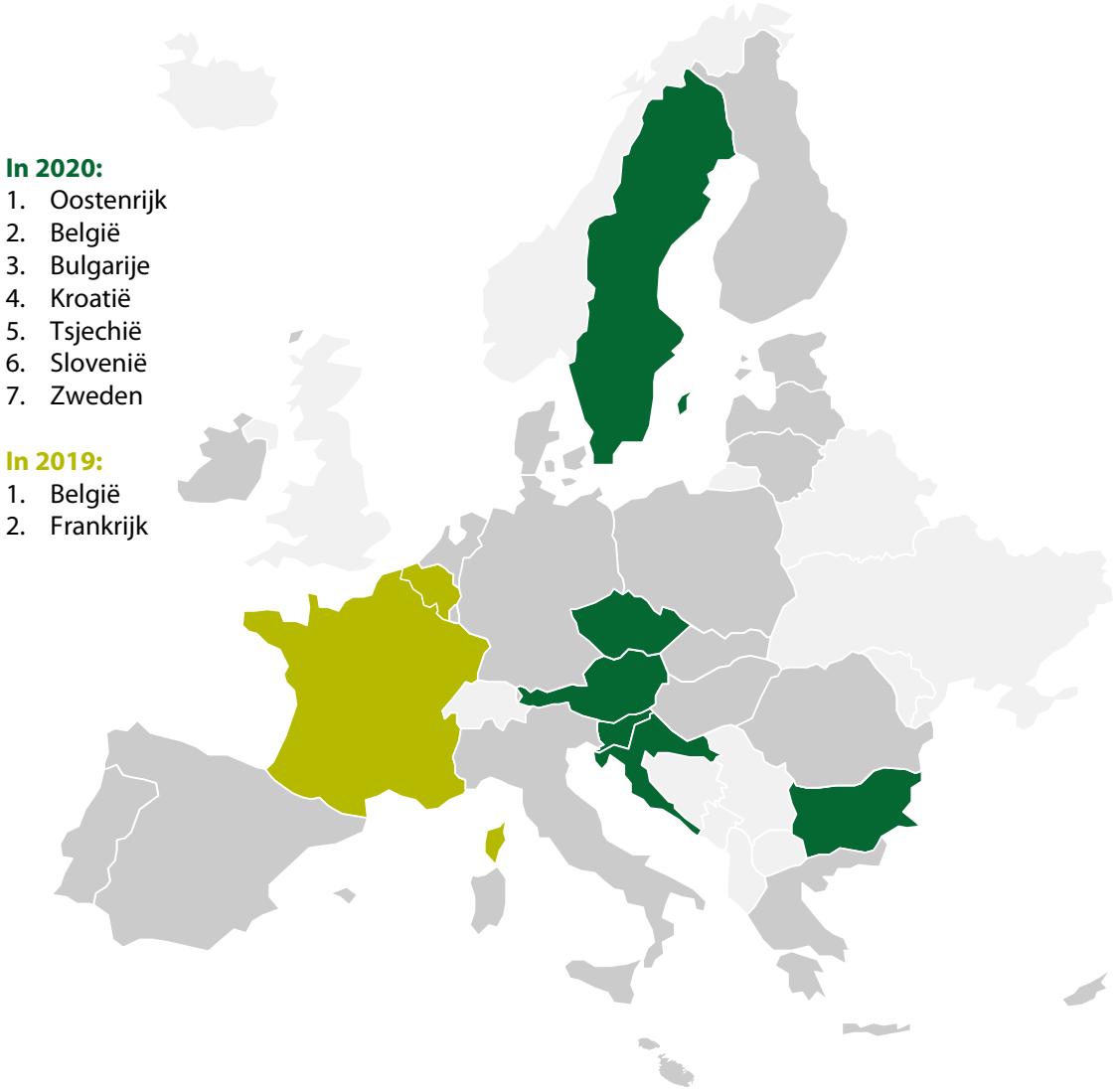
32 De Commissie monitort het niveau van invoering van 5G in de lidstaten via de 5G-waarnemingspost. Deze waarnemingspost verstrekt elk kwartaal informatie over de invoering van 5G en over de 5G-strategieën van de lidstaten. Wij hebben echter vastgesteld dat voor twee van de vier door ons onderzochte landen de in deze verslagen vervatte informatie niet altijd betrouwbaar was. In kwartaalverslag 10, waarin de informatie tot eind december 2020 wordt gepresenteerd, wordt bijvoorbeeld een veel kleiner aantal gemeenten met 5G in Finland vermeld dan het werkelijke aantal (veertig in plaats van zeventig) en wordt geen informatie verstrekt over het feit dat de veiling van 5G-frequenties in Polen was uitgesteld (zie paragraaf ***42***).

[22] Europese Commissie, Voorstel voor een verordening betreffende roaming op openbare mobielecommunicatienetwerken binnen de Unie (herschikking), COM(2021) 85 final van 24 februari 2021.

De Commissie heeft pas onlangs gebruikgemaakt van het proces van het Europees Semester om de vorderingen van de lidstaten bij de invoering van 5G-netwerken te monitoren

33 Wij hebben vastgesteld dat de Commissie de afgelopen twee jaar meer gebruik heeft gemaakt van het proces van het Europees Semester om de vooruitgang van de lidstaten bij de invoering van 5G-netwerken aan te moedigen. Het aantal lidstaten waartoe landspecifieke aanbevelingen zijn gericht die direct relevant zijn voor 5G is toegenomen van twee in 2019 tot zeven in 2020 (zie ***figuur 4***).

Figuur 4 — Landspecifieke aanbevelingen inzake 5G



Bron: ECA, op basis van landspecifieke aanbevelingen.

De lidstaten moeten nog steeds belangrijke belemmeringen voor de snelle uitrol van 5G-netwerken wegnemen

34 Om de EU-doelstellingen voor de invoering van 5G in 2025 en 2030 te behalen, moeten de lidstaten zorgen dat drie belangrijke bouwstenen aanwezig zijn: een strategische, door ervoor te zorgen dat hun nationale 5G-strategieën of nationale breedbandplannen deze doelstellingen weerspiegelen[23], een wetgevende, met de omzetting van het Europees wetboek voor elektronische communicatie (European Electronic Communications Code, EECC) van 2018[24] en een bedrijfsgerichte, met de toewijzing van de frequentie[25]. ***Tabel 3*** geeft een overzicht van de vorderingen van de lidstaten met betrekking tot deze drie elementen.

[23] Study on National Broadband Plans in the EU-27, Europese Commissie.

[24] Richtlijn (EU) 2018/1972 tot vaststelling van het Europees wetboek voor elektronische communicatie.

[25] Mededeling van de Europese Commissie, Uitrol van beveiligde 5G in de EU — uitvoering van de EU-toolbox, COM(2020) 50 final.

Tabel 3 — Stand van zaken van de bouwstenen met betrekking tot de doelstellingen voor 2025

Lidstaat	NBP in overeenstemming met de doelstellingen voor 2025	Omzetting van het EECC	5G-pioniersbanden (augustus 2021)			Waarschijnlijkheid dat de doelstelling wordt bereikt
			700 MHz	3,6 GHz	26 GHz	
België				Voorlopig gebruik		laag
Bulgarije		✓		✓		laag
Tsjechië	✓	✓	✓	✓		middelmatig
Denemarken		✓	✓	✓	✓	hoog
Duitsland	✓	✓	✓	✓	✓	middelmatig
Estland						middelmatig
Ierland				✓		middelmatig
Griekenland	✓	✓	✓	✓	✓	laag
Spanje	✓		✓	✓		hoog
Frankrijk	✓	✓	✓	✓		hoog
Kroatië			✓	✓	✓	laag
Italië			✓	✓	✓	hoog
Cyprus	✓		✓	✓		laag
Litouwen	✓					middelmatig
Letland				✓		hoog
Luxemburg			✓	✓		hoog
Hongarije	✓	✓	✓	✓		hoog
Malta		✓				middelmatig
Nederland	✓		✓			middelmatig
Oostenrijk	✓	✓	✓	✓		middelmatig
Polen	✓					middelmatig
Portugal				Voorlopig gebruik		middelhoog
Roemenië						hoog
Slovenië	✓		✓	✓	✓	middelmatig
Slowakije			✓			hoog
Finland	✓	✓	✓	✓	✓	hoog
Zweden	✓		✓	✓		hoog

Bron: Study on National Broadband Plans in the EU-27 van de Commissie, 5G-waarnemingspost en Beleidsgroep radiospectrum.

Een gering aantal lidstaten heeft de doelstellingen van invoering voor 2025 en 2030 in hun nationale 5G-strategieën opgenomen

35 De lidstaten zetten hun 5G-beleid uiteen door middel van specifieke nationale 5G-strategieën of door hun bestaande nationale breedbandplannen te actualiseren. In de studie van de Commissie van 2021 over de nationale breedbandplannen[26] wordt opgemerkt dat slechts 14 lidstaten de EU-doelstelling van ononderbroken 5G-dekking in alle stedelijke gebieden en op belangrijke transportroutes over land tegen 2025 hebben opgenomen in hun nationale 5G-strategieën of bijgewerkte nationale breedbandplannen (zie ***tabel 3***). Een dergelijke opname is van cruciaal belang om de succesvolle uitvoering van het beleid te ondersteunen.

De meeste lidstaten hadden de EECC-richtlijn eind 2020 nog niet omgezet

36 De EECC — een richtlijn waarin de taken van de nationale regelgevende en andere bevoegde autoriteiten zijn vastgelegd en termijnen voor de toewijzing van 5G-pioniersbanden zijn vastgesteld — had uiterlijk op 21 december 2020 door de lidstaten in nationaal recht moeten zijn omgezet. Eind februari 2021 hadden slechts drie lidstaten (Finland, Griekenland en Hongarije) verklaard dat zij alle nodige maatregelen voor de omzetting van de richtlijn hadden genomen. Bijgevolg heeft de Commissie inbreukprocedures ingeleid tegen de resterende 24 lidstaten[27].

37 Eind november 2021 liepen er nog 23 inbreukprocedures. Voor 6 lidstaten (Oostenrijk, Bulgarije, Tsjechië, Frankrijk, Duitsland en Malta) verwacht de Commissie de inbreukprocedure binnenkort af te sluiten maar tegen de overige 17 lidstaten moet de Commissie wellicht een zaak aanspannen bij het Hof van Justitie[28] (zie ***tabel 3***).

De toewijzing van 5G-pioniersbanden loopt achter

38 In 2016 hebben de Commissie en de lidstaten drie pioniersbanden aangewezen die voor 5G-diensten moeten worden gebruikt:

- het 700 MHz-bandspectrum, dat het voor draadloze signalen gemakkelijker maakt om door gebouwen heen te dringen en exploitanten in staat stelt bredere dekking te bieden (honderden vierkante kilometers). De snelheid en latentietijden van het

[26] Study on National Broadband Plans in the EU-27.

[27] Persbericht IP/21/206 van de Commissie van 4 februari 2021.

[28] Persbericht IP/21/4612 van de Commissie van 23 september 2021.

5G-netwerk liggen echter niet heel veel hoger dan bij 4G (van 150 tot 250 megabit per seconde);

- het middenbandspectrum op 3,6 GHz, waarmee aanzienlijke hoeveelheden gegevens over aanzienlijke afstanden (een straal van meerdere kilometers) kunnen worden overgebracht (tot 900 megabit per seconde), en

- het hogebandspectrum op 26 GHz, dat hoge snelheden tussen 1 en 3 gigabit per seconde levert over korte afstanden (d.w.z. minder dan 2 km), maar gevoeliger is voor interferentie.

39 De lidstaten hadden het lage- en het middenbandspectrum tegen respectievelijk 30 juni 2020[29] en 31 december 2020[30] voor gebruik beschikbaar moeten stellen. Eind 2020 hadden de lidstaten echter minder dan 40 % van de in totaal beschikbare pioniersbanden toegewezen (zie ***tabel 4***):

- de 700 MHz-band werd toegewezen in 13 lidstaten;

- de 3,6 GHz-band werd toegewezen in 17 lidstaten (waaronder twee lidstaten die voorlopig gebruik hadden toegestaan), en

- de 26 GHz-band werd toegewezen in vier lidstaten.

Eind 2021 was het toewijzingspercentage gestegen tot 53 %[31].

[29] Besluit (EU) 2017/899 betreffende het gebruik van de 470-790 MHz-frequentieband in de Unie.

[30] Richtlijn (EU) 2018/1972 tot vaststelling van het Europees wetboek voor elektronische communicatie.

[31] 5G-waarnemingspost en Beleidsgroep radiospectrum.

Tabel 4 — Stand van zaken met betrekking tot de toewijzing van 5G-pioniersbanden, december 2020

Lidstaat	700 MHZ	3,6 GHZ	26 GHZ
België		Voorlopig gebruik	
Bulgarije			
Tsjechië	✓	✓	
Denemarken	✓	✓	✓
Duitsland	✓	✓	✓
Estland		—	
Ierland		✓	
Griekenland	✓	✓	✓
Spanje		✓	
Frankrijk	✓	✓	
Kroatië			
Italië		✓	✓
Cyprus	✓	✓	
Letland		✓	
Litouwen			
Luxemburg	✓	✓	
Hongarije	✓	✓	
Malta			
Nederland	✓		
Oostenrijk	✓	✓	
Polen			
Portugal		Voorlopig gebruik	
Roemenië			
Slovenië			
Slowakije	✓	✓	
Finland	✓	✓	✓
Zweden	✓	✓	

Bron: 5G-waarnemingspost en Beleidsgroep radiospectrum.

Vertragingen bij de toewijzing van de pioniersbanden zijn aan allerlei oorzaken toe te schrijven

40 Wij hebben vastgesteld dat de vertragingen bij de toewijzing van de 26 GHz-band vooral te wijten zijn aan een geringe vraag van mobiele-netwerkexploitanten. In Spanje bijvoorbeeld is in totaal 1,5 GHz van de 26 GHz-band beschikbaar voor 5G-gebruik. Deze is echter nog niet aan exploitanten toegewezen omdat er geen vraag naar is, zo blijkt uit een openbare raadpleging die in juli 2019 is afgerond. Een nieuwe openbare raadpleging is gepland voor eind 2021, met het oog op het veilen van de band in het tweede kwartaal van 2022. Ook mobiele-netwerkexploitanten in Finland merkten op

dat er nog niet veel belangstelling is voor de 26 GHz-band en dat er evenmin zakelijke redenen voor de gebruikmaking ervan bestaan.

41 Grensoverschrijdende coördinatieproblemen met niet-EU-landen langs de oostgrenzen (Belarus, Rusland en Oekraïne) hebben ook bijgedragen tot vertragingen bij de toewijzing van 5G-frequenties. Deze niet-EU-landen gebruiken krachtens de huidige internationale overeenkomsten de 700 MHz-band voor televisie-uitzendingen en de 3,6 GHz-band voor militaire satellietdiensten. Deze kwestie betreft vooral de Baltische landen (Estland, Letland en Litouwen) en Polen. Volgens de Commissie is er enige vooruitgang geboekt met Oekraïne en Belarus, die de 700 MHz-band tegen eind 2022 zouden moeten vrijgeven. Bij de bilaterale besprekingen met Rusland is nog geen vooruitgang geboekt. Met het oog op deze situatie hebben Estland en Polen verzocht om afwijking van de termijnen voor de toewijzing van de 700 MHz-band tot medio 2022.

42 Bovendien werden in Polen en Spanje 5G-frequentieveilingen uitgesteld tijdens de COVID-19-pandemie (zie ***kader 3***).

Kader 3

Voorbeelden van door de COVID-19-pandemie veroorzaakte vertragingen bij de toewijzing van 5G-frequenties

- In maart 2020 heeft Polen een veiling aangekondigd voor de 3,6 GHz-band, die uiterlijk op 30 juni 2020 moest worden toegewezen. Na de uitbraak van de pandemie hebben de Poolse autoriteiten besloten alle administratieve procedures voor de duur van de pandemie op te schorten. In september 2021 was het proces voor het veilen van deze band nog steeds niet afgerond.

- In Spanje was de veiling voor de 700 MHz-band oorspronkelijk gepland voor maart 2020. Volgens de Spaanse autoriteiten heeft de COVID-19-pandemie de vrijgave van deze voor digitale televisie gebruikte band echter vertraagd. Vervolgens werd de veiling uitgesteld tot mei 2020 en daarna tot het eerste kwartaal van 2021. Na een wijziging van de Spaanse wetgeving in april 2021 om de duur van vergunningen in overeenstemming te brengen met het EECC, werd de veiling verschoven naar de zomer van 2021 en werd de 700 MHz-band uiteindelijk in juli 2021 toegewezen.

43 Een andere oorzaak van de vertraging bij de toewijzing van de 5G-pioniersbanden is de uiteenlopende aanpak van de lidstaten inzake de beveiliging van 5G en de vertragingen bij de vaststelling van hun wetten inzake beveiliging van 5G, hetgeen tot onzekerheid bij het bedrijfsleven leidt (zie de paragrafen ***74*** en ***75***):

- In Spanje is in de regels voor pioniersbandveilingen een algemene clausule opgenomen volgens welke de houders van overheidsconcessies verplicht zijn te voldoen aan alle verplichtingen op het gebied van veiligheid van 5G-netwerken die op enig moment in de toekomst door de Europese of Spaanse regelgeving worden vastgesteld. De door ons bevraagde Spaanse mobiele-netwerkexploitant was van mening dat hij door deze clausule beslissingen over strategieën en aankopen moest nemen in onzekere omstandigheden. Hij wees er ook op dat de nationale autoriteiten niet bereid waren bepaalde belangrijke voorwaarden te verduidelijken, zoals de mogelijkheid van compensatie indien de toekomstige wetgeving, die volgens plan tegen eind 2022 zal worden aangenomen, hen zou verplichten hun apparatuur te vervangen.

- In Polen was een van de redenen voor het uitstellen van de toewijzing van 5G-frequenties dat moest worden gewacht op een wet waarin de veiligheidseisen voor 5G-netwerken worden verduidelijkt.

Verdere inspanningen zijn nodig voor de aanpak van beveiligingskwesties bij de invoering van 5G

44 Wat de veiligheidsaspecten van 5G betreft, hebben wij onderzocht of:

- de Commissie de nodige stappen heeft ondernomen om een degelijke opzet van het veiligheidskader te bevorderen, en de lidstaten passende steun heeft verleend;

- de lidstaten op gecoördineerde wijze veilige 5G-netwerken invoeren, waarbij zij de risicobeperkende maatregelen treffen die zijn opgenomen in de EU-toolbox voor 5G-cyberbeveiliging (toolbox) en hun wetgeving in dit verband bijwerken.

De Commissie heeft snel gereageerd toen de beveiliging van 5G een belangrijk punt van zorg werd op EU-niveau

45 Het 5G-actieplan van 2016 bevat geen veiligheidsoverwegingen. De beveiliging van 5G-netwerken en een te grote afhankelijkheid van leveranciers uit derde landen, en met name China, werden in maart 2019 als kritieke kwesties aangemerkt. Het

Europees Parlement heeft in zijn resolutie van 12 maart 2019[32] zijn bezorgdheid geuit over 5G-leveranciers van buiten de EU die een veiligheidsrisico voor de EU kunnen vormen als gevolg van de wetgeving van hun landen van herkomst. Dezelfde dag heeft de Commissie in haar strategische visie op de betrekkingen tussen de EU en China benadrukt dat er als bescherming tegen potentieel ernstige gevolgen voor de veiligheid van kritieke digitale infrastructuur een gemeenschappelijke EU-benadering moet komen voor de beveiliging van 5G-netwerken[33]. De Europese Raad heeft in zijn conclusies van 21 en 22 maart 2019 de Commissie verzocht een aanbeveling te doen over een gezamenlijke aanpak van de veiligheid van 5G-netwerken[34].

46 Enkele dagen later bracht de Commissie een dergelijke aanbeveling uit met een reeks maatregelen op zowel nationaal (bijvoorbeeld risicobeoordeling inzake 5G) als EU-niveau (bijvoorbeeld gecoördineerde risicobeoordeling), die gericht zijn op het waarborgen van een hoog niveau van cyberbeveiliging van 5G-netwerken in de hele EU[35].

47 Bijna alle lidstaten hadden hun nationale risicobeoordelingen voltooid tegen de uiterste termijn van juli 2019[36]. In oktober 2019 heeft de NIS-samenwerkingsgroep een verslag over de gecoördineerde EU-risicobeoordeling van de cyberbeveiliging van 5G-netwerken uitgebracht, en in januari 2020 de EU-toolbox voor 5G-cyberbeveiliging[37] (zie ***bijlage VII***). Deze toolbox werd binnen korte tijd bekrachtigd door de Commissie en de Europese Raad[38].

---

[32] Resolutie van het Europees Parlement van 12 maart 2019 (2019/2575(RSP)).

[33] JOIN(2019) 5 final van 12 maart 2019.EU-China — Een strategische visie.

[34] Conclusies van de Europese Raad van 21 en 22 maart 2019.

[35] Aanbeveling (EU) 2019/534 van de Commissie van 26 maart 2019 Cyberbeveiliging van 5G-netwerken.

[36] Persbericht van 19 juli 2019.

[37] Cybersecurity of 5G networks — EU Toolbox of risk mitigating measures. NIS-samenwerkingsgroep, januari 2020.

[38] Mededeling van de Europese Commissie, Uitrol van beveiligde 5G in de EU — uitvoering van de EU-toolbox, COM(2020) 50 final en conclusies van de Europese Raad van 1 en 2 oktober 2020 (EUCO 13/10).

In de EU-toolbox voor 5G-cyberbeveiliging van 2020 zijn voor het eerst maatregelen vastgesteld om veiligheidsbedreigingen op EU-niveau aan te pakken, maar het normatieve gehalte was te laag

Door veiligheid van 5G-netwerken als een bevoegdheid inzake nationale veiligheid te beschouwen, worden de mogelijkheden van de Commissie om op te treden beperkt

48 In de EU-Verdragen[39] wordt het toepassingsgebied bepaald van acties om uitdagingen aan te pakken zoals die welke verband houden met de invoering van veilige 5G-netwerken op EU-niveau. Dit toepassingsgebied is ruim en biedt de Commissie en de lidstaten ruimte voor interpretatie (zie ***kader 4***).

[39] Verdrag betreffende de werking van de Europese Unie.

Kader 4

EU-bevoegdheden in verband met 5G-netwerken: een gedeelde bevoegdheid of een zaak van nationale veiligheid?

In beginsel vallen 5G-netwerken onder de bevoegdheid van de EU voor de eengemaakte markt (een gedeelde bevoegdheid), en dit zowel wat betreft de dienst (de levering van een dienst door mobiele-netwerkexploitanten) als wat betreft de goederen (de 5G-apparatuur zelf, die door mobiele-netwerkexploitanten wordt aangeschaft om hun 5G-netwerken aan te leggen). In het kader van de gedeelde bevoegdheid kan de EU (de Commissie en andere EU-instellingen) juridisch bindende maatregelen (wetgeving) vaststellen om de totstandbrenging van haar eengemaakte markt te waarborgen en de goede werking ervan te bevorderen. De veiligheid van 5G-netwerken kan ook in ruimere zin worden gezien als een aangelegenheid die verband houdt met de ruimte van vrijheid, veiligheid en recht van de EU. In die zin kan veiligheid worden opgevat als een algemene term die betrekking heeft op de preventie en de bestrijding van criminaliteit, waardoor het een andere gedeelde bevoegdheid is waarvoor de EU juridisch bindende maatregelen kan vaststellen.

Een engere interpretatie van het begrip veiligheid zou er daarentegen in bestaan het te beperken tot bedreigingen voor de nationale veiligheid van de lidstaten. Aangezien dit een exclusieve nationale bevoegdheid is, kan de EU alleen ondersteunende maatregelen nemen teneinde de nationale inspanningen van de lidstaten om de veiligheid van hun 5G-netwerken te waarborgen, te ondersteunen.

49 De veiligheid van 5G-netwerken bestrijkt zowel nationale als EU-bevoegdheden en is van belang voor de nationale veiligheid. De Commissie benaderde de veiligheid van 5G-netwerken in de zin van bedreigingen voor de nationale veiligheid en koos daarom voor “soft law”-maatregelen. Dit houdt in dat de EU geen juridisch bindende maatregelen kan nemen die de lidstaten zouden dwingen uniforme risicobeperkende maatregelen toe te passen, of afdwingbare voorschriften ten uitvoer kan leggen. In plaats daarvan kan de Commissie niet-bindende aanbevelingen en mededelingen doen, beste praktijken helpen verspreiden en de nationale acties van de lidstaten coördineren. Niettemin is een andere aanpak mogelijk. Een voorbeeld hiervan is de

NIS-richtlijn[40], een EU-wet die betrekking heeft op de beveiliging van netwerk- en informatiesystemen in de Unie. Deze wet was voorgesteld door de Commissie en vastgesteld op basis van de rechtsgrondslag betreffende de "eengemaakte markt" hoewel cyberbeveiliging grotendeels onder de nationale bevoegdheden valt[41].

EU-toolbox voor 5G-cyberbeveiliging werd in een vroeg stadium van de invoering vastgesteld, maar een aantal mobiele-netwerkexploitanten had al leveranciers geselecteerd

50 In januari 2020 stelde de NIS-samenwerkingsgroep een EU-toolbox voor 5G-cyberbeveiliging vast, waarin een aantal strategische, technische en ondersteunende maatregelen wordt beschreven om bedreigingen voor de veiligheid van het 5G-netwerk aan te pakken en de relevante actoren voor elk van deze maatregelen worden aangewezen. Deze door de Commissie en de Europese Raad bekrachtigde toolbox werd pas negen maanden nadat het Europees Parlement en de Raad voor het eerst hun bezorgdheid over de beveiliging van 5G hadden geuit, vastgesteld. Meer recentelijk is de EU-toolbox voor 5G-cyberbeveiliging genoemd in de nieuwe Europese strategie om slimme, schone en veilige verbindingen in digitale systemen over de hele wereld te stimuleren, als een instrument om investeringen in digitale infrastructuur te sturen[42]. De "soft law"-aanpak van de Commissie heeft ertoe bijgedragen dat snel maatregelen konden worden genomen om ook op EU-niveau het hoofd te bieden aan bedreigingen voor de veiligheid en om de samenwerking tussen de lidstaten op dit grensoverschrijdende gebied te vergemakkelijken. Ter vergelijking: bij de NIS-richtlijn was het tijdsverloop tussen de indiening van het voorstel van de Commissie[43] en de goedkeuring ervan[44] meer dan drie jaar, en bij de EECC-richtlijn meer dan twee jaar[45]. Er was zelfs nog meer tijd nodig voor de omzetting van de richtlijnen in de nationale rechtsstelsels van de lidstaten (zie ook de paragrafen ***36*** en ***37***).

---

[40] Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

[41] Analyse nr. 02/2019 "Uitdagingen voor een doeltreffend EU-beleid inzake cyberbeveiliging" (briefingdocument), paragraaf 36.

[42] Gezamenlijke mededeling aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité, het Comité van de Regio's en de Europese Investeringsbank — De Global Gateway. JOIN (2021) 30 final van 1.12.2021.

[43] COM(2013) 48 final van 7 februari 2013.

[44] Richtlijn (EU) 2016/1148.

[45] COM(2016) 590 final/2 van 12 oktober 2016 en Richtlijn (EU) 2018/1972 tot vaststelling van het Europees wetboek voor elektronische communicatie.

51 De EU-toolbox voor 5G-cyberbeveiliging werd vier jaar nadat het 5G-beleid in het 5G-actieplan was gepresenteerd, vastgesteld, in hetzelfde jaar waarin de tussentijdse mijlpalen voor de invoering die in het kader van dit 5G-actieplan waren vastgesteld, hadden moeten zijn bereikt. In dit verband waren voor deze controle bevraagde vertegenwoordigers van de ministeries van de lidstaten, de nationale regelgevende autoriteiten en mobiele-netwerkexploitanten van mening dat de maatregelen inzake de veiligheidsaspecten van 5G te laat van start zijn gegaan.

52 Tegelijkertijd werd de toolbox gepubliceerd toen de invoering van en plannen voor 5G in de meeste lidstaten nog in de kinderschoenen stonden. De meeste contracten tussen leveranciers en exploitanten voor 5G-apparatuur werden in 2020 en 2021 gesloten. Volgens de European Telecommunications Network Operators' Association (ETNO) had een aantal mobiele-netwerkexploitanten echter al leveranciers geselecteerd toen de EU-toolbox voor 5G-cyberbeveiliging beschikbaar werd.

De EU-toolbox voor 5G-cyberbeveiliging bood een kader voor de beoordeling van het risicoprofiel van leveranciers, maar er bleven tekortkomingen bestaan

Sommige lidstaten en nationale autoriteiten vinden een deel van de criteria die worden gehanteerd om leveranciers als leveranciers met een hoog risico te classificeren, niet duidelijk genoeg

53 Een belangrijk kenmerk van de EU-toolbox voor 5G-cyberbeveiliging is de eis dat de lidstaten leveranciers beoordelen en, voor essentiële voorzieningen die zijn aangemerkt als kritiek, beperkingen toepassen ten aanzien van leveranciers met een hoog risico. De lidstaten moeten deze beoordeling maken op basis van een niet-uitputtende lijst van criteria die zijn afgeleid van de gecoördineerde EU-risicobeoordeling. Dergelijke criteria zijn bijvoorbeeld:

- de waarschijnlijkheid dat een leverancier blootstaat aan inmenging van een niet-EU-land; bijvoorbeeld door het bestaan van een sterke band tussen de leverancier en een regering van een niet-EU-land; of door de wetgeving van het niet-EU-land, met name wanneer er geen wetgevende of democratische controlemechanismen bestaan, of bij het ontbreken van overeenkomsten inzake veiligheid of gegevensbescherming tussen de EU en het niet-EU-land;
- het vermogen van de leverancier om de levering te waarborgen, en
- de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van de leverancier.

54 De toolbox is ontwikkeld om versnippering te voorkomen en consistentie in de interne markt te bevorderen. De criteria in de toolbox bieden een operationeel kader dat nuttig is om het risicoprofiel van leveranciers in alle lidstaten op gecoördineerde wijze te beoordelen. Het stelde de Commissie ook in staat om, samen met de lidstaten, snel te reageren op nieuwe kwesties inzake de beveiliging van 5G. Tegelijkertijd blijft het de verantwoordelijkheid van de nationale autoriteiten om deze criteria toe te passen bij de beoordeling van de risico's in verband met specifieke leveranciers. Tegen oktober 2021 hadden 13 lidstaten, rekening houdend met dit kader, wetgeving inzake 5G-beveiliging vastgesteld of gewijzigd (zie paragraaf ***75*** en ***figuur 6***).

55 De vertegenwoordigers van twee van de vier ministeries van de lidstaten die we voor deze controle hebben bevraagd, waren echter van mening dat sommige van deze criteria voor de classificatie van 5G-leveranciers vatbaar zijn voor interpretatie en verder moeten worden verduidelijkt. Zij vroegen de Commissie ook om verdere steun en richtsnoeren met betrekking tot de classificatie van leveranciers met een hoog risico. Vertegenwoordigers van de lidstaten met wie we hebben gesproken, gaven ook aan dat deze situatie het risico met zich meebrengt dat de lidstaten uiteenlopende benaderingen toepassen ten aanzien van leveranciers met een hoog risico (zie ook de paragrafen ***74*** en ***75*** en ***kader 5***). Elf van de bevraagde nationale regelgevende instanties, die in verschillende mate betrokken zijn bij de beveiliging van 5G, hebben soortgelijke bezorgdheid geuit.

Het land van herkomst van 5G-leveranciers is van invloed op de beoordeling van veiligheidsrisico's

56 5G-leveranciers verschillen wat hun bedrijfskenmerken betreft en zijn afkomstig uit landen met verschillende banden met de EU. ***Figuur 5*** toont een aantal overeenkomsten en verschillen tussen de belangrijkste 5G-leveranciers en hun landen van herkomst, met name op gebieden die in de toolbox worden genoemd als waarschijnlijk van invloed op de beoordeling van hun risicoprofiel (zie paragraaf ***53***).

Figuur 5 — Overeenkomsten en verschillen tussen 5G-leveranciers en hun landen van herkomst

Bron: ERK, op basis van WTO-leden, OESO-leden, FDI Restrictiveness Index van de OESO, Wereldbank, Worldwide Governance Indicators Dataset, 2019, WEF Global Competitiveness Dataset, Ranking in 2018, adequaatheidsbesluiten, Statista, Who is leading the 5G patent race?, Ericsson-bedrijfsgegevens, Nokia-bedrijfsgegevens, Qualcomm-bedrijfsgegevens, Sharp-bedrijfsgegevens, LG-bedrijfsgegevens, Samsung-bedrijfsgegevens, Huawei-bedrijfsgegevens en ZTE-bedrijfsgegevens. Wisselkoersen per 31 december 2020.

57 Een risicofactor wordt gevormd door de mate waarin het land van herkomst van een leverancier zich houdt aan de politieke en economische kernwaarden van de EU. Gerelateerde landspecifieke factoren zoals de rechtsstaat, de onafhankelijkheid van de rechterlijke macht, de openheid voor buitenlandse investeringen en het bestaan van overeenkomsten inzake gegevensbescherming kunnen worden beschouwd als een maatstaf voor de juridische bescherming die een onderneming geniet tegen overheidsinmenging, alsmede voor de bescherming die zij haar klanten kan bieden.

58 Terwijl in de EU-lidstaten gevestigde leveranciers verplicht zijn de normen en wettelijke voorschriften van de EU na te leven, geldt dit niet voor zes van de belangrijkste in niet-EU-landen gevestigde leveranciers, die binnen het kader van de wetgeving van derde landen opereren (zie ***figuur 5***). Dergelijke wetgeving kan aanzienlijk afwijken van de EU-normen, bijvoorbeeld wat betreft de gegevensbescherming die aan burgers wordt geboden, de doeltreffendheid van die bescherming, of meer in het algemeen de wijze waarop de onafhankelijkheid van de rechterlijke macht wordt gewaarborgd door wetgevende en/of democratische controlemechanismen. Wat de onafhankelijkheid van de rechterlijke macht betreft, scoren de VS en Japan hoger dan de andere niet-EU-landen van herkomst van 5G-leveranciers, terwijl voor de beoordeling van de rechtsstaat Zuid-Korea het beste scoort van de niet-EU-landen.

59 5G-netwerken draaien overwegend op software. Het feit dat sommige leveranciers binnen het kader van wetgeving van een derde land opereren, kan bijzonder zorgwekkend zijn indien de controlecentra van de software ook in niet-EU-landen staan, waardoor gebruikers in de EU mogelijk worden onderworpen aan wetgeving van derde landen.

60 De Commissie is begonnen deze punten van zorg aan te pakken, waarbij zij van mening is dat elk bedrijf dat diensten verleent aan EU-burgers de EU-regels en -waarden in acht moet nemen[46]. Zij is met verschillende landen een dialoog aangegaan om een sterke privacybescherming voor persoonsgegevens te waarborgen[47]. Uit ***figuur 5*** blijkt ook dat de Commissie ten aanzien van Japan (en in het verleden, de VS) al heeft erkend dat de gegevensbeschermingsregelingen adequaat zijn. Er moet echter op worden gewezen dat adequaatheidsbesluiten kunnen worden aangevochten en aan

---

[46] Mededeling van de Europese Commissie, De digitale toekomst van Europa vormgeven, COM(2020) 67 final.

[47] EU-China — Een strategische visie.

strikte rechterlijke toetsing zijn onderworpen. Zo heeft het Europees Hof van Justitie in 2015 het toen geldende rechtsinstrument voor gegevensuitwisseling met de Verenigde Staten, de Safe Harbour-overeenkomst[48], vernietigd en later, in 2020, geoordeeld dat het privacyschild — dat de Safe Harbour-overeenkomst verving — EU-burgers onvoldoende bescherming bood[49]. Er is dus momenteel geen adequaatheidsbesluit voor de Verenigde Staten. Meer in het algemeen, en afgezien van het bestaan van een gegevensbeschermingsregeling, is het belangrijk rekening te houden met het bredere juridische en institutionele kader, met inbegrip van bijvoorbeeld de eerbiediging van de rechtsstaat en de wijze waarop de onafhankelijkheid van de rechterlijke macht wordt gewaarborgd.

61 ***Figuur 5*** toont ook een aanzienlijke variatie tussen de 5G-leveranciers qua aandeel 5G-octrooien, inkomsten en personeelsbestand. Dit heeft gevolgen voor de middelen waarover zij beschikken, wat op zijn beurt van invloed kan zijn op hun veerkracht en hun vermogen om een continue voorziening te garanderen. Samsung en Huawei zijn bijvoorbeeld de leveranciers met het grootste aandeel 5G-octrooien, die als bedrijf de hoogste inkomsten genereren en in totaal het grootste aantal werknemers hebben.

62 De waarschijnlijkheid dat een leverancier blootstaat aan inmenging van de regering van een niet-EU-land is een andere belangrijke factor die in de toolbox wordt omschreven als bepalend voor het risicoprofiel van een leverancier. In dit verband speelt eigendom een belangrijke rol, aangezien eigenaars met een groot aantal aandelen in staat kunnen zijn druk uit te oefenen of managementbeslissingen te beïnvloeden. Voorts worden ondernemingen die eigendom van de overheid of particulier eigendom zijn verondersteld minder open te staan voor publiek toezicht wat betreft controles en verantwoordingsplicht, vergeleken met beursgenoteerde ondernemingen, die het hele jaar door onderworpen zijn aan strenge openbaarmakingsvereisten ten behoeve van algemene beleggers en regelgevers. De meeste 5G-leveranciers zijn beursgenoteerd, hetzij in hun land van herkomst, hetzij in

[48] Arrest in zaak C-362/14 en https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117nl.pdf

[49] Arrest in zaak C-311/18 en https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091nl.pdf

het buitenland, terwijl de Chinese leveranciers moeilijker te classificeren zijn en over het algemeen worden beschouwd als nauw verbonden met de Chinese regering[50].

De lidstaten vonden de steun van de Commissie en het Enisa nuttig bij de uitvoering van de EU-toolbox voor 5G-cyberbeveiliging

63 De Commissie heeft de lidstaten steun verleend door middel van de uitwisseling van beste praktijken met betrekking tot een aantal belangrijke maatregelen van de EU-toolbox voor 5G-cyberbeveiliging, met inbegrip van maatregelen inzake leveranciers met een hoog risico. Deze steun, die vaak werd verleend in het kader van de NIS-samenwerkingsgroep, werd aangevuld met specifieke activiteiten van het Enisa, zoals de organisatie van webinars of de verstrekking van richtsnoeren over:

- de uitvoering van de toolbox, met de nadruk op de technische maatregelen, en
- beste praktijken inzake netwerkbeveiliging, in het bijzonder inzake:
  - de 5G-dreigingslandschappen[51];
  - de voorbereiding van nationale 5G-risicobeoordelingen, en
  - veiligheidsmaatregelen in het kader van het EECC[52], met inbegrip van specifieke richtsnoeren inzake de beveiliging van 5G[53].

64 De Commissie heeft het Enisa ook opgedragen de EU-certificeringsregeling voor cyberbeveiliging voor 5G-netwerken voor te bereiden, die de risico's in verband met technische kwetsbaarheden van de netwerken moet helpen aanpakken en de cyberbeveiliging verder moet verbeteren[54]. Hoewel deze certificering kan bijdragen tot een betere beveiliging, kan deze niet voorkomen dat bedreigingen via software-updates in de systemen worden geïntegreerd.

---

[50] https://www.europarl.europa.eu/doceo/document/E-9-2020-004305_EN.html en https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637912/EPRS_ATA(2019)637912_EN.pdf

[51] Enisa, Threat Landscape for 5G Networks, 14 december 2020.

[52] Enisa, Guideline on Security Measures under the EECC, 10 december 2020.

[53] Enisa, 5G supplement to the Guidelines on Security Measures under the EECC, 7 juli 2021.

[54] Persbericht van 3 februari 2021.

65 Alle voor deze controle door ons bevraagde vertegenwoordigers van de autoriteiten van de lidstaten benadrukten het nut van de steun van de Commissie en het Enisa bij de uitvoering van de EU-toolbox voor 5G-cyberbeveiliging. Bovendien verklaarden de meeste nationale regelgevende telecomautoriteiten (15 van de 21) dat de Commissie en/of het Enisa de nationale autoriteiten hebben gesteund bij de uitwisseling van beste praktijken voor de uitvoering van de belangrijkste strategische maatregelen.

De EU-toolbox voor 5G-cyberbeveiliging was te laat vastgesteld om in aanmerking te kunnen worden genomen voor door de EU gecofinancierde projecten in de periode 2014-2020

66 Een van de doelstellingen van de EU-toolbox voor 5G-cyberbeveiliging is ervoor te zorgen dat bij door de EU gecofinancierde 5G-projecten rekening wordt gehouden met cyberbeveiligingsrisico's. De toolbox is echter pas in januari 2020 vastgesteld. Omdat alle projecten die we voor deze controle hebben onderzocht, waren geselecteerd vóór de vaststelling van de EU-toolbox voor 5G-cyberbeveiliging, kon er niet worden verwacht dat hierbij de aanbevolen aanpak inzake cyberbeveiliging was gevolgd, ook niet ten aanzien van leveranciers met een hoog risico. In onze steekproef hebben wij bijvoorbeeld één Horizon 2020-project en twee EFRO-projecten in Spanje aangetroffen waarbij Chinese 5G-apparatuur werd gebruikt die vervolgens in Zweden werd verboden (zie paragraaf ***15***).

67 Voor de periode 2021-2027 wil de Commissie een samenhangende aanpak inzake beveiliging van 5G voor door de EU gecofinancierde projecten bevorderen door ervoor te zorgen dat de naleving van de toolbox een voorwaarde is voor EU-financiering. Dit zal echter variëren naar gelang van de wijze van uitvoering:

- bij programma's die rechtstreeks door de Commissie worden beheerd (bijvoorbeeld Horizon Europa 2021-2027) zullen leveranciers kunnen worden uitgesloten die blootstaan aan inmenging door de regering van een niet-EU-land. Dit zal er waarschijnlijk voor zorgen dat bij door de EU gefinancierde projecten rekening wordt gehouden met cyberbeveiligingsrisico's en dat situaties worden voorkomen waarin een leverancier in de ene lidstaat cofinanciering van de EU ontvangt, terwijl hij in een andere lidstaat als leverancier met een hoog risico wordt beschouwd en wordt uitgesloten;

- voor programma's die onder gedeeld beheer worden uitgevoerd, bevat de wetgeving geen voorschriften over cyberbeveiligingsrisico's. Daarom is de Commissie van plan de opname van een verwijzing naar de toolbox in de partnerschapsovereenkomsten van de lidstaten te bevorderen als een manier

waarop bij EFRO-financiering voor 5G-gerelateerde projecten rekening kan worden gehouden met cyberbeveiligingsrisico's, en

- voor InvestEU (het programma dat het EFSI vervangt)[55] en de RRF is de Commissie van plan de betrokken instanties aan te moedigen om in de financieringsovereenkomsten naar de EU-toolbox te verwijzen.

De lidstaten pakken bij de invoering van 5G-netwerken de veiligheidsaspecten nog niet op een gecoördineerde manier aan

De informatie over de wijze waarop de lidstaten veiligheidskwesties aanpakken, is ontoereikend

68 De Commissie volgt en rapporteert over de voortgang bij de uitvoering van de EU-toolbox voor 5G-cyberbeveiliging via de NIS-samenwerkingsgroep, bilaterale gesprekken met lidstaten en indirect via de media. De eerste resultaten van deze monitoring zijn in juli 2020 bekendgemaakt[56]. In december 2020 heeft de Commissie ook een verslag gepubliceerd over de impact van haar aanbeveling inzake de cyberbeveiliging van 5G-netwerken[57]. Vanaf september 2021 was geen verdere rapportage meer gepland.

69 In de bovengenoemde verslagen ontbreekt echter een gemeenschappelijke reeks kernprestatie-indicatoren en wordt geen vergelijkbare reeks gedetailleerde gegevens verstrekt over de wijze waarop de lidstaten kwesties inzake de beveiliging van 5G aanpakken.

70 Voorts is er weinig publiek beschikbare informatie over de benadering die de lidstaten volgen ten aanzien van leveranciers met een hoog risico, d.w.z. hun identificatie en of leveranciers worden uitgesloten van het leveren van hun 5G-apparatuur, en zelfs die informatie is tegenstrijdig en onvolledig. Enkele voorbeelden:

- In haar verslag van juli 2020 over de vorderingen van de lidstaten bij de uitvoering van de toolbox (zie paragraaf ***68***) stelde de Commissie dat ongeveer de helft van

---

[55] Verordening (EU) 2021/523 tot vaststelling van het InvestEU-programma.

[56] Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity, juli 2020.

[57] Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks, SWD(2020) 357 final van 16 december 2020.

de lidstaten (14 van de 27) het risicoprofiel van leveranciers had beoordeeld en beperkingen hadden toegepast ten aanzien van leveranciers die werden beschouwd als leveranciers met een hoog risico.

- In een verslag van Berec van december 2020[58] werd vermeld dat slechts 9 lidstaten dergelijke beperkingen hadden ingesteld, en dat 7 van de resterende 18 lidstaten niet van plan waren dat in de toekomst te doen.

71 Zelfs wanneer de lidstaten wetgeving inzake de veiligheid van 5G-netwerken hebben vastgesteld (zie ook paragraaf ***75***), wordt hiermee nog geen duidelijkheid over de aanpak van de lidstaten ten aanzien van leveranciers met een hoog risico verschaft. Concrete beslissingen zullen waarschijnlijk alleen via uitvoeringsbesluiten of niet-openbare administratieve of commerciële besluiten worden genomen.

72 Volgens de door ons bevraagde belanghebbenden en besluitvormers (bijvoorbeeld bij het Europees Parlement) is niet-openbare informatie (bijvoorbeeld via verslagen van de Commissie of de NIS-samenwerkingsgroep) over de aanpak van leveranciers met een hoog risico door de lidstaten eveneens schaars, en moeten deze entiteiten zich verlaten op de media en niet-officiële bronnen.

73 Ondanks de grensoverschrijdende aard van de kwesties inzake de beveiliging van 5G is er over het algemeen weinig openbare informatie beschikbaar over de wijze waarop de lidstaten beveiligingskwesties, en in het bijzonder de kwestie van leveranciers met een hoog risico, aanpakken. Dit belemmert de uitwisseling van kennis tussen de lidstaten en de mogelijkheid om gecoördineerde maatregelen toe te passen. Het beperkt ook de mogelijkheid voor de Commissie om verbeteringen in de veiligheid van 5G-netwerken voor te stellen.

Er zijn aanwijzingen dat sommige lidstaten uiteenlopende benaderingen ten aanzien van 5G-leveranciers volgen

74 Nationale autoriteiten hebben een ruime beoordelingsmarge met betrekking tot de uitvoering van belangrijke maatregelen inzake de beveiliging van 5G (zie de paragrafen ***48*** en ***49***). In de toolbox wordt rekening gehouden met nationale bevoegdheden en relevante landspecifieke factoren (dreigingsevaluatie van nationale veiligheidsdiensten, tijdpad voor de invoering van 5G, de aanwezigheid van leveranciers, cyberbeveiligingscapaciteiten). Tot dusver hebben de lidstaten

[58] Berec, Intern verslag over de strategische maatregelen 5 en 6 (diversifiëring van leveranciers en versterking van de nationale veerkracht) van de EU-toolbox voor 5G-cyberbeveiliging, BoR 20 (227), 10 december 2020.

uiteenlopende benaderingen toegepast wat betreft het gebruik van apparatuur van specifieke leveranciers of de reikwijdte van de beperkingen ten aanzien van leveranciers met een hoog risico (zie voorbeelden van vier lidstaten in ***kader 5***).

Kader 5

Voorbeelden van uiteenlopende benaderingen van de lidstaten ten aanzien van Chinese 5G-leveranciers

Vastgesteld kader en toegepaste beperkingen[1]

In oktober 2020 heeft de Zweedse nationale regelgevende telecomautoriteit (PTS) de volgende voorwaarden voor deelname aan de veiling van 5G-frequenties gesteld:

— nieuwe installaties en de implementatie van centrale functies voor het radiogebruik in de frequentiebanden mogen geen producten gebruiken van Chinese leveranciers, en

— alle bestaande infrastructuur van dergelijke leveranciers moet uiterlijk op 1 januari 2025 buiten gebruik zijn gesteld.

Kader vastgesteld, maar nog niet toegepast[2], [3], [4]

In Duitsland voorziet de wet inzake IT-veiligheid 2.0 van mei 2021 in verplichte certificering van kritieke onderdelen voordat het gebruik ervan kan worden toegestaan. De Duitse mobiele-netwerkexploitanten die wij hebben gesproken, zouden de voorkeur geven aan één enkele Europese certificeringsprocedure onder auspiciën van het Enisa, die als Europese “onestopshop” zou fungeren, in plaats van mogelijk allerlei nationale certificeringen te moeten doorlopen. De wet biedt het federale Ministerie van Binnenlandse Zaken ook de mogelijkheid het gebruik van kritieke onderdelen te verbieden indien deze een bedreiging kunnen vormen voor de nationale veiligheid.

In Oostenrijk stelt de geactualiseerde telecomwet die eind oktober 2021 is vastgesteld, de bevoegde minister in staat leveranciers als leveranciers met een hoog risico te classificeren en beperkingen op hen toe te passen of hen van de markt uit te sluiten. Openbaar beschikbare informatie van oktober 2021 geeft aan dat het land op koers is om zijn 5G-netwerk uit te breiden, met behulp van de Chinese leverancier Huawei.

Geen kader vastgesteld[5], [6]

Hongarije had in september 2021 nog ten aanzien van geen enkele 5G-leverancier beperkingen ingesteld en zal dat in de nabije toekomst waarschijnlijk ook niet doen. Hongarije heeft ook officieel geweigerd zich aan te sluiten bij het internationale 5G Clean Network Program, dat door de VS wordt gepromoot en dat tot doel heeft de aanwezigheid van Chinese leveranciers in 5G-kernnetwerken te beperken.

(1) Besluit 18-8496 van 20.10.2020 inzake de voorwaarden voor de veilig van de frequentiebanden 3,5 GHz en 2,3 GHz.

(2) Zweites Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

(3) Telecomwet Oostenrijk

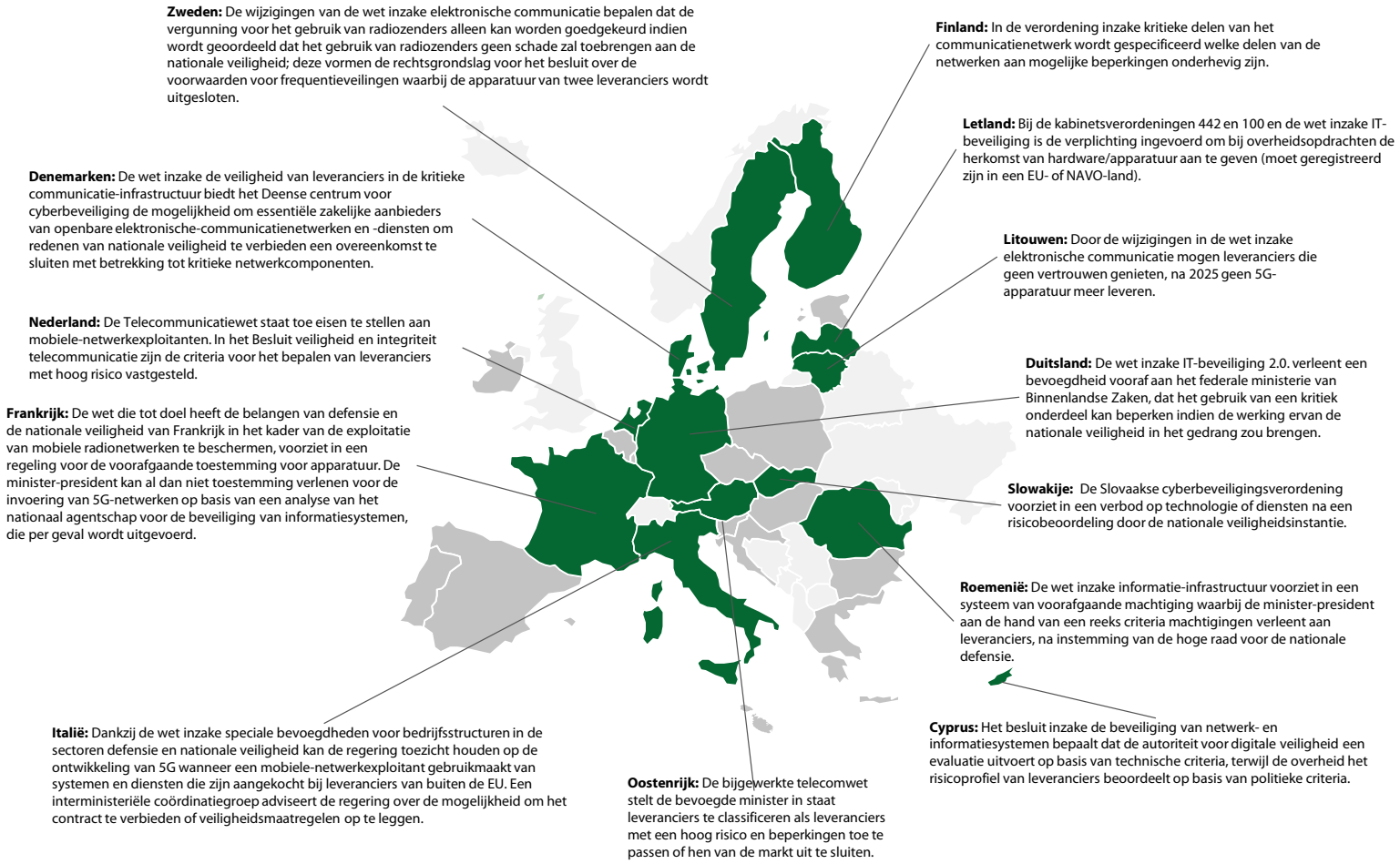
(4) https://www.euractiv.com/section/5g/news/austria-to-also-rely-on-huawei-in-5g-rollout/

(5) https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf

(6) https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/hungary

75 Sinds de goedkeuring van de toolbox is vooruitgang geboekt met het versterken van de beveiliging van 5G-netwerken, waarbij een meerderheid van de lidstaten beperkingen toepast of zal toepassen op leveranciers met een hoog risico. Eind 2021 hadden 13 lidstaten nationale wetgeving inzake 5G-beveiliging vastgesteld of gewijzigd. Bij deze regelgevende maatregelen is rekening gehouden met de in de toolbox vastgestelde criteria, maar worden verschillende benaderingen gevolgd (zie ***figuur 6***). Andere lidstaten zijn bezig met de indiening van dergelijke wetgeving. In de komende jaren kan dit leiden tot een meer convergente aanpak van 5G-leveranciers met een hoog risico, ten minste in de lidstaten die dergelijke wetgeving hebben vastgesteld.

Figuur 6 — Lidstaten die wetten hebben vastgesteld op grond waarvan apparatuur van leveranciers met een hoog risico van hun netwerken kan worden geweerd, oktober 2021



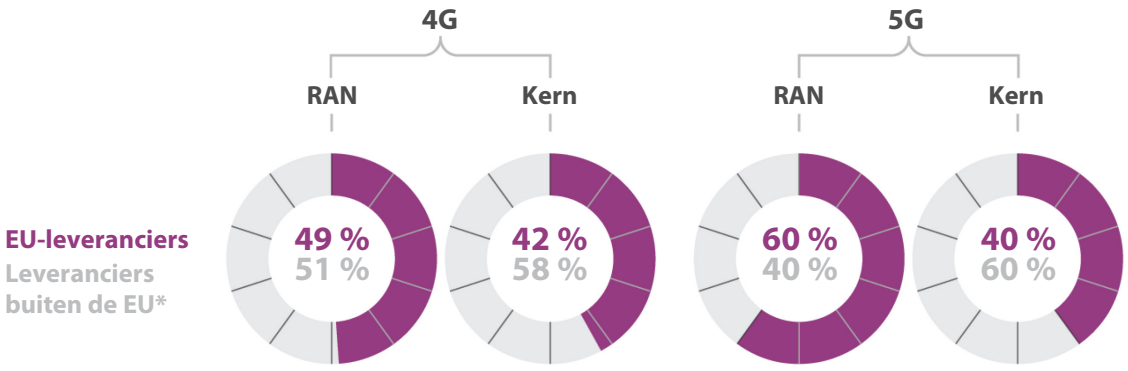
Bron: ERK, op basis van gegevens van de Europese Commissie.

76 Tot dusver heeft de Commissie niet beoordeeld wat de impact zou zijn van dergelijke uiteenlopende benaderingen wanneer de ene lidstaat zijn 5G-netwerken bouwt met apparatuur van een leverancier die in een andere lidstaat als leverancier met een hoog risico wordt beschouwd. Dit kan gevolgen hebben voor de grensoverschrijdende veiligheid of de concurrentie tussen mobiele-netwerkexploitanten die actief zijn op de eengemaakte markt van de EU.

De Commissie is onlangs begonnen met het aanpakken van de kwestie van buitenlandse subsidies die de interne markt verstoren

77 In december 2020 was meer dan de helft van de 4G- en 5G-apparatuur in de EU afkomstig van niet-EU-leveranciers (zie ***figuur 7***).

Figuur 7 — Aandeel mobiele-netwerkexploitanten dat apparatuur van leveranciers van binnen/buiten de EU* gebruikt



Bron: ERK, op basis van Berec. Intern verslag over de strategische maatregelen 5 en 6 (diversifiëring van leveranciers en versterking van de nationale veerkracht) van de EU-toolbox voor 5G-cyberbeveiliging. BoR (20) 227.

78 Met name maakten eind 2019 286 miljoen klanten in de EU-27 (64 % van de totale bevolking) gebruik van telecommunicatienetwerken op basis van 4G-apparatuur van Chinese leveranciers[59]. In oktober 2020 heeft een groep leden van het Europees Parlement zijn bezorgdheid geuit aan de ministers van Telecommunicatie en Handel van de lidstaten en de Commissie over het feit dat een van de redenen voor het grote marktaandeel van Chinese leveranciers was dat zij een oneerlijk economisch voordeel genoten, namelijk dat zij overheidssubsidies ontvingen die EU-leveranciers op grond

[59] StrandConsult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks.

van de EU-staatssteunregels niet kunnen krijgen[60]. In een recente analyse hebben wij gewezen op soortgelijke risico's in dit verband[61]. Dergelijke subsidies kunnen de interne markt verstoren en zo een ongelijk speelveld creëren tussen 5G-leveranciers, met mogelijke gevolgen voor de veiligheid. Om dit probleem aan te pakken, heeft de Commissie in mei 2021 een nieuwe verordening[62] voorgesteld, waarin procedures worden vastgesteld voor het onderzoeken van dergelijke subsidies en het verhelpen van de daarmee gepaard gaande marktverstoringen.

De Commissie beschikt niet over voldoende informatie inzake eventuele vervangingskosten voor de apparatuur van Chinese leveranciers

79 Volgens een verslag van juni 2020[63] zou het instellen van beperkingen ten aanzien van een belangrijke leverancier van 5G-infrastructuur in de EU de totale investeringskosten de komende tien jaar met bijna 2,4 miljard EUR per jaar (d.w.z. 24 miljard EUR) doen stijgen. Volgens een andere studie[64] staan Europese exploitanten nu al voor de upgrade van 4G-netwerken die tussen 2012 en 2016 zijn aangelegd, omdat het een standaardpraktijk is om netwerkapparatuur die meer dan drie tot vier jaar oud is, te reviseren en te moderniseren. In deze studie worden de totale kosten voor "rip and replace" (verwijderen en vervangen) van op te waarderen apparatuur die sinds 2016 bij Chinese leveranciers is gekocht, op ongeveer 3 miljard EUR geraamd.

80 Het grote aandeel apparatuur van Chinese leveranciers, in combinatie met het feit dat zij in bepaalde lidstaten mogelijk als leveranciers met een hoog risico worden aangemerkt, kan leiden tot vervangingskosten in de orde van grootte van miljarden indien mobiele-netwerkexploitanten de apparatuur van de Chinese leveranciers zonder een overgangsperiode uit de Europese netwerken moeten verwijderen en

---

[60] Brief van leden van het Europees Parlement aan de EU-ministers van Telecommunicatie en Handel en aan de Europese commissarissen Thierry Breton, Margrethe Vestager en Valdis Dombrovskis, 14 oktober 2020.

[61] Analyse nr. 03/2020: "De respons van de EU op de Chinese staatsgestuurde investeringsstrategie".

[62] Voorstel voor een verordening betreffende buitenlandse subsidies die de interne markt verstoren, COM(2021) 223 final van 5 mei 2021.

[63] Oxford Economics, Restricting competition in 5G network equipment throughout Europe, juni 2020. (Gesponsord door Huawei).

[64] StrandConsult, The real cost to "rip and replace" Chinese equipment from telecom networks.

vervangen (zie de paragrafen ***77***-***79***). In beginsel kan staatssteun niet worden verleend om marktdeelnemers te compenseren voor het nakomen van wettelijke verplichtingen, tenzij de lidstaten tegenover de Commissie kunnen aantonen dat aan de nodige voorwaarden is voldaan (zoals een stimulerend effect). Uit onze analyse is gebleken dat er één geval is waarin het op grond van de nationale wetgeving wellicht is toegestaan vervangingskosten te ondersteunen met nationale overheidsfinanciering (zie de Finse wet inzake elektronische communicatiediensten[65]). De lidstaten moeten de Commissie in kennis stellen van alle gevallen van staatssteun waarmee mobiele-netwerkexploitanten worden gecompenseerd voor dergelijke kosten. Volgens de Commissie heeft tot dusver geen enkele lidstaat of belanghebbende contact met haar opgenomen om staatssteun voor de kosten van de vervanging van apparatuur te bespreken. Volgens belanghebbenden uit de sector die tijdens de controle werden bevraagd, ondermijnen de onzekerheid over de behandeling van dergelijke kosten door de lidstaten en mogelijke verschillen tussen de lidstaten de bedrijfszekerheid en dreigen zij de tijdige invoering van 5G te beïnvloeden.

[65] Wet inzake elektronische communicatiediensten 1207/2020 van 30 december 2020, artikel 301.

Conclusies en aanbevelingen

81 In het algemeen bleek uit onze controle dat er, ondanks de steun van de Commissie, aanzienlijke vertragingen zijn bij de invoering van 5G-netwerken door de lidstaten en dat verdere inspanningen nodig zijn voor de aanpak van beveiligingskwesties bij de invoering van 5G.

82 De Commissie heeft in haar 5G-actieplan van 2016 opgeroepen tot een 5G-dekking van alle stedelijke gebieden en op belangrijke transportroutes tegen 2025 en, in maart 2021, tot een volledige dekking tegen 2030. Eind 2020 hadden 23 lidstaten commerciële 5G-diensten ingevoerd en hadden zij de tussentijdse doelstelling behaald dat ten minste één grote stad toegang heeft tot dergelijke diensten. We constateerden echter dat niet alle lidstaten in hun nationale 5G-strategieën of breedbandplannen naar de doelstellingen van de Commissie verwijzen. In verschillende landen is het Europees wetboek voor elektronische communicatie bovendien nog niet in nationaal recht omgezet en heeft de toewijzing van 5G-frequenties vertraging opgelopen. Deze vertragingen bij de toewijzing van de frequenties kunnen worden toegeschreven aan verschillende oorzaken: een geringe vraag van mobiele-netwerkexploitanten, grensoverschrijdende coördinatieproblemen met niet-EU-landen langs de oostgrenzen, de impact van COVID-19 op de geplande veilingen en onzekerheid over de aanpak van beveiligingskwesties. Volgens de Commissie zullen waarschijnlijk slechts elf lidstaten de doelstelling voor 2025 halen (zie de paragrafen ***22-43***).

83 De Commissie heeft de lidstaten ondersteund bij de uitvoering van het 5G-actieplan van 2016 door middel van initiatieven, richtsnoeren en de financiering van 5G-gerelateerd onderzoek. De Commissie heeft de verwachte kwaliteit van de dienstverlening van 5G-netwerken, bijvoorbeeld de prestaties die zij moeten leveren wat betreft minimumsnelheid en maximale latentietijd, echter niet omschreven. Dit heeft ertoe geleid dat de term “5G-kwaliteit” door de lidstaten verschillend wordt opgevat. Wij hebben vastgesteld dat de lidstaten bij de invoering van 5G-diensten uiteenlopende benaderingen volgen, zoals het feit dat slechts twee lidstaten een minimumsnelheid en een maximumlatentietijd hebben vastgesteld. Uiteindelijk houden deze uiteenlopende benaderingen het risico in dat de toegang tot en de kwaliteit van 5G-diensten in de EU ongelijk worden, waardoor de “digitale kloof” tussen lidstaten en regio’s eerder groter dan kleiner wordt (zie de paragrafen ***22-31***).

Aanbeveling 1 — Bevorder een gelijkmatige en tijdige invoering van 5G-netwerken in de EU

De Commissie moet:

a) samen met de lidstaten een gemeenschappelijke omschrijving ontwikkelen van de verwachte kwaliteit van de dienst van 5G-netwerken, zoals de prestatie-eisen die deze netwerken moeten bieden qua minimumsnelheid en maximumlatentietijd;

b) de lidstaten aanmoedigen de doelstellingen voor 2025 en 2030 voor de invoering van 5G, alsmede de maatregelen die nodig zijn om deze te verwezenlijken, op te nemen in de volgende actualiseringen van hun 5G-/digitale strategieën of breedbandplannen, en

c) de lidstaten ondersteunen bij het aanpakken van problemen in verband met de coördinatie van frequenties met buurlanden die geen EU-lidstaat zijn, bijvoorbeeld door ervoor te pleiten dat dit onderwerp op de agenda van elke relevante bijeenkomst wordt geplaatst.

Tijdpad: december 2022

84 De beveiligingsaspecten van 5G-netwerken zijn pas onlangs een belangrijk punt van zorg geworden op EU-niveau. De daarmee samenhangende noodzaak van actie op EU-niveau werd benadrukt door de Europese Raad in 2019, die opriep tot een gezamenlijke aanpak en samenwerking van de lidstaten met betrekking tot dit grensoverschrijdende onderwerp. De Commissie heeft, samen met de lidstaten, snel gereageerd op nieuwe kwesties inzake de beveiliging van 5G. In 2020 heeft de NIS-samenwerkingsgroep een EU-toolbox voor 5G-cyberbeveiliging vastgesteld, waarin een aantal strategische, technische en ondersteunende maatregelen wordt beschreven om bedreigingen voor de veiligheid van het 5G-netwerk aan te pakken en de actoren worden aangewezen die voor elk van deze maatregelen verantwoordelijk zijn. Een aantal van deze maatregelen heeft betrekking op leveranciers van 5G-apparatuur die een hoog risico inhouden. Deze toolbox werd vervolgens bekrachtigd door de Commissie en de Europese Raad (zie de paragrafen ***45***-***47***). Omdat de toolbox een “soft law”-instrument is, zijn deze maatregelen niet bindend voor de lidstaten. Meer recentelijk is de EU-toolbox voor 5G-cyberbeveiliging genoemd in de nieuwe Europese strategie om slimme, schone en veilige verbindingen in digitale systemen over de hele wereld te stimuleren, als een instrument om investeringen in digitale infrastructuur te sturen (zie paragraaf ***50***).

85 De criteria in de toolbox bieden een operationeel kader dat nuttig is om het risicoprofiel van leveranciers in alle lidstaten op gecoördineerde wijze te beoordelen. Tegelijkertijd blijft het uitvoeren van deze beoordeling een nationale verantwoordelijkheid (zie paragraaf ***54***).

86 Sinds de goedkeuring van de toolbox is vooruitgang geboekt met het versterken van de beveiliging van 5G-netwerken, waarbij een meerderheid van de lidstaten beperkingen toepast of zal toepassen op leveranciers met een hoog risico. Tegen oktober 2021 hadden 13 lidstaten, rekening houdend met dit kader, wetgeving inzake 5G-beveiliging vastgesteld of gewijzigd. Andere lidstaten zijn bezig met de indiening van wetgeving die rekening houdt met de in de toolbox vastgestelde criteria (zie de paragrafen ***54*** en ***75***).

87 De toolbox werd in een vroeg stadium van de invoering van 5G vastgesteld, maar een aantal mobiele-netwerkexploitanten had al leveranciers voor 5G-apparatuur geselecteerd (zie paragraaf ***52***). Als bij het ontwerp van een beleid geen rekening wordt gehouden met beveiligingskwesties, bestaat het risico dat de uitvoering ervan negatief wordt beïnvloed; zo kunnen de verwachte voordelen (bijvoorbeeld groei van het bbp) worden uitgehold door de kosten voor de aanpak van bedreigingen (bijvoorbeeld kosten van cybercriminaliteit) (zie de paragrafen ***02*** en ***04***).

88 In de toolbox wordt rekening gehouden met nationale bevoegdheden en relevante landspecifieke factoren. Uit onze controle bleek dat de lidstaten tot dusver uiteenlopende benaderingen hebben toegepast wat betreft het gebruik van apparatuur van leveranciers met een hoog risico of de reikwijdte van de beperkingen (bijvoorbeeld alleen kern- en kritieke onderdelen van het 5G-netwerk, of het radiotoegangsnetwerk of een deel daarvan) (zie de paragrafen ***74*** en ***75***).

89 In de komende jaren kan wetgeving inzake 5G-beveiliging die door de lidstaten wordt vastgesteld op basis van de toolbox, leiden tot meer convergente benaderingen van 5G-leveranciers met een hoog risico. Aangezien geen van de in deze toolbox opgenomen maatregelen juridisch bindend is, is de Commissie echter niet bevoegd deze te handhaven. Daarom blijft het risico bestaan dat de toolbox op zich geen garantie is voor een gecoördineerde aanpak door de lidstaten van de veiligheidsaspecten (zie de paragrafen ***49***-***75***).

90 Veel 5G-leveranciers zijn buiten de EU gevestigd en opereren dus binnen het kader van wetgeving van derde landen, die aanzienlijk kan afwijken van de EU-normen, bijvoorbeeld wat betreft doeltreffende gegevensbescherming die aan burgers wordt

geboden, en meer in het algemeen wat betreft de wijze waarop de onafhankelijkheid van de rechterlijke macht wordt gewaarborgd door wetgevende of democratische controlemechanismen. Het feit dat 5G-netwerken overwegend op software draaien, kan ook een bijzonder veiligheidsrisico inhouden indien controlecentra van dergelijke software in niet-EU-landen worden neergezet, waardoor EU-burgers mogelijk worden onderworpen aan wetgeving van derde landen. De Commissie is begonnen deze punten van zorg aan te pakken, waarbij zij van mening is dat elk bedrijf dat diensten verleent aan EU-burgers de EU-regels en -waarden in acht moet nemen. Zij is ook met verschillende landen een dialoog aangegaan om een sterke privacybescherming voor persoonsgegevens te waarborgen (zie de paragrafen ***56***-***62***).

91 Ondanks de grensoverschrijdende aard van kwesties inzake de beveiliging van 5G is er over het algemeen een gebrek aan beschikbare openbare informatie over de wijze waarop de lidstaten beveiligingskwesties aanpakken en over hun afhankelijkheid van leveranciers met een hoog risico. De Commissie volgt de uitvoering van de toolbox en brengt er verslag over uit. De verslagen bevatten echter geen gedetailleerde en vergelijkbare informatie over de wijze waarop de lidstaten kwesties inzake de beveiliging van 5G aanpakken. Voorts is per september 2021 geen verdere rapportage meer gepland. Dit gebrek aan informatie belemmert de uitwisseling van kennis tussen de lidstaten en de mogelijkheid om gecoördineerde maatregelen toe te passen. Het beperkt ook de mogelijkheid voor de Commissie om verbeteringen in de beveiliging van 5G-netwerken voor te stellen (zie de paragrafen ***68***-***73***).

Aanbeveling 2 — Bevorder een gecoördineerde aanpak van de beveiliging van 5G onder de lidstaten

De Commissie moet:

a) verdere richtsnoeren verstrekken of maatregelen ondersteunen inzake belangrijke elementen van de EU-toolbox voor 5G-cyberbeveiliging, zoals criteria voor de beoordeling van 5G-leveranciers, hun classificatie als leveranciers met een hoog risico en overwegingen inzake gegevensbescherming;

Tijdpad: december 2022

b) transparantie over de aanpak van de lidstaten van de beveiliging van 5G bevorderen door de uitvoering van de beveiligingsmaatregelen van de EU-toolbox voor 5G-cyberbeveiliging te monitoren en er verslag over uit te brengen. Dit moet

worden gedaan aan de hand van een gemeenschappelijke reeks kernprestatie-indicatoren;

Tijdpad: december 2022

c) samen met de lidstaten nagaan voor welke veiligheidsaspecten van 5G-netwerken er behoefte is aan het specificeren van afdwingbare eisen en in voorkomend geval het initiatief nemen tot wetgeving.

Tijdpad: december 2022

92 De Commissie is begonnen met de behandeling van de gerelateerde beschuldigingen van oneerlijk economisch voordeel als gevolg van buitenlandse subsidies. Dergelijke subsidies kunnen de interne markt verstoren en zo een ongelijk speelveld tussen 5G-verkopers creëren, met mogelijke gevolgen voor de veiligheid (zie paragraaf ***78***).

93 De Commissie beschikt niet over voldoende informatie over de behandeling door de lidstaten van potentiële vervangingskosten die zouden kunnen ontstaan als mobiele-netwerkexploitanten apparatuur van leveranciers met een hoog risico zonder een overgangsperiode van EU-netwerken zouden moeten verwijderen. Verschillen in behandeling kunnen de zekerheid voor het bedrijfsleven ondermijnen en dreigen gevolgen te hebben voor de tijdige invoering van 5G (zie de paragrafen ***79*** en ***80***). Tegelijkertijd kan de aanpak van de lidstaten inzake de beveiliging van 5G, en met name het ontbreken van een gecoördineerde aanpak in de EU, gevolgen hebben voor de doeltreffende werking van de eengemaakte markt. Tot dusver heeft de Commissie deze kwestie niet beoordeeld (zie de paragrafen ***74***-***76***).

Aanbeveling 3 — Monitor de aanpak van de lidstaten inzake de beveiliging van 5G en beoordeel de impact van verschillen op de doeltreffende werking van de eengemaakte markt

De Commissie moet:

a) een transparante en consistente aanpak bevorderen met betrekking tot de behandeling door de lidstaten van de kosten van mobiele-netwerkexploitanten voor de vervanging van 5G-apparatuur die is aangekocht bij leveranciers met een hoog risico, door deze kwestie regelmatig te monitoren en daarover verslag uit te

brengen in het kader van de uitvoering van de EU-toolbox voor 5G-cyberbeveiliging;

b) beoordelen wat de gevolgen zouden zijn voor de eengemaakte markt wanneer de ene lidstaat zijn 5G-netwerken bouwt met apparatuur van een leverancier die in een andere lidstaat als leverancier met een hoog risico wordt beschouwd.

Tijdpad: december 2022

Dit verslag werd door kamer II onder leiding van mevrouw Iliana Ivanova, lid van de Rekenkamer, te Luxemburg vastgesteld op 15 december 2021.

Voor de Rekenkamer

Klaus-Heiner Lehne
President

Bijlagen

Bijlage I — Belangrijkste mogelijkheden en risico's van 5G

MOGELIJKHEDEN	RISICO'S
Ontwikkeling van nieuwe technologieën door het bedrijven	**Privacyrisico's**
Grotere mobiliteit en **modernisering** van het vervoerssysteem	**Bedreigingen** voor de nationale veiligheid
De interconnectiviteit van alledaagse fysieke voorwerpen verder **mogelijk maken**	**Afhankelijkheid** van de toeleveringsketen
Het gebruik van elektronische processen in de gezondheidszorg (e-gezondheid)**verbeteren**	**Cyberaanvallen**
De veiligheid van de burgers **verhogen**	**Negatieve effecten** op de gezondheid
De veranderingen in het mediagebruik van de samenleving **ondersteunen**	**Verlies van banen** als gevolg van efficiëntieverbeteringen
De schepping van werkgelegenheid in tal van sectoren **stimuleren** en de arbeidsmarkt **transformeren**	
De democratie **versterken**	
De digitale kloof **verkleinen**	

Bron: ERK, op basis van de Onderzoeksdienst van het Europees Parlement — European Science-Media hub.

Bijlage II — Voorbeelden van de impact van de verstoring van telecommunicatienetwerken en van cyberbeveiligingsincidenten

Storing noodnummers Frankrijk[66,67]

01 Op 3 juni 2021 konden door een netwerkstoring bij Orange, het grootste telecombedrijf van Frankrijk, gedurende een periode van enkele uren geen noodoproepen worden gedaan. Hoewel werd uitgesloten dat de storing door een cyberaanval werd veroorzaakt, laat het incident zien welke impact een verstoring van een kritieke netwerkinfrastructuur kan hebben.

Ransomware-aanvallen openbare gezondheidszorg Ierland[68,69,70]

02 In mei 2021 legde de Ierse gezondheidsdienst (de Health Service Executive) al zijn IT-systemen plat als gevolg van een ransomware-aanval. De aanval had gevolgen voor alle aspecten van de patiëntenzorg, aangezien de toegang tot patiëntendossiers werd bemoeilijkt, waardoor het risico op vertragingen en fouten toenam. Hoewel er voor zover de Ierse ambtenaren weten geen patiëntgegevens waren gecompromitteerd, had het delen van gezondheidsdossiers kunnen leiden tot allerlei soorten bijkomende misdrijven zoals fraude en chantage. Volgens de directeur-generaal van de gezondheidsdienst zullen de geraamde herstelkosten waarschijnlijk in totaal 500 miljoen EUR (600 miljoen USD) bedragen.

---

66 https://www.euronews.com/2021/06/03/french-telecom-operator-orange-apologises-after-emergency-numbers-crash-nationwide

67 https://www.reuters.com/business/media-telecom/orange-blames-network-outage-software-failure-audit-2021-06-11/

68 https://www.wsj.com/articles/irish-healthcare-service-shuts-down-it-systems-after-ransomware-attack-11620998875

69 https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

70 https://www.cert.europa.eu/cert/moreclusteredition/en/blog_DataBreachTodayinRSSSyndication-in-299786a86ffeab5aec16d55392d94819.20210624.en.html

Solarwinds[71,72,73]

03 Solarwinds is een Amerikaans bedrijf dat software ontwikkelt met behulp waarvan bedrijven en staats- en federale agentschappen hun netwerken, systemen en informatietechnologie-infrastructuur kunnen beheren. Begin 2020 was Solarwinds het doelwit van software-aanval. De hackers slaagden erin de aanvallen via software-upgrades die kwaadaardige codes bevatten naar klanten van Solarwinds te verspreiden. Hiermee werden achterdeurtjes in de platforms van de klanten geopend waardoor een gemakkelijke toegang voor aanvallen en de installatie van nog meer malware en spyware mogelijk werd.

[71] https://www.solarwinds.com/

[72] https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R

[73] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?international=true&r=US&IR=T

Bijlage III — Wettelijk en beleidskader

Europese Commissie

Europese Raad/Raad van de EU

Wetgeving

NIS-samenwerkingsgroep

2016 — NIS-richtlijn, juli 2016 — voorziet in wettelijke maatregelen om het algemene niveau van cyberbeveiliging in de EU te verhogen.

2016 — 5G-actieplan, september 2016 — beoogd wordt de invoering van 5G-diensten in alle lidstaten uiterlijk eind 2020, gevolgd door een snelle uitbouw om te zorgen voor ononderbroken 5G-dekking in stedelijke gebieden en op belangrijke transportroutes tegen 2025.

2018 — Europees wetboek voor elektronische communicatie, december 2018 — beoogd wordt een interne markt voor elektronische-communicatienetwerken en -diensten tot stand te brengen.

2019 — Conclusies van de Europese Raad, maart 2019 — hierin wordt uitgezien naar de aanbeveling van de Commissie over een gezamenlijke aanpak van de veiligheid van 5G-netwerken.

2019 — Aanbeveling inzake 5G-cyberbeveiliging, maart 2019 — hierin wordt aanbevolen dat de lidstaten de cyberbeveiligingsrisico's voor 5G-netwerken op nationaal niveau beoordelen en de nodige beveiligingsmaatregelen nemen.

2019 — Conclusies van de Raad over het belang van 5G voor de Europese economie, december 2019 — hierin wordt benadrukt dat een snelle en veilige uitrol van de 5G-netwerken essentieel is voor het verbeteren van het concurrentievermogen van de EU, en een gecoördineerde aanpak in de EU vereist.

2020 — Toolbox voor 5G-cyberbeveiliging, januari 2020 — hierin wordt een mogelijke gemeenschappelijke reeks maatregelen vastgesteld die de voornaamste cyberbeveiligingsrisico's van 5G-netwerken kunnen beperken.

2020 — Uitrol van beveiligde 5G in de EU — uitvoering van de EU-toolbox, januari 2020 — de Europese Commissie bekrachtigt de toolbox en zet haar volgende stappen uiteen (zoals een verslag over de uitvoering tegen juni 2020).

2020 — Conclusies van de Raad over het vormgeven van de digitale toekomst van Europa, juni 2020 — waarin de Raad aangeeft het ermee eens te zijn dat er moet worden gezorgd voor en uitvoering moet worden gegeven aan een gecoördineerde aanpak om de voornaamste risico's voor de uitrol van beveiligde 5G in de EU te beperken.

2020 — Conclusies van de Europese Raad, oktober 2020 — hierin wordt de toolbox voor 5G-cyberbeveiliging, en met name de noodzaak om de relevante beperkingen toe te passen op leveranciers met een hoog risico, onderschreven.

2020 — Aanbeveling betreffende (...) toegang tot 5G-radiospectrum, september 2020 — hierin worden richtsnoeren uiteengezet voor de ontwikkeling van beste praktijken voor het bevorderen van connectiviteit en het bieden van tijdige en investeringsvriendelijke toegang tot 5G-radiospectrum.

2020 — De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk, december 2020 — een "soft law"-document, waarin de prioriteiten en geplande acties van de Commissie voor cyberbeveiliging als geheel, met inbegrip van 5G-netwerken, worden uiteengezet.

2020 — Voorstel voor een NIS 2-richtlijn, december 2020 — doel is de huidige richtlijn te moderniseren en het toepassingsgebied ervan uit te breiden, waarbij ook 5G-cyberbeveiliging explicieter aan bod komt.

2020 — Voorstel voor een richtlijn betreffende de veerkracht van kritieke entiteiten, december 2020 — gericht op het aanpakken van kwetsbare punten van kritieke infrastructuur die van essentieel belang is voor de werking van de samenleving en de economie van de EU.

2020 — Digitaal kompas 2030: de Europese aanpak voor het digitale decennium, maart 2021 — hierin wordt een traject uitgestippeld naar een gemeenschappelijke visie en acties om Europa te doen slagen in het digitale decennium.

2021 — Conclusies van de Raad over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk, maart 2021 — hierin wordt steun uitgesproken voor de volgende stappen die op het gebied van de cyberbeveiliging van 5G-netwerken gezet moeten worden, zoals uiteengezet in de strategie inzake cyberbeveiliging van de Commissie.

Bijlage IV — Voorbeelden van door het EFSI gecofinancierde projecten

5G-gerelateerde EFSI-projecten

De twee EFSI-projecten die wij hebben geanalyseerd, betroffen de investeringen in onderzoek, ontwikkeling en innovatie voor de ontwikkeling van het assortiment van producten voor het 5G-netwerk. Zij omvatten de ontwikkeling van hardware en software voor zowel het radiotoegangsnetwerk als het kernnetwerk. Beide projecten droegen bij tot de uitrol van een dichter netwerk van cellen, ondersteunden de normalisatie en bevorderden belangrijke technologische experimenten.

De projecten zijn in 2018 van start gegaan en in december 2020 afgesloten. De totale investeringskosten bedroegen samen 3,9 miljard EUR, waaronder 1 miljard EUR aan EFSI-financiering.

Bijlage V — Voorbeelden van Horizon 2020- en EFRO-projecten

5G-gerelateerd Horizon 2020-project

Bij dit project, waarbij apparatuur van de drie belangrijkste 5G-leveranciers (Ericsson, Huawei en Nokia) wordt gebruikt om 5G-technologieën te testen in de grensoverschrijdende corridor die de steden Metz (Frankrijk), Merzig (Duitsland) en Luxemburg met elkaar verbindt. Het project is in november 2018 van start gegaan en zou volgens de planning 31 maanden lopen. De EU heeft 12,9 miljoen EUR toegekend voor de totale begrote kosten van 17,1 miljoen EUR.

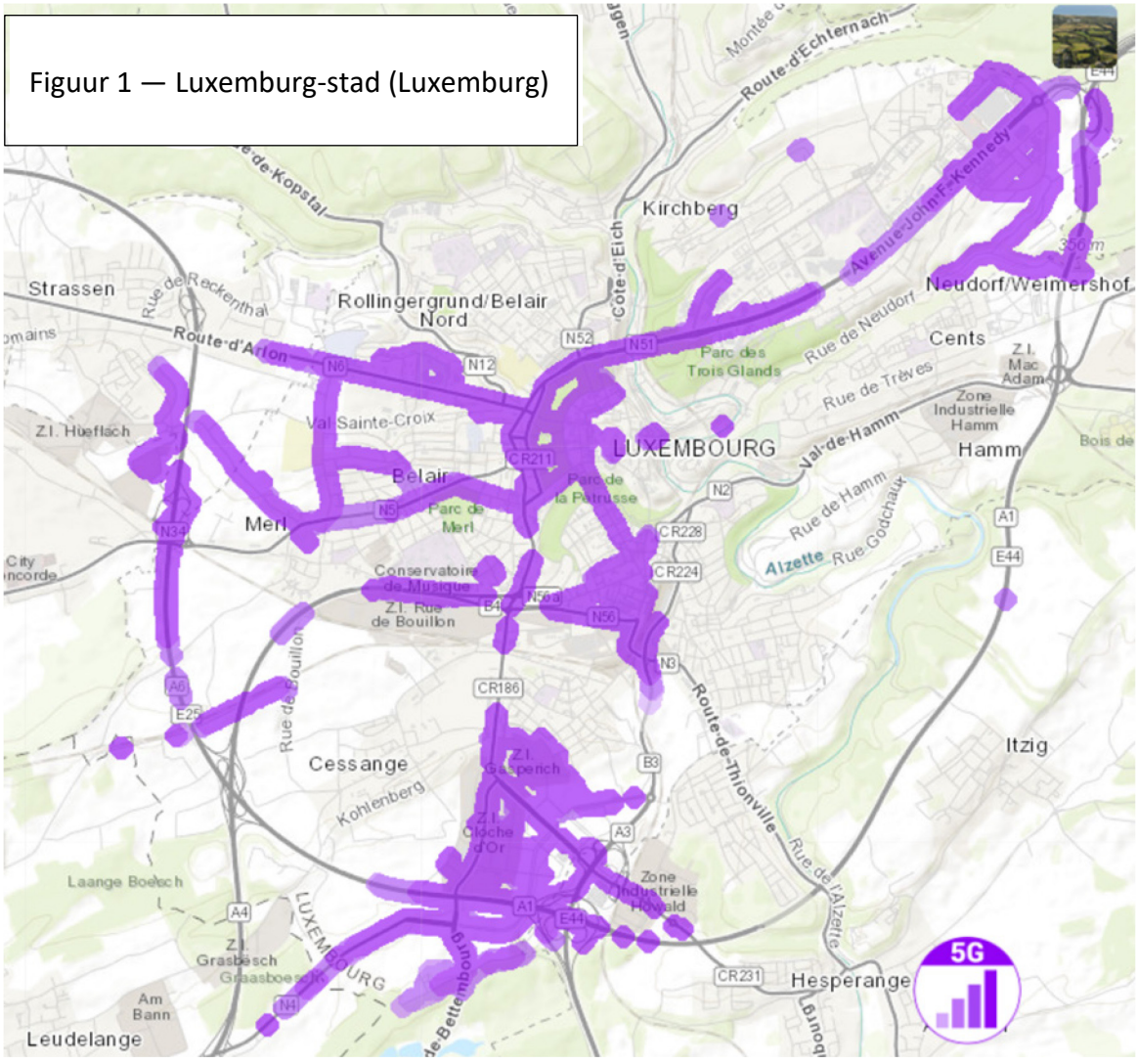
5G-gerelateerd EFRO-project

Dit project in Spanje heeft tot doel inzicht te verschaffen in 5G-netwerkimplementaties. Het doet dit onder meer door te experimenteren met netwerkbeheertechnieken die door 5G-technologie mogelijk worden gemaakt, zoals netwerkvirtualisatie, edge computing, dynamische toewijzing van netwerkdiensten, of netwerkslicing, en door use cases voor 5G te ontwikkelen. Het project is in 2019 van start gegaan en zou volgens de planning 30 maanden duren. De EU heeft 2,2 miljoen EUR van de totale verwachte kosten ten belope van 7,1 miljoen EUR bijgedragen.

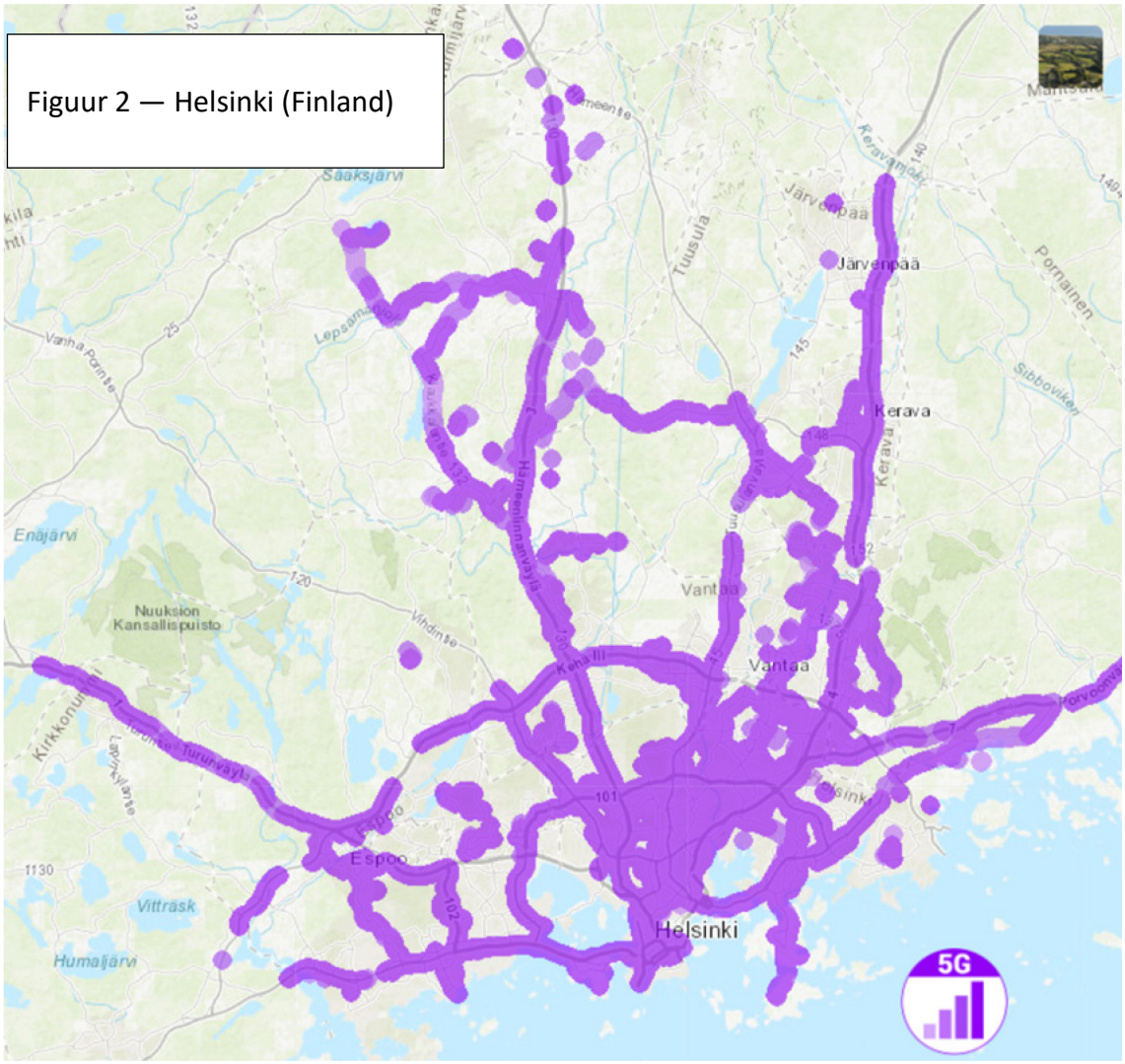
Bijlage VI — 5G-dekking in geselecteerde steden

De onderstaande cijfers zijn gebaseerd op gegevens over mobiele breedbandconnectiviteit die zijn verkregen door middel van tests die door gebruikers van de nPerf-app zijn uitgevoerd. De gebieden waar 5G is aangetroffen, zijn niet noodzakelijkerwijs commercieel opengesteld. Aangezien de netwerkprestaties afhangen van de individuele mobiele-netwerkexploitanten, geven de volgende kaarten, die op 4 oktober 2021 aan de nPerf-website zijn ontleend, alleen een beeld van de dekking, en niet van de prestaties zoals snelheid en latentietijd.

Figuur 1 — Luxemburg-stad (Luxemburg)

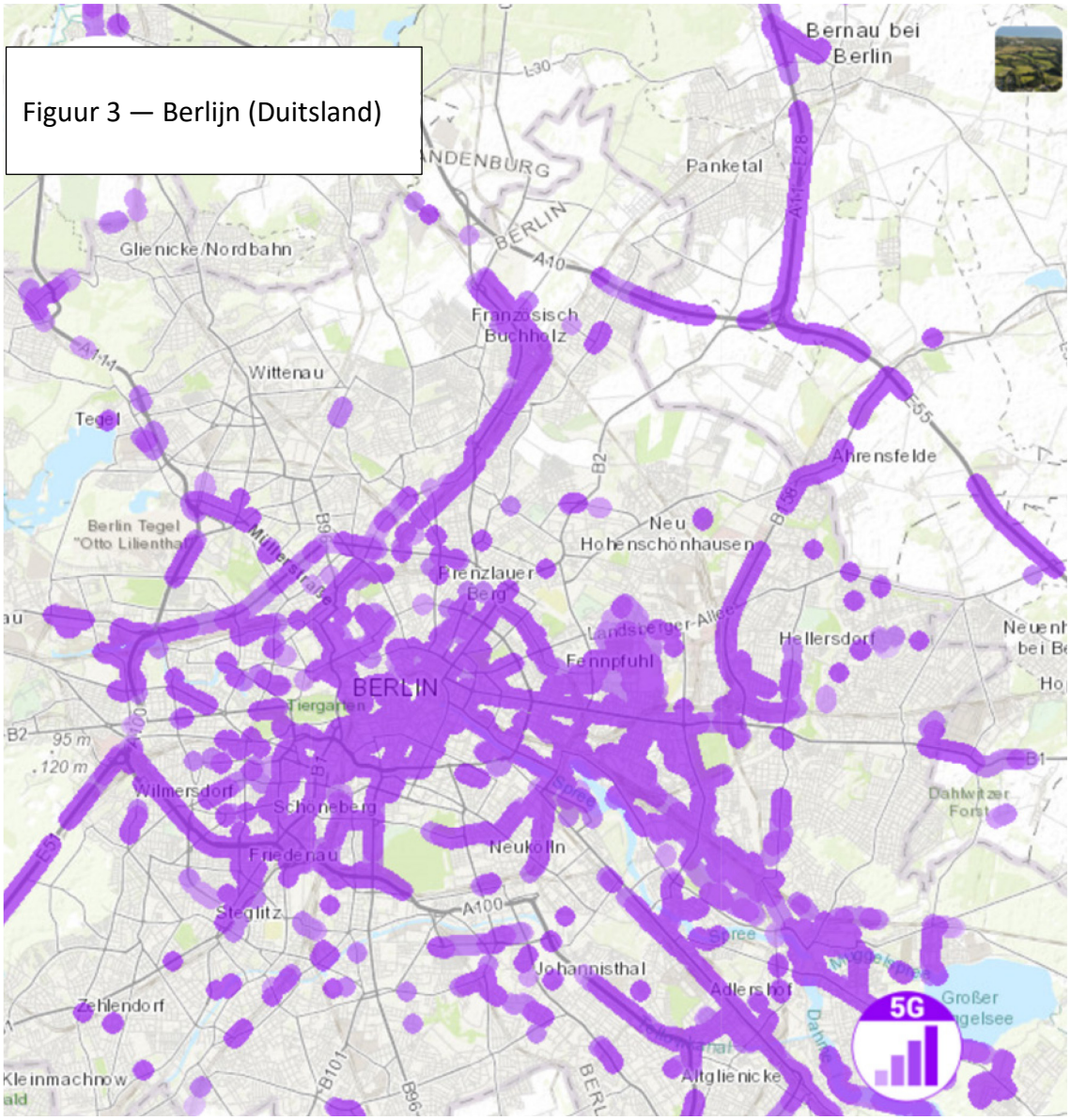


© nPerf.

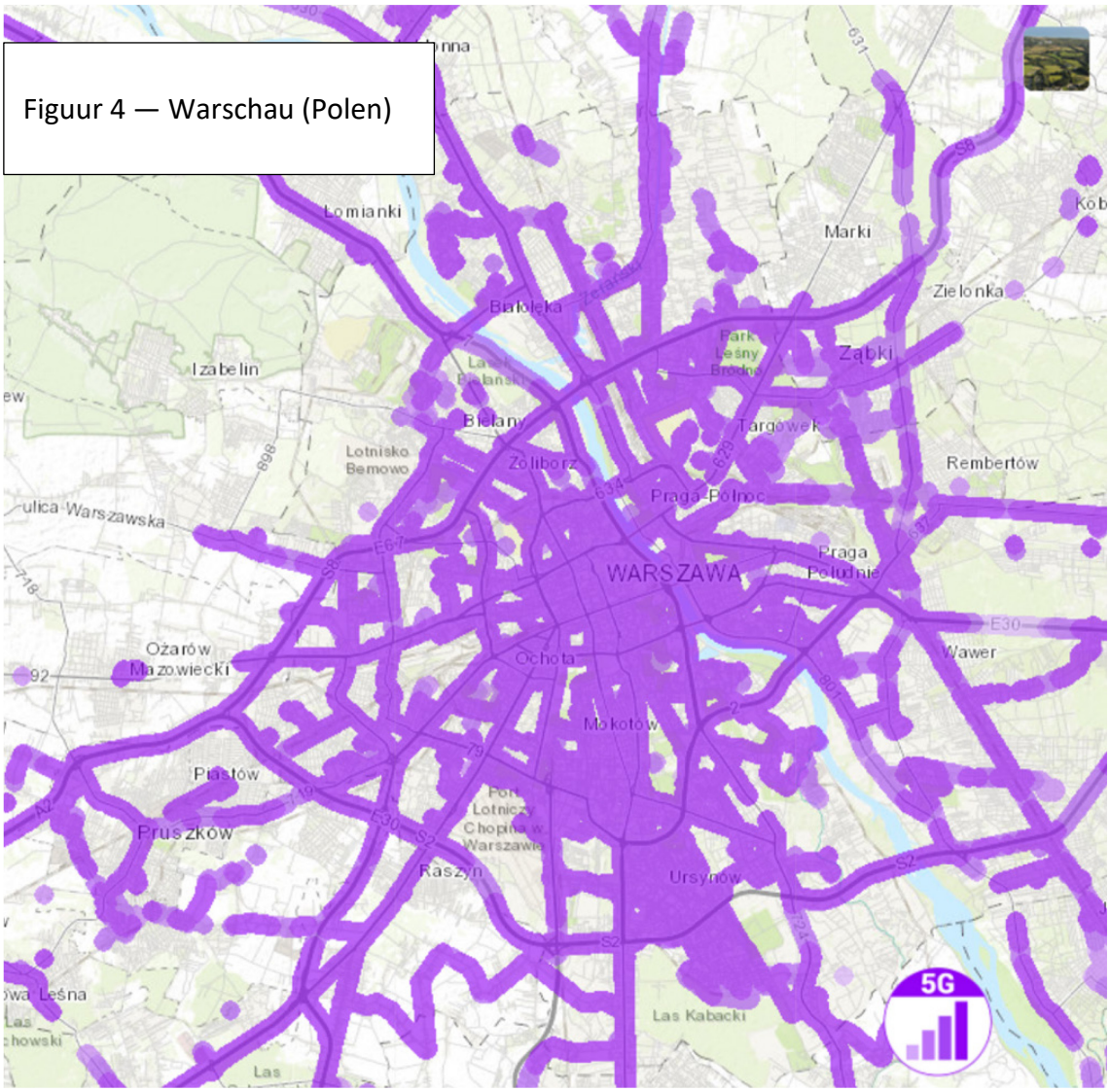


Figuur 2 — Helsinki (Finland)

© nPerf.

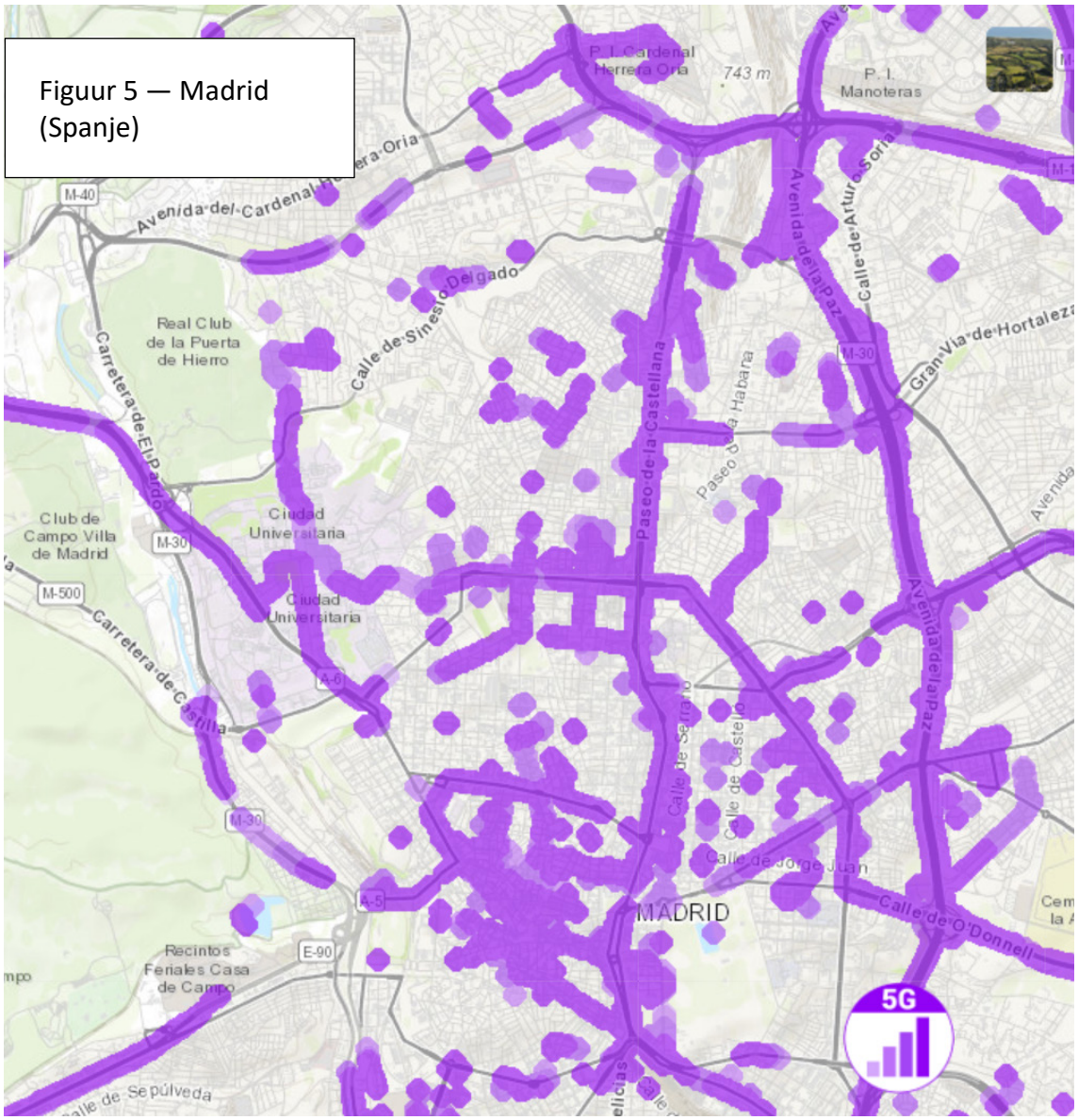


Figuur 3 — Berlijn (Duitsland)



Figuur 4 — Warschau (Polen)

© nPerf.



Figuur 5 — Madrid (Spanje)

© nPerf.

Bijlage VII — EU-toolbox voor 5G-cyberbeveiliging

De EU-toolbox voor 5G-cyberbeveiliging, die door de NIS-samenwerkingsgroep is vastgesteld en door de Commissie werd bekrachtigd, bevat drie soorten niet-bindende maatregelen (strategische, technische en ondersteunende maatregelen) die door verschillende actoren moeten uitgevoerd, zoals hieronder samengevat.

Maatregelen	Relevante actoren				
	Autoriteiten van de lidstaten	Mobiele-netwerkexploitanten	Europese Commissie	Enisa	Belanghebbenden (incl. leveranciers)
Strategische maatregelen					
SM01 — Versterking van de rol van nationale autoriteiten	✓	✓			
SM02 — Uitvoering van controles bij exploitanten en het opvragen van informatie	✓	✓			
SM03 — Beoordeling van het risicoprofiel van leveranciers en toepassing, voor essentiële voorzieningen, van beperkingen ten aanzien van leveranciers die als leveranciers met een hoog risico worden beschouwd — met inbegrip van de nodige uitsluitingen om de risico's doeltreffend te beperken	✓	✓			
SM04 — Controle van het gebruik van verleners van beheerde diensten en derdelijnsondersteuning door leveranciers van apparatuur	✓	✓			
SM05 — Waarborging van de diversiteit van leveranciers voor individuele mobiele-netwerkexploitanten door middel van passende multi-vendorstrategieën	✓	✓			
SM06 — Versterking van de veerkracht op nationaal niveau	✓	✓			
SM07 — Inventarisatie van de essentiële voorzieningen en bevordering van een divers en duurzaam 5G-ecosysteem in de EU	✓		✓		
SM08 — Behoud en opbouw van diversiteit en EU-capaciteiten in toekomstige netwerktechnologieën	✓		✓		✓

Maatregelen	Relevante actoren				
	Autoriteiten van de lidstaten	Mobiele-netwerkexploitanten	Europese Commissie	Enisa	Belanghebbenden (incl. leveranciers)
Technische maatregelen					
TM01 — Toezien op de toepassing van basisveiligheidseisen ontwerp en architectuur van veilige netwerken)	✓	✓			
TM02 — Zorgen voor en evalueren van de uitvoering van veiligheidsmaatregelen in bestaande 5G-normen	✓	✓			✓
TM03 — Zorgen voor strikte toegangscontrole	✓	✓			
TM04 — Verbetering van de veiligheid van gevirtualiseerde netwerkfuncties	✓	✓			
TM05 — Zorgen voor een veilige vorm van beheer, exploitatie en monitoring van 5G-netwerken	✓	✓			
TM06 — Versterking van de fysieke veiligheid	✓	✓			
TM07 — Versterking van de software-integriteit, -updates en het patchbeheer	✓	✓			
TM08 — Verhoging van de veiligheidsnormen in de processen van leveranciers door middel van robuuste aanbestedingsvoorwaarden	✓	✓			✓
TM09 — Gebruik van EU-certificering voor 5G-netwerkcomponenten, klantenapparatuur en/of processen van leveranciers	✓	✓	✓	✓	✓
TM10 — Gebruik van EU-certificering voor andere, niet specifiek aan 5G-gerelateerde ICT-producten en -diensten (verbonden apparaten, clouddiensten)	✓		✓	✓	✓
TM11 — Versterking van veerkracht- en continuïteitsplannen	✓	✓			✓
Ondersteunende maatregelen					
SA01 — Herziening of ontwikkeling van richtsnoeren en beste praktijken inzake netwerkbeveiliging	✓	✓		✓	
SA02 — Versterking van de test- en controlecapaciteit op nationaal en EU-niveau	✓		✓	✓	
SA03 — Ondersteuning en vormgeving van 5G-normalisatie	✓	✓	✓	✓	✓
SA04 — Ontwikkeling van richtsnoeren voor de uitvoering van veiligheidsmaatregelen in bestaande 5G-normen	✓			✓	

Maatregelen	Relevante actoren				
	Autoriteiten van de lidstaten	Mobiele-netwerkexploitanten	Europese Commissie	Enisa	Belanghebbenden (incl. leveranciers)
SA05 — Waarborging van de toepassing van gestandaardiseerde technische en organisatorische veiligheidsmaatregelen door middel van een specifieke certificeringsregeling voor de hele EU	✓			✓	✓
SA06 — Uitwisseling van beste praktijken inzake de uitvoering van strategische maatregelen, met name nationale kaders voor de beoordeling van het risicoprofiel van leveranciers	✓				
SA07 — Verbetering van de coördinatie bij de respons op incidenten en crisisbeheersing	✓			✓	
SA08 — Uitvoering van controles van onderlinge afhankelijkheid tussen 5G-netwerken en andere kritieke diensten	✓				
SA09 — Verbetering van de mechanismen voor samenwerking, coördinatie en informatiedeling	✓			✓	
SA10 — Ervoor zorgen dat bij met overheidsgeld gesteunde 5G-projecten rekening wordt gehouden met cyberbeveiligingsrisico's	✓		✓		

Bron: EU-toolbox voor 5G-cyberbeveiliging.

Acroniemen en afkortingen

Bbp: bruto binnenlands product

Berec: Orgaan van Europese regulerende instanties voor elektronische communicatie

EECC: Europees wetboek voor elektronische communicatie (European Electronic Communications Code)

EFRO: Europees Fonds voor regionale ontwikkeling

EFSI: Europees Fonds voor strategische investeringen

EIB: Europese Investeringsbank

Enisa: Agentschap van de Europese Unie voor cyberbeveiliging

NBP: nationaal breedbandplan

NIS: netwerk- en informatiesystemen

RAN: radiotoegangsnetwerk (Radio Access Network)

RRF: herstel- en veerkrachtfaciliteit (Recovery and Resilience Facility)

RSPG: Beleidsgroep radiospectrum (Radio Spectrum Policy Group)

Woordenlijst

Agentschap van de Europese Unie voor cyberbeveiliging: EU-agentschap dat is opgericht om een hoog niveau van netwerk- en informatiebeveiliging te ontwikkelen en te handhaven in alle sectoren van het particuliere en openbare leven.

Beleidsgroep radiospectrum (Radio Spectrum Policy Group): adviesgroep op hoog niveau, bestaande uit vertegenwoordigers van de lidstaten, die de EU-instellingen bijstaat en adviseert bij de ontwikkeling van de eengemaakte markt voor draadloze producten en diensten.

Breedband: snelle, gelijktijdige transmissie van meerdere informatieformaten (zoals data, spraak en video).

Europees Fonds voor strategische investeringen: investeringssteunmechanisme dat door de Europese Investeringsbank (EIB) en de Commissie is opgezet als onderdeel van het investeringsplan voor Europa om particuliere investeringen te mobiliseren voor projecten die van strategisch belang zijn voor de EU.

Exabyte: een maat voor de opslagcapaciteit van digitale informatie, gelijk aan 1 miljard gigabyte.

Global System for Mobile Communications Association (GSMA): brancheorganisatie die de belangen behartigt van mobiele exploitanten over de hele wereld, alsmede van productie- en dienstverlenende bedrijven en organisaties die belang hebben bij mobiele infrastructuur.

Internet der dingen (Internet of Things): fysieke objecten die zijn uitgerust met sensoren, software en andere technologieën waardoor zij draadloos verbinding kunnen maken en gegevens kunnen uitwisselen met andere apparaten en systemen.

Latentietijd: in computernetwerken; de tijd die nodig is voor de verplaatsing van een reeks gegevens tussen twee punten.

Mobiele-netwerkexploitant: telecommunicatiebedrijf dat draadloze spraak- en datacommunicatie aanbiedt aan geabonneerde mobieletelefoongebruikers.

Nationale breedbandplannen: documenten van de lidstaten met strategische doelstellingen voor de verwezenlijking van de breedbanddoelstellingen van de EU.

NIS-samenwerkingsgroep (NIS — netwerk- en informatiesystemen): orgaan dat is opgericht bij de NIS-richtlijn om te zorgen voor samenwerking en informatie-

uitwisseling tussen de lidstaten en dat bestaat uit vertegenwoordigers van de EU-lidstaten, de Europese Commissie en het EU-agentschap voor cyberbeveiliging.

Orgaan van Europese regelgevende instanties voor elektronische communicatie: orgaan, bestaande uit vertegenwoordigers van de nationale regelgevende autoriteiten van de lidstaten, dat deze autoriteiten en de Commissie bijstaat bij de uitvoering van het regelgevingskader van de EU met het oog op de totstandbrenging van een eengemaakte markt voor elektronische communicatie.

Radiospectrum: het deel van het elektromagnetisch spectrum dat overeenkomt met radiofrequenties.

Radiotoegangsnetwerk (Radio Access Network): een belangrijk onderdeel van de moderne telecommunicatietechnologie, waarbij afzonderlijke apparaten via radioverbindingen met andere delen van een netwerk worden verbonden.

Ransomware: malware die slachtoffers de toegang tot een computersysteem ontzegt of bestanden onleesbaar maakt, waardoor het slachtoffer gedwongen wordt losgeld te betalen om de toegang te herstellen.

Antwoorden van de Commissie

https://www.eca.europa.eu/nl/Pages/DocItem.aspx?did=60614

Tijdlijn

https://www.eca.europa.eu/nl/Pages/DocItem.aspx?did=60614

Controleteam

In de speciale verslagen van de ERK worden de resultaten van haar controles van EU-beleid en -programma's of beheersthema's met betrekking tot specifieke begrotingsterreinen uiteengezet. Bij haar selectie en opzet van deze controletaken zorgt de ERK ervoor dat deze een maximale impact hebben door rekening te houden met de risico's voor de prestaties of de naleving, de omvang van de betrokken inkomsten of uitgaven, de verwachte ontwikkelingen en de politieke en publieke belangstelling.

Deze doelmatigheidscontrole werd verricht door controlekamer II "Investeringen ten behoeve van cohesie, groei en inclusie", die onder leiding staat van ERK-lid Iliana Ivanova. De controle werd geleid door ERK-lid Annemie Turtelboom, ondersteund door Florence Fornaroli, kabinetschef, en Celil Ishik, kabinetsattaché; Niels-Erik Brokopp, hoofdmanager; Paolo Pesce, taakleider; Jussi Bright, Rafal Gorajski, Zuzana Gullová, Alexandre Tan, Aleksandar Latinov, en Nils Westphal, auditors.

Annemie Turtelboom

Florence Fornaroli

Celil Ishik

Niels-Erik Brokopp

Paolo Pesce

Jussi Bright

Rafal Gorajski

Zuzana Gullová

Aleksandar Latinov

Nils Westphal

PDF	ISBN 978-92-847-7399-2	ISSN 1977-575X	doi:10.2865/147892	QJ-AB-21-029-NL-N
HTML	ISBN 978-92-847-7391-6	ISSN 1977-575X	doi:10.2865/044294	QJ-AB-21-029-NL-Q

5G zal naar verwachting tussen 2021 en 2025 het Europese bbp met 1 biljoen EUR verhogen en zou 20 miljoen banen in alle sectoren van de economie kunnen creëren of transformeren. We constateerden dat vertragingen de verwezenlijking van de EU-doelstellingen voor de invoering van 5G in gevaar brengen en dat verdere inspanningen nodig zijn om beveiligingskwesties aan te pakken. In het verslag doen we een aantal aanbevelingen aan de Commissie ter bevordering van de tijdige en gecoördineerde implementatie van veilige 5G-netwerken in de EU.

Speciaal verslag van de ERK, uitgebracht krachtens artikel 287, lid 4, tweede alinea, VWEU.

CURIA RATIONIUM
EUROPESE REKENKAMER

Bureau voor publicaties van de Europese Unie

EUROPESE REKENKAMER
12, rue Alcide De Gasperi
L-1615 Luxemburg
LUXEMBURG

Tel. +352 4398-1

Inlichtingen: eca.europa.eu/nl/Pages/ContactForm.aspx
Website: eca.europa.eu
Twitter: @EUAuditors