DA 2022

03

Særberetning

5G-udrulningen i EU:

Udrulningen af net er forsinket, og der er stadig uafklarede sikkerhedsspørgsmål

DEN EUROPÆISKE REVISIONSRET

Indhold

Resumé

I Den "femte generation" af telekommunikationssystemer - 5G - bygger på en ny global standard for trådløs kommunikation, der har en meget højere datakapacitet og transmissionshastighed. 5G-tjenester er afgørende for en bred vifte af innovative applikationer med potentiale til at omdanne mange sektorer i vores økonomier og forbedre borgernes dagligdag. 5G har derfor strategisk betydning for hele det indre marked.

II I sin 5G-handlingsplan fra 2016 opstillede Kommissionen et mål om at sikre uafbrudt 5G-dækning i byområder og langs større transportveje senest i 2025. I marts 2021 tilføjede den et mål om, at alle befolkede områder skal være omfattet af 5G senest i 2030.

III 5G har potentiale til at skabe mange vækstmuligheder, men er også forbundet med visse risici. I sin 2019-henstilling om 5G-cybersikkerhed advarede Kommissionen om, at mange kritiske tjenesters afhængighed af 5G-nettene vil medføre særlig alvorlige konsekvenser i tilfælde af systemiske og omfattende forstyrrelser, og at de involverede truslers grænseoverskridende karakter betyder, at alle væsentligt svage punkter eller cybersikkerhedshændelser i en enkelt medlemsstat vil påvirke hele EU. Kommissionens henstilling førte bl.a. til udarbejdelsen af EU-værktøjskassen til 5G-cybersikkerhed ("værktøjskassen "), som blev vedtaget i januar 2020.

IV I hele EU kan de samlede omkostninger til 5G-udrulning nå op på 400 milliarder euro. I perioden 2014-2020 leverede EU over 4 milliarder euro i finansiering til 5G-projekter.

V Vi undersøgte, om Kommissionen effektivt støttede medlemsstaternes bestræbelser på at nå EU-målene for udrulning af 5G-net og adressere 5G-sikkerhedsbekymringer på en samordnet måde. Vi undersøgte aspekter, der vedrørte både 5G-nettenes implementering, hvor 2020 var et vigtigt år, og deres sikkerhed. Vores sigte med denne beretning er at præsentere viden og fremsætte anbefalinger om rettidig udrulning af sikre 5G-net i alle EU-lande. Vores revision fokuserede på Kommissionen, men vi undersøgte også de nationale forvaltningers og andre aktørers rolle.

VI Vores revision viste, at der er forsinkelser i medlemsstaternes udrulning af 5G-net. Ved udgangen af 2020 havde 23 medlemsstater lanceret kommercielle 5G-tjenester og nået delmålet om, at der i mindst én stor by skulle være adgang til 5G. Men ikke alle medlemsstater henviser til EU's 2025- og 2030-mål i deres nationale 5G-strategier eller bredbåndsplaner. Hertil kommer, at flere lande endnu ikke har gennemført den europæiske kodeks for elektronisk kommunikation i national ret, og at tildelingen af 5G-frekvenser er forsinket. Forsinkelserne i frekvenstildelingen har forskellige årsager: svag efterspørgsel fra mobilnetoperatørerne, problemer vedrørende koordinering med ikke-EU-lande langs de østlige grænser, covid-19's indvirkning på auktionskalenderne og usikkerhed om håndteringen af sikkerhedsspørgsmål. Medlemsstaterne er så langt bagud med hensyn til 5G-implementeringen, at EU's mål måske ikke kan nås. Kommissionen har støttet medlemsstaternes gennemførelse af 5G-handlingsplanen fra 2016 med både hard law- og soft law-initiativer, vejledning og finansiering af 5G-relateret forskning. Kommissionen har dog ikke klart defineret den kvalitet, der forventes af 5G-tjenesterne.

VII EU-værktøjskassen til 5G-cybersikkerhed angiver en række strategiske foranstaltninger, tekniske foranstaltninger og støttetiltag vedrørende håndtering af sikkerhedstrusler mod 5G-net og identificerer de relevante aktører i forbindelse med de enkelte foranstaltninger. Flere foranstaltninger adresserer spørgsmålet om højrisikoleverandører af 5G-udstyr. Denne værktøjskasse er blevet godkendt af Kommissionen og Det Europæiske Råd. Kriterierne i værktøjskassen skaber en operationel ramme, der er nyttig til på en koordineret måde at vurdere leverandørernes risikoprofil i samtlige medlemsstater. Gennemførelsen af denne vurdering forbliver dog et nationalt ansvar. Værktøjskassen blev vedtaget i en tidlig fase af 5G-udrulningen, men en række mobilnetoperatører havde allerede valgt deres leverandører. Siden værktøjskassens vedtagelse er der sket fremskridt med hensyn til at styrke sikkerheden i 5G-net, og de fleste medlemsstater anvender eller er ved at indføre restriktioner over for højrisikoleverandører. I de kommende år kan den lovgivning om 5G-sikkerhed, som medlemsstaterne har indført på grundlag af værktøjskassen, føre til mere ensartede tilgange til højrisikoleverandører af 5G-udstyr. Ingen af de foreslåede foranstaltninger er imidlertid juridisk bindende, så Kommissionen har ikke beføjelser til at kræve dem indført. Der er derfor en risiko for, at værktøjskassen ikke i sig selv kan garantere, at medlemsstaterne behandler netsikkerhedsaspekter på en samordnet måde.

VIII Kommissionen er begyndt at behandle spørgsmålet om udenlandske subsidier til 5G-leverandører og de mulige sikkerhedsmæssige konsekvenser. Kommissionen har ikke tilstrækkelige oplysninger om medlemsstaternes behandling af de potentielle udskiftningsomkostninger, der skal afholdes, hvis mobilnetoperatører er nødt til at fjerne højrisikoleverandørers udstyr i EU-net uden en overgangsperiode.

IX Vi anbefaler, at Kommissionen:

- fremmer en jævn og rettidig udrulning af 5G-net i EU
- fremmer en samordnet tilgang til 5G-sikkerhed blandt medlemsstaterne
- overvåger medlemsstaternes tilgange til 5G-sikkerhed og vurderer, hvordan forskellene påvirker det indre markeds effektive funktion.

Indledning

5G's art og betydning

01 Den "femte generation" af telekommunikationssystemer - 5G - bygger på en ny global standard for trådløs kommunikation. Sammenlignet med 3G- og 4G-net har 5G-net en meget højere datakapacitet og transmissionshastighed. 5G indeholder visse netelementer baseret på tidligere generationer af mobil og trådløs kommunikationsteknologi, men er ikke en videreudvikling af disse net. 5G giver alle brugere og tilsluttede enheder adgang til ultrahøj båndbredde og konnektivitet med lav latenstid.

02 5G vil forbinde flere enheder end nogensinde før på "tingenes internet". Det anslås, at der ved udgangen af 2018 var 22 milliarder tilsluttede enheder i brug på verdensplan. Dette tal forventes at stige til omkring 50 milliarder i 2030[1] og skabe et massivt net af indbyrdes forbundne enheder, lige fra smartphones til køkkenapparater. Det globale dataforbrug forventes at springe fra 12 exabyte mobil datatrafik pr. måned i 2017[2] til over 5 000 exabyte i 2030[3].

03 5G-tjenester er afgørende for en bred vifte af innovative applikationer med potentiale til at omdanne mange sektorer i EU's økonomi og forbedre borgernes dagligdag (jf. ***figur 1***). En undersøgelse foretaget for Kommissionen i 2017 indikerede, at der ved indførelse af 5G i fire vigtige strategiske sektorer (bilindustrien, sundhedssektoren, transportsektoren og energisektoren) kunne opnås fordele til en værdi af op til 113 milliarder euro om året[4]. Undersøgelsen angav også, at implementeringen af 5G kunne skabe 2,3 millioner job i medlemsstaterne. I en undersøgelse fra 2021 blev det anslået, at 5G mellem 2021 og 2025 ville øge det europæiske bruttonationalprodukt (BNP) i perioden med op til 1 billion euro og have

---

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", februar 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*, februar 2017.

potentiale til at skabe eller omdanne op til 20 millioner arbejdspladser i alle sektorer af økonomien[5].

Figur 1 - 5G vil dække alle aspekter af vores liv

Kilde: Europa-Kommissionen.

Sikkerhedsbekymringer

04 5G har potentiale til at skabe mange vækstmuligheder, men er også forbundet med visse risici (jf. ***bilag II***, der skitserer de væsentligste muligheder og risici i forbindelse med 5G). En af disse risici er risikoen for sikkerhedstrusler. Telekommunikationssystemer har altid kunnet udsættes for cyberangreb (jf. ***bilag II***)[6]. Men sikkerhedsspørgsmålene er særlig væsentlige med hensyn til 5G-systemet, fordi det på grund af sin teknologi og navnlig sin afhængighed af software har en større angrebsflade end 3G- og 4G-telekommunikationssystemerne[7].

---

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

[6] Analyse nr. 2/2019: "Udfordringer for en effektiv cybersikkerhedspolitik i EU" (briefingpapir); Kontaktkomitéens 2020-revisionskompendium om cybersikkerhed; Europa-Parlamentets Forskningstjeneste - European Science-Media hub.

[7] NIS-samarbejdsgruppen, "EU coordinated risk assessment of the cybersecurity of 5G networks", 9.10.2019. punkt 3.4.

05 Eftersom 5G-net forventes at blive rygraden i en bred vifte af tjenester og applikationer, vil tilgængeligheden af disse net blive en stor sikkerhedsmæssig udfordring på nationalt plan og EU-plan. Hvis hackere trængte ind i et 5G-net, kunne de angribe dets centrale funktioner med det formål at forstyrre tjenester eller få kontrol over kritisk infrastruktur (f.eks. elnet), som i EU ofte har en grænseoverskridende dimension. I undersøgelser anslås det, at den økonomiske effekt af cyberkriminalitet kan beløbe sig til så meget som 5 000 milliarder euro om året, dvs. over 6 % af det globale BNP i 2020[8]

06 En anden 5G-sikkerhedsudfordring består i, at et begrænset antal leverandører spiller en afgørende rolle i forbindelse med opbygning og drift af 5G-net. Dette øger eksponeringen for en potentiel forsyningsafbrydelse ved afhængighed af en enkelt leverandør - navnlig hvis leverandøren udgør en høj risiko, f.eks. hvis vedkommende udsættes for indgriben fra et tredjeland. I 2019 påpegede samarbejdsgruppen for net- og informationssystemer (NIS-samarbejdsgruppen) - der består af repræsentanter for medlemsstaterne og for EU-organer - at der var en risiko for, at fjendtlige statslige aktører kunne skaffe sig et let adgangspunkt til et 5G-net ved privilegeret adgang, ved at lægge pres på en leverandør eller ved at påberåbe sig nationale retlige krav[9] (jf. ***tekstboks 1***). Det var på denne baggrund, EU begyndte at udvikle initiativer vedrørende 5G-sikkerhed.

---

[8] World Economic Forum, "Wild Wide Web - Consequences of Digital Fragmentation", 2021.

[9] NIS-samarbejdsgruppen, "EU coordinated risk assessment of the cybersecurity of 5G networks", 9.10.2019.

Tekstboks 1

Sikkerhedsbekymringer vedrørende 5G-samarbejdet mellem EU og Kina

- I 2015 undertegnede EU og Kina en fælles erklæring om strategisk 5G-samarbejde, som omfatter forpligtelser til gensidighed og åbenhed for så vidt angår adgang til finansiering af forskning i 5G-net og markedsadgang[10].
- I 2017 vedtog Kina en national efterretningslov, som fastsætter, at alle kinesiske organisationer og borgere skal samarbejde med de nationale efterretningstjenester under strenge krav om hemmeligholdelse[11]. Som reaktion traf USA i 2018 foranstaltninger til at begrænse de aktiviteter, der udøves af flere kinesiske virksomheder - bl.a. Huawei, som er en af de vigtigste 5G-leverandører.

I marts 2019 gav Europa-Parlamentet udtryk for bekymring over, at kinesiske 5G-leverandører kan udgøre en sikkerhedsrisiko for EU som følge af lovgivningen i deres oprindelsesland.

07 Der kan potentielt også forekomme trusler mod fortroligheden og privatlivets fred, da teleoperatører ofte outsourcer deres data til datacentre. Der er en risiko for, at sådanne data lagres på 5G-leverandørers udstyr, som befinder sig i ikke-EU-lande med andre niveauer af retlig beskyttelse og databeskyttelse end i EU.

5G-initiativer på EU-plan

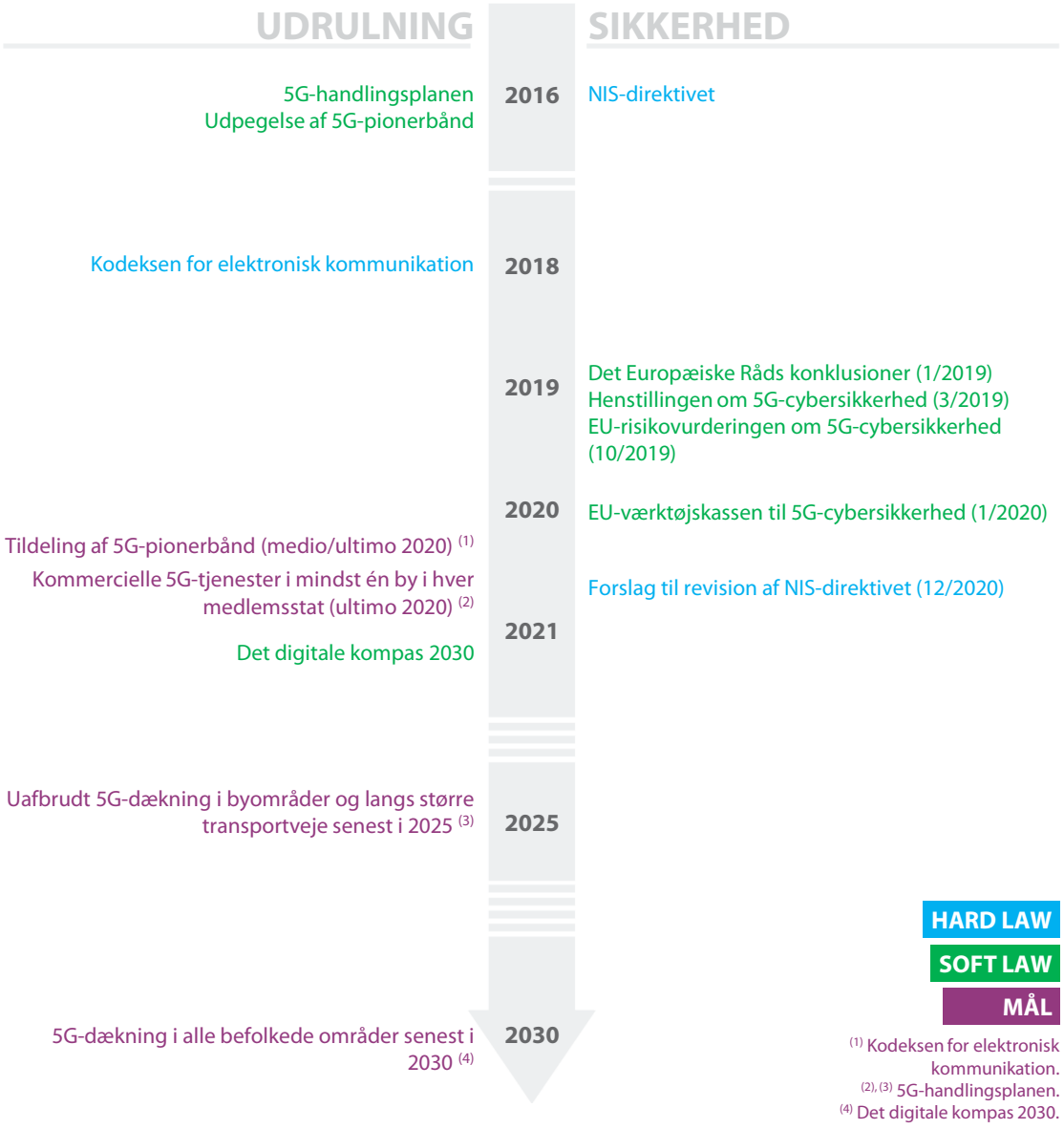
08 Den politiske ramme for 5G og 5G-sikkerhed består af både "hard law", der er juridisk bindende og kan håndhæves (f.eks. forordninger), og ikkebindende "soft law" (f.eks. meddelelser fra Kommissionen). I ***bilag III*** præsenteres den retlige og politiske ramme. I ***figur 2*** vises de væsentligste politikdokumenter og de vigtigste mål.

---

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

[11] Europa-Parlamentets beslutning af 12. marts 2019; Folkerepublikken Kinas nationale efterretningslov, artikel 14. Loven kan ses i engelsk oversættelse på https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

Figur 2 - De væsentligste politikdokumenter og de vigtigste mål vedrørende 5G-udrulning og -sikkerhed



Kilde: Revisionsretten.

Roller og ansvarsområder

09 Mens mobilnetoperatører er ansvarlige for en sikker 5G-udrulning ved anvendelse af udstyr fra teknologileverandører, og medlemsstaterne er ansvarlige for den nationale sikkerhed, er 5G-netsikkerheden et spørgsmål af strategisk betydning for hele det indre marked og EU's teknologiske suverænitet[12]. For så vidt angår de tekniske og sikkerhedsmæssige aspekter ved 5G-net støtter og koordinerer Kommissionen og en række EU-agenturer derfor medlemsstaternes indsats.

10 I ***tabel 1*** er de vigtigste roller og ansvarsområder i forbindelse med 5G-net angivet nærmere.

Tabel 1 - Roller og ansvarsområder

	Kommissionen og EU-agenturer	Medlems-staternes myndigheder	Mobilnet-operatører og 5G-leverandører
Tildeling af 5G-pionerbånd		✓	
Fastlæggelse af EU's 5G-politik	✓	✓	
Udrulning af 5G-net			✓
Investeringer og finansiering	✓	✓	✓
National sikkerhed		✓	
Sikkerhed i 5G-net		✓	✓
Støtte til og koordinering af medlemsstaternes indsats	✓		

Kilde: Revisionsretten.

Omkostningerne til 5G-udrulning og EU's relaterede finansielle støtte

De samlede omkostninger til 5G-udrulning i samtlige medlemsstater kan nå op på 400 milliarder euro

11 I 2021 er de samlede omkostninger til 5G-udrulning i samtlige EU-medlemsstater frem til 2025 blevet anslået til mellem 281 og 391 milliarder euro, fordelt ligeligt på anlæggelse af ny 5G-infrastruktur og opgradering af fast infrastruktur til

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

gigabithastigheder[13]. Størstedelen af disse investeringer skal finansieres af mobilnetoperatørerne.

I perioden 2014-2020 støttede EU 5G-udviklingen med over 4 milliarder euro

12 I perioden 2014-2020 støttede EU 5G-udviklingen med over 4 milliarder euro, både direkte over EU-budgettet og indirekte med finansiering via Den Europæiske Investeringsbank (EIB). EU-budgettet finansierede projekter, der udelukkende vedrørte forskning, mens EIB-finansieringen støttede både forskning og udrulning.

13 EIB har været den største kilde til EU-finansiering af 5G-relaterede projekter. Pr. august 2021 havde EIB ydet lån på i alt 2,5 milliarder euro til ni 5G-projekter i fem medlemsstater[14]. Desuden blev der i perioden 2014-2020 stillet 1,9 milliarder euro til rådighed over EU-budgettet. ***Tabel 2*** giver en oversigt over de største kilder til EU's finansielle støtte til 5G.

Tabel 2 - EU-finansiering af 5G (2014-2020)

EU-finansiering	Beløb
EIB	2,485 milliarder euro[1]
Den Europæiske Fond for Strategiske Investeringer (EFSI)	1 milliard euro[2]
Horisont 2020	755 millioner euro[3]
EFRU	Mindst 147 millioner euro[4]

1) EIB-projektliste.
2) EFSI-projektliste.
3) Horisont 2020-dashboard.
4) Datasæt for projekter medfinansieret af EFRU under den flerårige finansielle ramme for 2014-2020.

Kilde: Revisionsretten.

[13] Kommissionens skøn, baseret på data fra EIB, Analysys, GSMA og virksomhedsmeddelelser samt på ETNO - European Telecommunications, Connectivity & Beyond: *How Telcos Can Accelerate a Digital Future for All*, marts 2021.

[14] EIB-projektliste.

14 EFSI (som forvaltes af EIB) støttede to projekter, der havde til formål at opnå større tæthed i udrulningen af celler og støtte standardisering. Disse projekters samlede investeringsomkostninger var på 3,9 milliarder euro, hvoraf 1 milliard euro kom fra EFSI (jf. ***bilag IV***).

15 Siden 2014 har Kommissionen også direkte medfinansieret mere end 100 5G-projekter via Horisont 2020 og i mindre omfang via EFRU. ***Bilag V*** indeholder eksempler på sådanne projekter.

Genopretnings- og resiliensfaciliteten vil levere yderligere EU-finansiering til 5G-udrulningen i de kommende år

16 Genopretnings- og resiliensfaciliteten vil være en supplerende kilde til finansiering af 5G-udrulningen i de kommende år. Pr. september 2021 havde 16 medlemsstater planer om at finansiere 5G-udrulning med midler fra faciliteten, mens 10 havde besluttet ikke at gøre det. Der forelå endnu ikke oplysninger fra den sidste medlemsstat.

Revisionens omfang og revisionsmetoden

17 Ved denne revision vurderede vi, om Kommissionen effektivt støtter medlemsstaterne med hensyn til:

- at opfylde EU's 2025- og 2030-mål for udrulning af 5G-net
- at adressere 5G-sikkerhedsbekymringer på en samordnet måde.

På begge disse områder undersøgte vi også medlemsstaternes foranstaltninger og aktiviteter.

18 Med begrebet "5G-sikkerhed" henviser vi til cybersikkerhed og sikkerhed i forbindelse med hardware/software. Vi undersøgte både 5G-nettenes sikkerhed og deres implementering, hvor 2020 var et vigtigt år (jf. ***figur 2***). Vores sigte med denne beretning er at præsentere viden og fremsætte anbefalinger om rettidig udrulning af sikre 5G-net i EU.

19 Vores revision dækkede perioden fra 2016 til maj 2021. Vi inkluderede yderligere ajourførte oplysninger så vidt muligt. Vores revisionsarbejde omfattede følgende:

- Vi gennemgik EU-lovgivning, initiativer fra Kommissionen og anden relevant dokumentation.
- Vi interviewede repræsentanter for Kommissionen, EIB, Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), Den Europæiske Unions Agentur for Cybersikkerhed (ENISA), telekommunikationssammenslutninger, mobilnetoperatører, 5G-leverandører, internationale organisationer og myndigheder i Finland, Tyskland, Polen og Spanien samt eksperter på området for at indsamle viden. Vores kriterier for udvælgelsen af medlemsstater var bl.a. de afsatte EU-midler til 5G-projekter, landenes udrulningsstatus og hensynet til en geografisk balance.
- Vi sendte et spørgeskema til alle EU's 27 nationale telemyndigheder for at få et bredere perspektiv på 5G-udfordringerne i medlemsstaterne.
- Vi gennemgik ti 5G-relaterede projekter medfinansieret af EU (under EFSI, EFRU og Horisont 2020), som vi udvalgte til illustrative formål.

20 Vi trak også på vores nylige analyse af EU's reaktion på Kinas statsdrevne investeringsstrategi[15] samt på andre beretninger om f.eks. bredbånd[16], initiativet til digitalisering af EU's industri[17] og EU's cybersikkerhedspolitik[18].

[15] Analyse nr. 3/2020 "EU's reaktion på Kinas statsdrevne investeringsstrategi".

[16] Særberetning nr. 12/2018 "Bredbånd i EU's medlemsstater: På trods af fremskridt vil ikke alle Europa 2020-målene blive nået".

[17] Særberetning nr. 19/2020 "Digitalisering af EU's industri: Et ambitiøst initiativ, hvis succes afhænger af et vedvarende engagement fra EU, myndigheder og virksomheder".

[18] Analyse nr. 2/2019 "Udfordringer for en effektiv cybersikkerhedspolitik i EU" (briefingpapir).

Bemærkninger

Forsinkelserne i udrulningen af 5G-net betyder, at EU's 2025- og 2030-mål måske ikke kan nås

21 Med hensyn til rettidig udrulning af 5G-net undersøgte vi:

- om medlemsstaternes 5G-udrulning går planmæssigt
- om Kommissionen har ydet medlemsstaterne passende støtte
- om medlemsstaterne har fjernet væsentlige hindringer for en hurtig udrulning af 5G-net.

Medlemsstaterne er bagud med 5G-implementeringen

Kommissionen fastsatte frister for udrulningen af 5G-net i sin 5G-handlingsplan fra 2016

22 I sin 5G-handlingsplan fra 2016 foreslog Kommissionen frister for udrulningen af 5G-net i EU: Medlemsstaterne skulle lancere tidlige 5G-net inden udgangen af 2018, lancere fuldt ud kommercielle 5G-tjenester i mindst én stor by inden udgangen af 2020 og sikre uafbrudt 5G-dækning i byområder og langs større transportveje senest i 2025.

23 I marts 2021 tilføjede Kommissionen et mål om, at alle befolkede områder skal være omfattet af 5G senest i 2030[19].

23 medlemsstater lancerede kommercielle 5G-tjenester inden udgangen af 2020

24 Ved udgangen af 2020 havde 23 medlemsstater nået målet om, at der i mindst én stor by skulle være adgang til 5G-tjenester. Kun Cypern, Litauen, Malta og Portugal havde ikke opfyldt dette mål. Ved udgangen af oktober 2021 var det kun Litauen og Portugal, der stadig ikke havde 5G-tjenester i nogen af deres store byer.

---

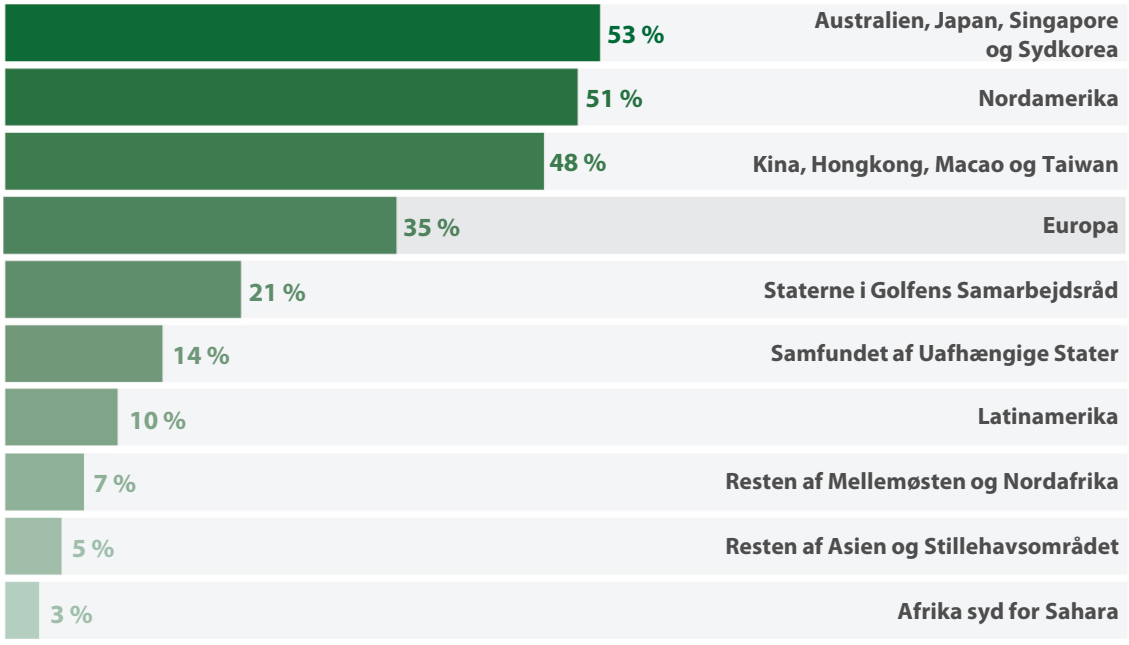
[19] Europa-Kommissionen, Det digitale kompas 2030: Europas kurs i det digitale årti, COM(2021) 118 final.

Der er en risiko for, at de fleste medlemsstater ikke kan holde fristerne i 2025 og 2030

25 Ifølge en nylig undersøgelse fra Kommissionen er det kun sandsynligt, at 11 medlemsstater opnår uafbrudt 5G-dækning i alle byområder og langs større landtransportveje senest i 2025[20]. Kommissionen vurderer, at sandsynligheden for at nå dette mål i de resterende 16 medlemsstater er enten mellemhøj (Østrig, Tjekkiet, Estland, Tyskland, Irland, Polen, Litauen og Slovenien) eller lav (Belgien, Bulgarien, Kroatien, Cypern og Grækenland).

26 I 2021 bemærkede brancheorganisationen Global System for Mobile Communications Association (GSMA), at 5G-udrulningen har et andet tempo i EU end i andre dele af verden. Den vurderede f.eks., at 51 % af alle mobilforbindelser i Nordamerika vil være 5G-baserede i 2025, mens det tilsvarende tal for Europa (inklusive lande uden for EU) kun er 35 % (jf. ***figur 3***).

Figur 3 - 5G-forbindelser som andel af de samlede mobilforbindelser i 2025



Kilde: GSMA. *The Mobile Economy 2021*.

[20] Undersøgelse af de nationale bredbåndsplaner i EU-27.

27 Med det nuværende udrulningstempo er der en høj risiko for, at 2025-fristen - og dermed også 2030-fristen for dækning af alle befolkede områder - vil blive overskredet af de fleste medlemsstater. På denne baggrund undersøgte vi, om Kommissionen effektivt har støttet medlemsstaternes bestræbelser på at nå EU's 2025- og 2030-mål for udrulning af 5G-net.

En række svagheder i Kommissionens støtte til medlemsstaterne

Kommissionen definerede ikke den forventede servicekvalitet i 5G-nettene

28 Kommissionen har indtil videre ikke defineret den forventede servicekvalitet i 5G-nettene, f.eks. med hensyn til minimumshastighed og maksimal latenstid. Hertil kommer, at Kommissionen i handlingsplanen fra 2016 opfordrede medlemsstaterne til at lancere "fuldt ud kommercielle" 5G-tjenester i Europa inden udgangen af 2020 uden at definere disse kvalitetsrelaterede begreber.

29 Denne mangel på klarhed om den forventede servicekvalitet skaber risiko for, at medlemsstaterne fortolker begreberne forskelligt. Vi bemærkede eksempler på forskellige tilgange til 5G-udrulning i medlemsstaterne (jf. ***tekstboks 2***).

Tekstboks 2

Eksempler på forskellige tilgange til 5G-udrulning

Hastighed og latenstid er to centrale præstationsaspekter for tjenester, der anvender 5G. Eksempelvis kræver fjernkirurgi og industriel automatisering via 5G meget høj hastighed og lav latenstid. Indtil videre er der imidlertid kun to medlemsstater (Tyskland og Grækenland), der har fastsat krav vedrørende minimumshastighed og maksimal latenstid[21].

Kravet om, at der i mindst én stor by skulle være adgang til 5G-tjenester inden udgangen af 2020, er blevet fortolket forskelligt af medlemsstaterne. Det har ført til en situation, hvor betegnelsen "byer med adgang til 5G-tjenester" spænder fra byer med dækning af nogle få gader, f.eks. Luxembourg, til byer med dækning af næsten hele byområdet, f.eks. Helsinki. I ***bilag VI*** beskrives dækningen i udvalgte byer.

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

30 Hvis denne situation fortsætter, kan den føre til uligheder i adgangen til og kvaliteten af 5G-tjenester i EU (en "digital kløft"): Mennesker i nogle dele af EU vil have bedre 5G-adgang og bedre 5G-tjenester end andre. Denne digitale kløft kan også påvirke potentialet for økonomisk udvikling, da 5G kun kan revolutionere sektorer som sundhedspleje, uddannelse og arbejdsmarked, hvis 5G-tjenesternes præstationer er gode nok.

31 Klarhed om 5G-nettets forventede præstationer er også nødvendig i lyset af Kommissionens initiativ vedrørende øget gennemsigtighed med hensyn til kvaliteten af mobilnetoperatørernes roamingtjenester, som Kommissionen for nylig har fremsat et lovgivningsforslag om[22].

Kommissionens kvartalsrapportering om 5G-udrulningen er ikke altid pålidelig

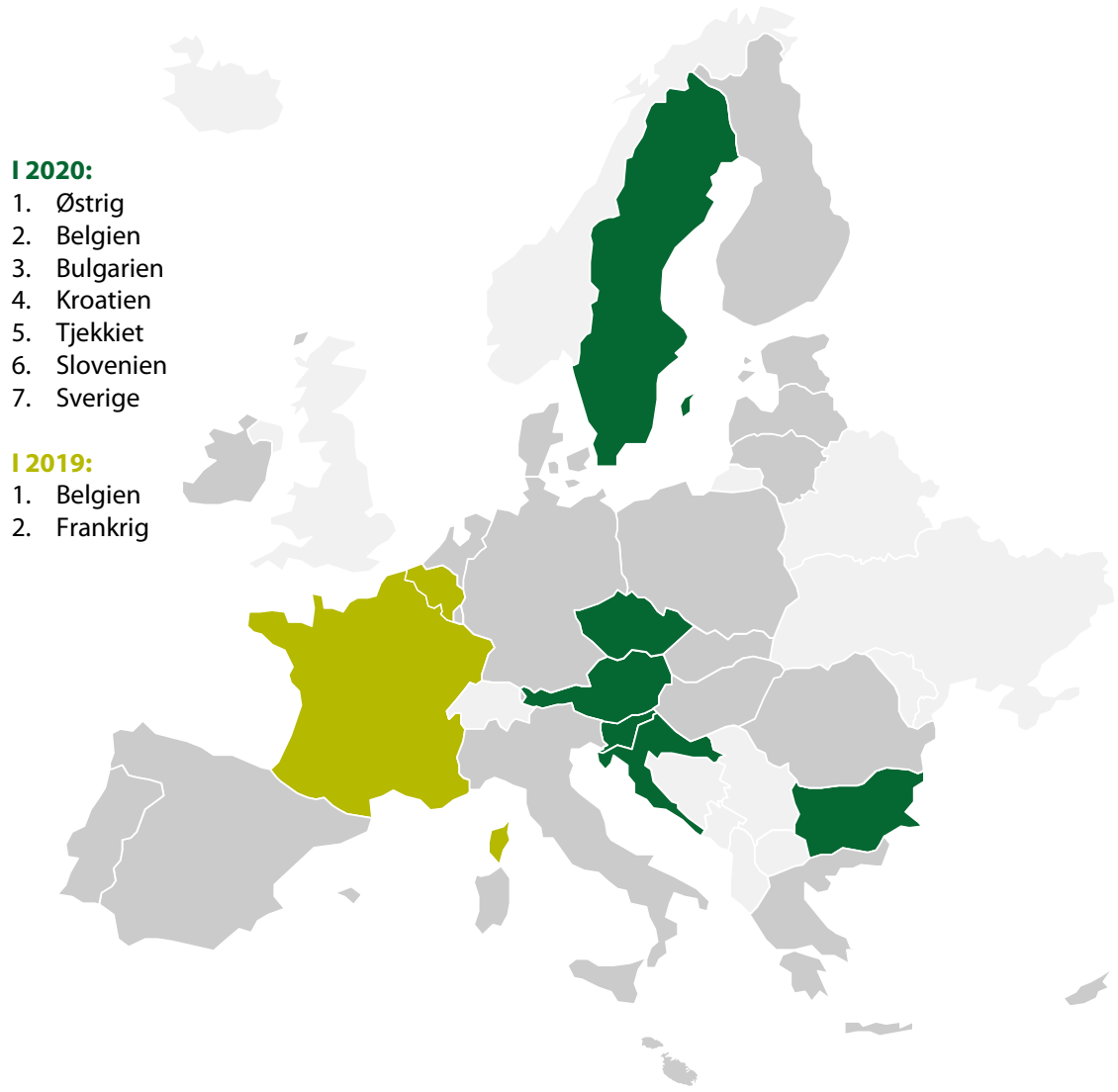
32 Kommissionen overvåger 5G-udrulningen i medlemsstaterne via det såkaldte 5G-observatorium. Observatoriet giver på kvartalsbasis oplysninger om 5G-udrulningen og om medlemsstaternes 5G-strategier. Vi konstaterede imidlertid med hensyn til to af de fire undersøgte lande, at oplysningerne i disse rapporter ikke altid var pålidelige. Kvartalsrapport nr. 10 for kvartalet frem til udgangen af december 2020 angav f.eks. et meget lavere antal finske kommuner med 5G end det faktiske antal (40 i stedet for 70) og indeholdt ingen oplysninger om, at 5G-frekvensauktionerne i Polen var blevet udsat (jf. punkt ***42***).

Kommissionen har først for nylig gjort brug af det europæiske semester til at overvåge medlemsstaternes fremskridt med udrulning af 5G-net

33 Vi konstaterede, at Kommissionen i de seneste to har gjort mere brug af det europæiske semester med henblik på at tilskynde medlemsstaterne til at gøre fremskridt med udrulning af 5G-net. Der blev fremsat landespecifikke henstillinger med direkte 5G-relevans til to medlemsstater i 2019, men dette steg til syv medlemsstater i 2020 (jf. ***figur 4***).

[22] Europa-Kommissionen, Forslag til forordning om roaming på offentlige mobilkommunikationsnet i Unionen(omarbejdning), COM(2021) 85 final af 24.2.2021.

Figur 4 - Landespecifikke henstillinger vedrørende 5G



Kilde: Revisionsretten, baseret på landespecifikke henstillinger.

Medlemsstaterne mangler stadig at fjerne væsentlige hindringer for en hurtig udrulning af 5G-net

34 For at kunne nå EU's 2025- og 2030-mål vedrørende 5G skal medlemsstaterne have lagt tre vigtige byggesten: en strategisk byggesten ved sikring af, at deres nationale 5G-strategier eller nationale bredbåndsplaner afspejler disse mål[23], en lovgivningsmæssig byggesten ved gennemførelse af den europæiske kodeks for elektronisk kommunikation fra 2018 (EECC)[24] og en forretningsorienteret byggesten ved tildeling af frekvenser[25]. ***Tabel 3*** giver et overblik over medlemsstaternes fremskridt med hensyn til disse tre elementer.

[23] Kommissionens undersøgelse af de nationale bredbåndsplaner i EU-27.

[24] Direktiv (EU) 2018/1972 om oprettelse af en europæisk kodeks for elektronisk kommunikation.

[25] Meddelelse fra Kommissionen: En EU-værktøjskasse til udrulning af sikre 5G-net i EU, COM(2020) 50 final.

Tabel 3 - Status for byggestenene vedrørende 2025-målene

Medlemsstat	National bredbåndsplan på linje med 2025-målene	EECC-gennemførelse	5G-pionerbånd (august 2021)			Sandsynlighed for at nå målene
			700 MHz	3,6 GHz	26 GHz	
Belgien				Midlertidig anvendelse		lav
Bulgarien		✓		✓		lav
Tjekkiet	✓	✓	✓	✓		mellemhøj
Danmark		✓	✓	✓	✓	høj
Tyskland	✓	✓	✓	✓	✓	mellemhøj
Estland						mellemhøj
Irland				✓		mellemhøj
Grækenland	✓	✓	✓	✓	✓	lav
Spanien	✓		✓	✓		høj
Frankrig	✓	✓	✓	✓		høj
Kroatien			✓	✓	✓	lav
Italien			✓	✓	✓	høj
Cypern	✓		✓	✓		lav
Litauen	✓					mellemhøj
Letland				✓		høj
Luxembourg			✓	✓		høj
Ungarn	✓	✓	✓	✓		høj
Malta		✓				mellemhøj
Nederlandene	✓		✓			mellemhøj
Østrig	✓	✓	✓	✓		mellemhøj
Polen	✓					mellemhøj
Portugal				Midlertidig anvendelse		mellemhøj
Rumænien						høj
Slovenien	✓		✓	✓	✓	mellemhøj
Slovakiet			✓			høj
Finland	✓	✓	✓	✓	✓	høj
Sverige	✓		✓	✓		høj

Kilde: Kommissionens undersøgelse af de nationale bredbåndsplaner i EU-27, 5G-observatoriet og Frekvenspolitikgruppen.

Kun få medlemsstater har medtaget udrulningsmålene for 2025 og 2030 i deres nationale 5G-strategier

35 Medlemsstaterne fastlægger deres 5G-politik ved udarbejdelse af dedikerede nationale 5G-strategier eller ved ajourføring af deres eksisterende nationale bredbåndsplaner. Kommissionen bemærker i sin 2021-undersøgelse af de nationale bredbåndsplaner[26], at kun 14 medlemsstater har medtaget EU's mål om uafbrudt 5G-dækning i alle byområder og langs større landtransportveje senest i 2025 i deres nationale 5G-strategier eller ajourførte bredbåndsplaner (jf. ***tabel 3***). Medtagelse af dette mål er afgørende for at støtte en vellykket gennemførelse af politikken.

De fleste medlemsstater havde ikke gennemført EECC-direktivet ved udgangen af 2020

36 EECC-direktivet - der fastlægger de nationale tilsynsmyndigheders og andre kompetente myndigheders opgaver og fastsætter frister for tildeling af 5G-pionerbånd - skulle gennemføres af medlemsstaterne senest den 21. december 2020. Ved udgangen af februar 2021 havde kun tre medlemsstater (Finland, Grækenland og Ungarn) meddelt, at de havde vedtaget alle de nødvendige foranstaltninger til gennemførelse af direktivet. Kommissionen indledte derfor traktatbrudssager mod de resterende 24 medlemsstater[27].

37 Ved udgangen af november 2021 verserede 23 traktatbrudssager stadig. Kommissionen forventer snart at afslutte traktatbrudssagerne mod seks medlemsstater (Østrig, Bulgarien, Tjekkiet, Frankrig, Tyskland og Malta), men den kan blive nødt til at indbringe sagerne mod de andre 17 medlemsstater for Domstolen[28] (jf. ***tabel 3***).

---

[26] Undersøgelse af de nationale bredbåndsplaner i EU-27.

[27] Kommissionens pressemeddelelse IP/21/206 af 4.2.2021.

[28] Kommissionens pressemeddelelse IP/21/4612 af 23.9.2021.

Tildelingen af 5G-pionerbånd er forsinket

38 I 2016 identificerede Kommissionen og medlemsstaterne tre pionerbånd til 5G-tjenester:

- 700 Mhz-frekvensbåndet, der gør det lettere for trådløse signaler at trænge ind i bygninger og giver operatører mulighed for at tilbyde en bredere dækning (hundredvis af kvadratkilometer). Med hensyn til hastighed og latenstid giver 5G-nettet dog her kun et beskedent fremskridt i forhold til 4G (fra 150 til 250 megabit pr. sekund).

- Mellemfrekvensbåndet ved 3,6 Ghz, der kan bære betydelige datamængder (op til 900 megabit pr. sekund) over betydelige afstande (radius på flere kilometer).

- Højfrekvensbåndet ved 26 Ghz, der kan give høje hastigheder på mellem 1 og 3 gigabit pr. sekund over korte afstande (dvs. under 2 km), men med en højere følsomhed over for interferens.

39 Medlemsstaterne skulle stille lavfrekvensbåndet til rådighed senest den 30. juni 2020[29] og herefter stille mellem- og højfrekvensbåndene til rådighed senest den 31. december 2020[30]. Ved udgangen af 2020 havde medlemsstaterne imidlertid tildelt under 40 % af de samlede pionerbånd (jf. ***tabel 4***):

- 700 MHz-båndet var tildelt i 13 medlemsstater.

- 3,6 GHz-båndet var tildelt i 17 medlemsstater (herunder to medlemsstater, der havde givet tilladelse til midlertidig anvendelse).

- 26 GHz-båndet var tildelt i fire medlemsstater.

Ved udgangen af oktober 2021 var tildelingssatsen steget til 53 %[31].

---

[29] Afgørelse (EU) 2017/899 om anvendelsen af 470-790 MHz-frekvensbåndet.

[30] Direktiv (EU) 2018/1972 om oprettelse af en europæisk kodeks for elektronisk kommunikation.

[31] 5G-observatoriet og Frekvenspolitikgruppen.

Tabel 4 - Status for tildelingen af 5G-pionerbånd, december 2020

Medlemsstat	700 MHZ	3,6 GHZ	26 GHZ
Belgien		Midlertidig anvendelse	
Bulgarien			
Tjekkiet	✓	✓	
Danmark	✓	✓	✓
Tyskland	✓	✓	✓
Estland			
Irland		✓	
Grækenland	✓	✓	✓
Spanien		✓	
Frankrig	✓	✓	
Kroatien			
Italien		✓	✓
Cypern	✓	✓	
Letland		✓	
Litauen			
Luxembourg	✓	✓	
Ungarn	✓	✓	
Malta			
Nederlandene	✓		
Østrig	✓	✓	
Polen			
Portugal		Midlertidig anvendelse	
Rumænien			
Slovenien			
Slovakiet	✓	✓	
Finland	✓	✓	✓
Sverige	✓	✓	

Kilde: 5G-observatoriet og Frekvenspolitikgruppen.

Forsinkelser i tildelingen af pionerbånd har forskellige årsager

40 Vi konstaterede, at forsinkelserne i tildelingen af 26 GHz-båndet hovedsagelig skyldes svag efterspørgsel fra mobilnetoperatørerne. F.eks. er i alt 1,5 GHz af 26 GHz-båndet til rådighed til 5G-brug i Spanien. Det er imidlertid endnu ikke blevet tildelt operatører, fordi der ifølge en offentlig høring, som blev afsluttet i juli 2019, ikke er nogen efterspørgsel. Der er planlagt en ny offentlig høring i slutningen af 2021 med henblik på en frekvensauktion i andet kvartal af 2022. Også mobilnetoperatører i Finland bemærkede, at der endnu ikke er nogen væsentlig interesse eller business case for 26 GHz-båndet.

41 Problemer vedrørende koordinering med ikke-EU-lande langs de østlige grænser (Belarus, Rusland og Ukraine) har også bidraget til forsinkelser i tildelingen af 5G-frekvenser. I henhold til gældende internationale aftaler anvender disse ikke-EU-lande 700 MHz-båndet til TV-transmission og 3,6 GHz-båndet til militære satellittjenester. Dette problem vedrører hovedsagelig de baltiske lande (Estland, Letland og Litauen) og Polen. Ifølge Kommissionen er der sket fremskridt med hensyn til Ukraine og Belarus, som forventes at frigive 700 MHz-båndet inden udgangen af 2022. Der er endnu ikke gjort fremskridt i de bilaterale forhandlinger med Rusland. I lyset af denne situation har Estland og Polen anmodet om en udsættelse af fristerne for tildeling af 700 MHz-båndet til medio 2022.

42 Desuden blev 5G-frekvensauktioner i Polen og Spanien udsat under covid-19-pandemien (jf. ***tekstboks 3***).

Tekstboks 3

Eksempler på forsinkelser i 5G-frekvenstildelingen forårsaget af covid-19

- I marts 2020 annoncerede Polen en auktion om 3,6 GHz-båndet med henblik på tildeling senest den 30. juni 2020. Efter pandemiens udbrud besluttede de polske myndigheder at suspendere alle administrative procedurer i hele pandemiens varighed. I september 2021 var auktionsprocessen vedrørende dette bånd endnu ikke afsluttet.

- I Spanien var den oprindelige plan at afholde auktion om 700 MHz-båndet i marts 2020. Ifølge de spanske myndigheder forsinkede covid-19-pandemien imidlertid frigivelsen af dette bånd, der blev anvendt til digitalt tv. Auktionen blev udsat til maj 2020 og derefter til første kvartal af 2021. Efter en ændring af den spanske lovgivning i april 2021 for at tilpasse licensernes varighed til EECC blev auktionen flyttet til sommeren 2021, og frekvenserne på 700 MHz-båndet blev endelig tildelt i juli 2021.

43 Yderligere grunde til den forsinkede tildeling af 5G-pionerbåndene er, at medlemsstaterne har forskellige tilgange til 5G-sikkerhed, og at deres vedtagelse af 5G-sikkerhedslove er forsinket, hvilket skaber usikkerhed for erhvervslivet (jf. punkt ***74*** og ***75***):

- I Spanien indeholdt pionerbåndsauktionsreglerne en generel klausul om, at indehavere af offentlige koncessioner skal overholde alle de krav vedrørende sikkerheden i 5G-net, der i fremtiden måtte blive fastsat i EU-regler eller spanske regler. Den spanske mobilnetoperatør, vi interviewede, følte sig tvunget af denne klausul til at træffe beslutninger om strategier og indkøb på usikre vilkår. Virksomheden påpegede også, at de nationale myndigheder var uvillige til at præcisere visse centrale betingelser såsom muligheden for kompensation, hvis den fremtidige lovgivning, der efter planen skal vedtages inden udgangen af 2022, kræver udskiftning af udstyr.

- I Polen var en af grundene til at udsætte tildelingen af 5G-frekvenser behovet for at afvente en lov, der præciserer sikkerhedskravene til 5G-net.

Der er behov for en yderligere indsats for at håndtere sikkerhedsspørgsmål vedrørende 5G-udrulning

44 Med hensyn til 5G-sikkerhedsaspekterne undersøgte vi:

- om Kommissionen har taget de nødvendige skridt til at fremme udarbejdelse af en forsvarlig sikkerhedsramme og ydet passende støtte til medlemsstaterne

- om medlemsstaterne implementerer sikre 5G-net på en samordnet måde ved anvendelse af de risikobegrænsende foranstaltninger i EU's værktøjskasse til cybersikkerhed i 5G-net (værktøjskassen) og ajourfører deres lovgivning.

Kommissionen reagerede hurtigt, da 5G-sikkerhed blev et væsentligt bekymringspunkt på EU-plan

45 5G-handlingsplanen fra 2016 omhandler ikke sikkerhedsforhold. Sikkerheden i 5G-net og risikoen for overdreven afhængighed af leverandører fra tredjelande, navnlig Kina, blev identificeret som et kritisk spørgsmål i marts 2019. Europa-Parlamentet gav i sin beslutning af 12. marts 2019[32] udtryk for bekymring over, at ikke-EU-leverandører af 5G-udstyr kan udgøre en sikkerhedsrisiko for EU som følge af

[32] Europa-Parlamentets beslutning af 12. marts 2019 (2019/2575 (RSP)).

lovgivningen i deres oprindelseslande. Samme dag fremhævede Kommissionen i sin meddelelse om forbindelserne mellem EU og Kina i et strategisk perspektiv, at det er nødvendigt med en fælles EU-tilgang til sikkerheden i forbindelse med 5G-nettet for at beskytte kritisk digital infrastruktur mod potentielle alvorlige sikkerhedsmæssige konsekvenser[33]. Det Europæiske Råd anmodede i sine konklusioner af 21. og 22. marts 2019 Kommissionen om at udstede en henstilling om en fælles tilgang til 5G-nets sikkerhed[34].

46 Nogle dage senere udsendte Kommissionen en sådan henstilling med en række foranstaltninger både på nationalt plan (f.eks. 5G-risikovurderinger) og på EU-plan (f.eks. en koordineret risikovurdering), der skulle sikre et højt cybersikkerhedsniveau for 5G-net i hele EU[35].

47 Næsten alle medlemsstater havde afsluttet deres nationale risikovurderinger inden fristen i juli 2019[36]. NIS-samarbejdsgruppen udsendte i oktober 2019 en rapport om EU's koordinerede risikovurdering af cybersikkerheden i 5G-net og i januar 2020 EU-værktøjskassen til 5G-cybersikkerhed[37] (jf. ***bilag VII***). Den blev hurtigt godkendt af Kommissionen og Det Europæiske Råd[38].

---

[33] JOIN(2019) 5 final af 12.3.2019 - Forbindelserne mellem EU og Kina i et strategisk perspektiv.

[34] Det Europæiske Råds konklusioner af 21. og 22. marts 2019.

[35] Kommissionens henstilling (EU) 2019/534 af 26. marts 2019 - Cybersikkerheden i forbindelse med 5G-net.

[36] Pressemeddelelse af 19. juli 2019.

[37] *Cybersikkerhed i 5G-net - EU-værktøjskasse med risikobegrænsende foranstaltninger*, NIS-samarbejdsgruppen, 1/2020.

[38] Meddelelse fra Kommissionen: En EU-værktøjskasse til udrulning af sikre 5G-net i EU, COM(2020) 50 final og Det Europæiske Råds konklusioner af 1. og 2. oktober 2020 (EUCO 13/20).

5G-værktøjskassen til 5G-cybersikkerhed fra 2020 indførte for første gang foranstaltninger til håndtering af sikkerhedstrusler på EU-plan, men var ikke præskriptiv

Hvis sikkerheden i 5G-net betragtes som hørende under den nationale sikkerhedskompetence, begrænser det Kommissionens handlemuligheder

48 EU-traktaterne[39] fastlægger anvendelsesområdet for EU-tiltag til tackling af udfordringer som dem, der vedrører udrulning af sikre 5G-net. Anvendelsesområdet er bredt og giver Kommissionen og medlemsstaterne en vis fortolkningsmargin (jf. ***tekstboks 4***).

Tekstboks 4

EU-kompetencer vedrørende 5G-net: Delt kompetence eller et spørgsmål om national sikkerhed?

I princippet hører 5G-net under EU's kompetence vedrørende det indre marked (en delt kompetence), både som en tjeneste (leveret af mobilnetoperatører) og som en vare (selve det 5G-udstyr, mobilnetoperatører køber med henblik på at opbygge deres 5G-net). Under denne delte kompetence kan EU (Kommissionen og andre EU-institutioner) vedtage juridisk bindende foranstaltninger (lovgivning) for at sikre det indre marked og fremme dets funktion. Sikkerheden i 5G-net kan også betragtes mere bredt som relateret til EU's område med frihed, sikkerhed og retfærdighed. I så fald skal sikkerhed forstås som et generelt begreb vedrørende forebyggelse og bekæmpelse af kriminalitet, og dermed hører det under endnu en delt kompetence, der giver EU mulighed for at vedtage juridisk bindende foranstaltninger.

Sikkerhed kan imidlertid også fortolkes mere snævert, så begrebet kun vedrører trusler mod medlemsstaternes nationale sikkerhed. Hvis sikkerheden i 5G-net således hører under en national enekompetence, har EU kun beføjelser til at støtte medlemsstaternes nationale indsats for at garantere sikkerheden i deres 5G-net.

[39] Traktaten om Den Europæiske Unions funktionsmåde.

49 Spørgsmålet om sikkerhed i 5G-net går på tværs af medlemsstaternes og EU's kompetencer og berører den nationale sikkerhed. Kommissionen betragtede sikkerheden i 5G-net som relateret til trusler mod medlemsstaternes nationale sikkerhed og valgte derfor soft law-foranstaltninger. Den valgte tilgang betyder, at EU ikke kan vedtage juridisk bindende foranstaltninger, der tvinger medlemsstaterne til at anvende ensartede risikobegrænsende tiltag, og ikke kan indføre krav, som det er muligt at håndhæve. I stedet kan Kommissionen udsende ikkebindende henstillinger og meddelelser, bidrage til at udbrede bedste praksis og koordinere medlemsstaternes nationale foranstaltninger. Men en anden tilgang er mulig. Et eksempel på dette er NIS-direktivet[40], som er en EU-retsakt, der beskæftiger sig med sikkerheden i net- og informationssystemer i hele Unionen. Denne retsakt blev foreslået af Kommissionen og vedtaget i henhold til retsgrundlaget for det indre marked, selv om cybersikkerhed i vid udstrækning er et nationalt anliggende[41].

EU-værktøjskassen til 5G-cybersikkerhed blev vedtaget i en tidlig fase af udrulningen, men en række mobilnetoperatører havde allerede valgt deres leverandører

50 I januar 2020 vedtog NIS-samarbejdsgruppen en EU-værktøjskasse til 5G-cybersikkerhed, som angiver en række strategiske foranstaltninger, tekniske foranstaltninger og støttetiltag vedrørende håndtering af sikkerhedstrusler mod 5G-net og identificerer de relevante aktører i forbindelse med de enkelte foranstaltninger. Denne værktøjskasse, som er godkendt af Kommissionen og Det Europæiske Råd, blev først vedtaget ni måneder efter, at Europa-Parlamentet og Rådet første gang havde givet udtryk for bekymring vedrørende 5G-sikkerheden. I den nye europæiske strategi for fremme af intelligente, rene og sikre forbindelser i digitale systemer i hele verden omtales EU-værktøjskassen til 5G-cybersikkerhed som et retningsgivende værktøj for investeringer i digital infrastruktur[42]. Kommissionens soft law-tilgang bidrog til hurtig iværksættelse af foranstaltninger til håndtering af sikkerhedstrusler, også på EU-plan, og til at fremme samarbejde mellem medlemsstaterne om dette grænseoverskridende emne. Til sammenligning gik der med hensyn til NIS-direktivet mere end tre år fra

---

[40] Direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

[41] Analyse nr. 02/2019 "Udfordringer for en effektiv cybersikkerhedspolitik i EU" (briefingpapir), punkt 36.

[42] Fælles meddelelse til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg, Regionsudvalget og Den Europæiske Investeringsbank - Global Gateway. JOIN(2021) 30 final af 1.12.2021.

Kommissionens forslag[43] til direktivets vedtagelse[44], og i forbindelse med EECC-direktivet gik der over to år[45]. Herefter gik der endnu mere tid med at gennemføre direktiverne i medlemsstaternes nationale ret (jf. også punkt ***36*** og ***37***).

51 EU-værktøjskassen til 5G-cybersikkerhed blev først vedtaget fire år efter fremlæggelsen af 5G-politikken i 5G-handlingsplanen, dvs. det år hvor handlingsplanens delmål for udrulning skulle være opfyldt. I lyset af dette mente de repræsentanter for medlemsstaternes ministerier, nationale tilsynsmyndigheder og mobilnetoperatører, der blev interviewet i forbindelse med denne revision, at foranstaltningerne vedrørende 5G-sikkerhedsaspekterne blev iværksat for sent.

52 Værktøjskassen blev endvidere offentliggjort, da 5G-udrulningen og -planerne i de fleste medlemsstater stadig befandt sig i en tidlig fase. De fleste kontrakter mellem 5G-leverandører og -operatører blev indgået i 2020 og 2021. Ifølge ETNO (European Telecommunications Network Operators' Association) havde en række mobilnetoperatører dog allerede valgt deres leverandører, da EU-værktøjskassen til 5G-cybersikkerhed blev fremlagt.

EU-værktøjskassen til 5G-cybersikkerhed skabte en ramme for vurdering af leverandørernes risikoprofil, men der var stadig svagheder

Nogle medlemsstater og nationale myndigheder mener, at en del af de kriterier, der anvendes til at klassificere leverandører som højrisikoleverandører, ikke er klare nok

53 Et centralt element i EU-værktøjskassen til 5G-cybersikkerhed er, at medlemsstaterne skal vurdere leverandørerne og med hensyn til vigtige aktiver, der defineres som kritiske, anvende restriktioner over for leverandører, der er klassificeret som højrisikoleverandører. Medlemsstaternes vurdering skal foretages på grundlag af en ikkeudtømmende liste over kriterier, der er taget fra EU's koordinerede risikovurdering. Som eksempler på sådanne kriterier kan nævnes:

- sandsynligheden for, at leverandøren udsættes for indgriben fra et tredjeland, f.eks. via en stærk forbindelse mellem leverandøren og et tredjelands regering eller via tredjelandets lovgivning, navnlig hvis der ikke findes nogen

[43] COM(2013) 48 final af 7.2.2013.

[44] Direktiv (EU) 2016/1148.

[45] COM(2016) 590 final/2 af 12.10.2016 og Direktiv (EU) 2018/1972 om oprettelse af en europæisk kodeks for elektronisk kommunikation.

lovgivningsmæssig eller demokratisk kontrol eller domstolsprøvelse, eller hvis der ikke findes aftaler om sikkerhed eller databeskyttelse mellem EU og tredjelandet

- leverandørens evne til at sikre leveringen
- den generelle kvalitet af leverandørens produkter og cybersikkerhedspraksis.

54 Værktøjskassen er blevet udviklet for at undgå fragmentering og fremme ensartethed på det indre marked. Kriterierne i værktøjskassen skaber en operationel ramme, der er nyttig til på en koordineret måde at vurdere leverandørernes risikoprofil i samtlige medlemsstater. Den gjorde det også muligt for Kommissionen sammen med medlemsstaterne at reagere hurtigt på nye 5G-sikkerhedsbekymringer. Det er dog fortsat de nationale myndigheders ansvar at anvende disse kriterier ved vurderingen af de risici, der er forbundet med specifikke leverandører. Under hensyntagen til denne ramme havde 13 medlemsstater i oktober 2021 vedtaget eller ændret lovgivning om 5G-sikkerhed (jf. punkt ***75*** og ***figur 6***).

55 Repræsentanterne for to af de fire nationale ministerier, vi interviewede i forbindelse med denne revision, mente dog, at nogle af disse kriterier for klassificering af 5G-leverandører er åbne for fortolkning og bør præciseres yderligere. De mente også, at Kommissionen bør give yderligere støtte og vejledning vedrørende klassificering af højrisikoleverandører. De interviewede repræsentanter for medlemsstaterne angav også, at denne situation skaber en risiko for, at medlemsstaterne anvender forskellige tilgange vedrørende højrisikoleverandører (jf. også punkt ***74*** og ***75*** samt ***tekstboks 5***). Elleve af de nationale tilsynsmyndigheder, der besvarede vores spørgeundersøgelse, og som i forskellig grad er involveret i 5G-sikkerhed, gav udtryk for lignede bekymringer.

5G-leverandørernes oprindelsesland har betydning for vurderingen af sikkerhedsrisiciene

56 5G-leverandørerne er forskellige som virksomheder og har hjemsted i lande med forskellige forbindelser til EU. ***Figur 5*** viser nogle fællestræk og forskelle mellem de vigtigste 5G-leverandører og deres oprindelseslande, navnlig på de områder, som er nævnt i værktøjskassen, og som sandsynligvis vil påvirke vurderingen af leverandørernes risikoprofil (jf. punkt ***53***).

Figur 5 - Fællestræk og forskelle mellem 5G-leverandører og deres oprindelseslande

Kilde: Revisionsretten, baseret på WTO-medlemmer; OECD-medlemmer; OECD's indeks for FDI-restriktioner; Verdensbanken, "Worldwide Governance Indicators Dataset", 2019; Det Verdensøkonomiske Forum, "Global Competitiveness Dataset", 2018; afgørelser om tilstrækkelighed; Statista, "Who is leading the 5G patent race?"; Ericsson, virksomhedsdata; Nokia, virksomhedsdata; Qualcomm, virksomhedsdata; Sharp, virksomhedsdata; LG, virksomhedsdata; Samsung, virksomhedsdata; Huawei, virksomhedsdata; ZTE, virksomhedsdata. Vekselkurser pr. 31.12.2020.

57 Én risikofaktor er, i hvilket omfang en leverandørs oprindelsesland overholder EU's politiske og økonomiske kerneværdier. Landespecifikke faktorer såsom retsstatsforhold, domstolenes uafhængighed, åbenheden over for udenlandske investeringer og eksistensen af databeskyttelsesaftaler kan tages som udtryk for en virksomheds retlige beskyttelse mod statslig indgriben og for den retlige beskyttelse, som virksomheden kan tilbyde sine kunder.

58 De leverandører, der er etableret i EU-medlemsstater, er forpligtet til at overholde EU's standarder og retlige krav, men dette gælder ikke seks af de store leverandører, som har hjemsted i ikke-EU-lande og opererer inden for rammerne af disse landes lovgivning (jf. ***figur 5***). En sådan lovgivning kan adskille sig meget fra EU's standarder, f.eks. med hensyn til beskyttelsen af borgernes data og effektiviteten af denne beskyttelse eller mere generelt med hensyn til, hvordan domstolenes uafhængighed er sikret ved hjælp af lovgivningsmæssige og/eller demokratiske kontrolforanstaltninger. Hvad angår domstolenes uafhængighed scorer USA og Japan højere end andre oprindelseslande for 5G-leverandører uden for EU, mens det er Sydkorea, der scorer højest blandt ikke-EU-landene, når det gælder retsstatsforhold.

59 5G-net er i overvejende grad softwaredrevne. Det forhold, at nogle leverandører opererer inden for rammerne af ikke-EU-landes lovgivning, kan give anledning til særlige bekymringer i de tilfælde, hvor kontrolcentrene for denne type software også er placeret uden for EU, og EU-borgere dermed potentielt underlægges lovgivning uden for EU.

60 Kommissionen er begyndt at adressere disse bekymringer og har den holdning, at alle virksomheder, der leverer tjenester til EU-borgere, skal acceptere og respektere EU's regler og værdier[46]. Den har indledt dialog med flere lande for at sikre en stærk beskyttelse af privatlivets fred og af personoplysninger[47]. ***Figur 5*** viser også, at Kommissionen allerede har anerkendt tilstrækkeligheden af Japans (og førhen USA's) databeskyttelsesordninger. Det bør dog bemærkes, at afgørelser om tilstrækkelighed kan anfægtes og er underlagt streng retslig kontrol. Eksempelvis fastslog Domstolen i 2015, at det dagældende retlige instrument for dataudveksling med USA, Safe Harbor-ordningen, var ugyldigt[48], og i 2020 fastslog den, at Privacy Shield - som havde afløst

---

[46] Meddelelse fra Kommissionen: Europas digitale fremtid i støbeskeen, COM(2020) 67 final.

[47] Forbindelserne mellem EU og Kina i et strategisk perspektiv.

[48] Dom i sag C-362/14 og https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117da.pdf

Safe Harbor-aftalen - ikke gav EU-borgere tilstrækkelig beskyttelse[49]. På nuværende tidspunkt er der derfor ingen afgørelser om tilstrækkelighed for så vidt angår USA. Mere generelt og i tillæg til eksistensen af en databeskyttelsesordning er det nødvendigt at tage højde for den bredere retlige og institutionelle ramme, herunder f.eks. overholdelsen af retsstatsprincippet og den måde, hvorpå domstolenes uafhængighed sikres.

61 ***Figur 5*** viser også en betydelig variation mellem 5G-leverandørernes andel af 5G-patenterne, deres indtægter og deres medarbejderantal. Dette har betydning for deres disponible ressourcer, hvilket igen har betydning for deres modstandsdygtighed og evne til at sikre en fortsat levering. F.eks. er Samsung og Huawei de leverandører, der har de største andele af 5G-patenterne, genererer de højeste indtægter som selskaber og har de højeste antal ansatte samlet set.

62 En anden væsentlig risikofaktor, der i henhold til værktøjskassen har betydning for en leverandørs risikoprofil, er sandsynligheden for, at leverandøren udsættes for indgriben fra regeringen i et tredjeland. Ejerskabsforholdene spiller en vigtig rolle i denne forbindelse, da ejere med et stort antal aktier kan være i stand til at udøve pres eller påvirke ledelsesbeslutninger. Endvidere anses virksomheder under privat eller statsligt ejerskab for at være mindre åbne for offentlig kontrol - dvs. revisioner og ansvarlighedsordninger - end aktieselskaber, som er underlagt strenge oplysningskrav i hele regnskabsåret af hensyn til almindelige investorer og tilsynsmyndigheder. De fleste 5G-leverandører er børsnoteret enten i deres oprindelsesland eller i udlandet, mens de kinesiske leverandører er sværere at klassificere og generelt opfattes som tæt knyttet til den kinesiske regering[50].

---

[49] Dom i sag C-311/18 og https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091da.pdf

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

Ifølge medlemsstaterne var Kommissionens og ENISA's støtte nyttig i forbindelse med implementeringen af EU-værktøjskassen til 5G-cybersikkerhed

63 Kommissionen støttede medlemsstaterne gennem udveksling af bedste praksis vedrørende væsentlige foranstaltninger i EU-værktøjskassen til 5G-cybersikkerhed, herunder vedrørende højrisikoleverandører. Denne støtte, der ofte blev ydet via NIS-samarbejdsgruppen, blev suppleret med specifikke ENISA-aktiviteter såsom afholdelse af webinarer og udsendelse af vejledning om:

- implementeringen af værktøjskassen med fokus på de tekniske foranstaltninger
- bedste praksis vedrørende netsikkerhed, især:
  - 5G-trusselsbilleder[51]
  - udarbejdelse af nationale 5G-risikovurderinger
  - sikkerhedsforanstaltninger under EECC[52], herunder særlige retningslinjer om 5G-sikkerhed[53].

64 Kommissionen gav også ENISA til opgave at udarbejde EU's cybersikkerhedscertificeringsordning for 5G-net, som skal lette håndteringen af risici vedrørende nettenes tekniske sårbarheder og forbedre cybersikkerheden yderligere[54]. Denne certificering kan bidrage til at forbedre sikkerheden, men den kan ikke forhindre, at trusler indføres i systemerne via softwareopdateringer.

65 Alle de repræsentanter for medlemsstaternes myndigheder, vi interviewede i forbindelse med denne revision, fremhævede, at Kommissionens og ENISA's støtte havde været nyttig i forbindelse med implementeringen af EU-værktøjskassen til 5G-sikkerhed. Desuden oplyste de fleste af de nationale telemyndigheder (15 ud af 21), at Kommissionen og/eller ENISA havde støttet de nationale myndigheders udveksling af bedste praksis vedrørende gennemførelsen af de væsentligste strategiske foranstaltninger.

---

[51] ENISA, "Threat Landscape for 5G Networks", 14.12.2020.

[52] ENISA, "Guideline on Security Measures under the EECC", 10.12.2020.

[53] ENISA, "5G supplement to the Guidelines on Security Measures under the EECC", 7.7.2021.

[54] Pressemeddelelse af 3. februar 2021.

EU-værktøjskassen til 5G-cybersikkerhed blev vedtaget for sent til, at den kunne anvendes i forbindelse med EU-medfinansierede projekter i perioden 2014-2020

66 Et af målene med EU's værktøjskasse til 5G-cybersikkerhed er at sikre, at EU-medfinansierede 5G-projekter tager højde for cybersikkerhedsrisici. Værktøjskassen blev imidlertid først vedtaget i januar 2020. Da alle de projekter, vi gennemgik i forbindelse med denne revision, var udvalgt før vedtagelsen af EU-værktøjskassen til 5G-cybersikkerhed, kunne de ikke forventes at have fulgt den anbefalede tilgang til cybersikkerhed, bl.a. vedrørende højrisikoleverandører. I vores stikprøve havde vi f.eks. ét Horisont 2020-projekt og to EFRU-projekter i Spanien, hvor der blev brugt kinesisk 5G-udstyr, som efterfølgende blev forbudt i Sverige (jf. punkt ***15***).

67 I perioden 2021-2027 agter Kommissionen at fremme en sammenhængende tilgang til 5G-sikkerhed i EU-medfinansierede projekter ved at sikre, at anvendelse af værktøjskassen er en betingelse for EU-finansiering. Dette skal dog sikres på forskellige måder afhængigt af gennemførelsesmetoden:

- Under programmer, der forvaltes direkte af Kommissionen (f.eks. Horisont Europa for 2021-2027), vil det være muligt at udelukke leverandører, der udsættes for indgriben fra regeringen i et tredjeland. Dette kan sandsynligvis sikre, at der i EU-finansierede projekter tages højde for cybersikkerhedsrisici, og forhindre situationer, hvor en leverandør, der modtager EU-medfinansiering i en medlemsstat, er udelukket som højrisikoleverandør i en anden medlemsstat.

- For programmer, der gennemføres under delt forvaltning, indeholder lovgivningen ikke krav vedrørende cybersikkerhedsrisici. Kommissionen agter derfor at tilskynde til, at der indsættes henvisninger til værktøjskassen i medlemsstaternes partnerskabsaftaler for at sikre, at der i forbindelse med EFRU-finansiering til 5G-relaterede projekter tages højde for cybersikkerhedsrisici.

- Med hensyn til InvestEU-programmet (der erstatter EFSI)[55] og genopretnings- og resiliensfaciliteten vil Kommissionen også tilskynde de ansvarlige organer til at indsætte henvisninger til EU-værktøjskassen i finansieringsaftalerne.

[55] Forordning (EU) 2021/523 om oprettelse af InvestEU-programmet.

Medlemsstaterne adresserer endnu ikke sikkerhedsaspekter på en samordnet måde ved udrulning af 5G-net

Oplysningerne om medlemsstaternes tilgang til sikkerhedsspørgsmål er utilstrækkelige

68 Kommissionen overvåger og rapporterer om fremskridtene med implementeringen af EU-værktøjskassen til 5G-cybersikkerhed gennem NIS-samarbejdsgruppen, gennem bilaterale drøftelser med medlemsstaterne og indirekte gennem medierne. De første resultater af denne overvågning blev offentliggjort i juli 2020[56]. I december 2020 offentliggjorde Kommissionen desuden en rapport om virkningerne af sin henstilling om cybersikkerhed i forbindelse med 5G-net[57]. I september 2021 var der ingen planer om fremtidig rapportering.

69 De ovennævnte rapporter mangler imidlertid et fælles sæt nøgleresultatindikatorer og indeholder ikke sammenlignelige sæt af detaljerede oplysninger om, hvordan medlemsstaterne håndterer 5G-sikkerhedsbekymringer.

70 Desuden er der kun få offentligt tilgængelige oplysninger om medlemsstaternes tilgang til højrisikoleverandører - dvs. hvordan de identificeres, og om de udelukkes fra at levere 5G-udstyr - og selv disse oplysninger er modstridende og ufuldstændige. Som eksempler kan følgende nævnes:

- Kommissionen anførte i sin rapport fra juli 2020 om medlemsstaternes fremskridt med implementeringen af værktøjskassen (jf. punkt ***68***), at omkring halvdelen af medlemsstaterne (14 ud af 27) havde vurderet leverandørernes risikoprofil og anvendt restriktioner over for leverandører, der vurderedes at være højrisikoleverandører.

- BEREC anførte i en rapport fra december 2020[58], at kun ni medlemsstater havde indført sådanne restriktioner, og at syv af de resterende 18 medlemsstater ikke agtede at gøre det i fremtiden.

---

[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 af 16.12.2020.

[58] BEREC, "Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience), BoR 20 (227)", 10.12.2020.

71 Selv i de tilfælde, hvor medlemsstaterne har vedtaget lovgivning om sikkerheden i 5G-net (jf. også punkt ***75***), præciserer lovgivningen stadig ikke medlemsstaternes tilgang til højrisikoleverandører. Konkrete beslutninger vil sandsynligvis kun blive truffet ved gennemførelsesretsakter eller ved administrative eller kommercielle afgørelser, som ikke offentliggøres.

72 Ifølge de interessenter og beslutningstagere, vi interviewede (f.eks. i Europa-Parlamentet), har de kun begrænset adgang til ikkeoffentliggjort information (f.eks. i rapporter fra Kommissionen eller NIS-gruppen) om medlemsstaternes tilgang til højrisikoleverandører og må derfor forlade sig på medier og uofficielle kilder.

73 Trods 5G-sikkerhedsbekymringernes grænseoverskridende karakter foreligger der samlet set kun få offentlige oplysninger om medlemsstaternes tilgang til sikkerhedsspørgsmål, navnlig spørgsmålet om højrisikoleverandører. Dette begrænser udvekslingen af viden mellem medlemsstaterne og muligheden for at anvende samordnede foranstaltninger. Det begrænser også Kommissionens mulighed for at foreslå forbedringer af sikkerheden i 5G-net.

Der er tegn på, at medlemsstaterne anvender forskellige tilgange til 5G-leverandører

74 De nationale myndigheder har vide skønsbeføjelser i forbindelse med gennemførelsen af væsentlige foranstaltninger vedrørende 5G-sikkerhed (jf. punkt ***48*** og ***49***). Værktøjskassen tager hensyn til nationale kompetencer og relevante landespecifikke faktorer (trusselsvurderinger fra nationale sikkerhedstjenester, tidsplan for udrulning af 5G-net, tilstedeværelse af leverandører, cybersikkerhedskapacitet). Indtil videre har medlemsstaterne anvendt forskellige tilgange til brug af udstyr fra specifikke leverandører og til omfanget af restriktioner over for højrisikoleverandører (jf. eksemplerne i ***tekstboks 5*** vedrørende fire medlemsstater).

Tekstboks 5

Eksempler på medlemsstaternes forskellige tilgange til kinesiske 5G-leverandører

En ramme er på plads, og der anvendes restriktioner[(1)]

I oktober 2020 fastsatte den svenske telemyndighed (PTS) følgende betingelser for deltagelse i auktionen om 5G-frekvenser:

- at nye installationer og implementering af centrale funktioner til anvendelse af frekvensbåndene ikke udføres med produkter fra kinesiske leverandører

- at eksisterende infrastruktur fra sådanne leverandører udfases senest den 1. januar 2025.

En ramme er på plads, men anvendes endnu ikke[2], [3], [4]

Tysklands IT-sikkerhedslov 2.0 fra maj 2021 fastsætter, at der skal foretages en obligatorisk certificering af kritiske komponenter, før de kan godkendes til brug. De tyske mobilnetoperatører, vi interviewede, ville foretrække en fælles europæisk certificeringsprocedure under ENISA, der kunne fungere som en europæisk "one-stop-shop", i stedet for en masse nationale certificeringer. Loven giver også forbundsindenrigsministeriet mulighed for at forbyde brugen af kritiske komponenter, hvis de formodes at kunne udgøre en trussel mod den nationale sikkerhed.

I Østrig blev der i slutningen af oktober 2021 vedtaget en ajourføring af telekommunikationsloven, der giver den kompetente minister mulighed for at klassificere leverandører som højrisikoleverandører og anvende restriktioner eller udelukke dem fra markedet. Ifølge offentligt tilgængelige oplysninger fra oktober 2021 er landet ved at udvide sit 5G-net med udstyr fra den kinesiske leverandør Huawei.

Ingen ramme er på plads[5], [6]

Ungarn havde pr. september 2021 ikke anvendt restriktioner over for nogen 5G-leverandører og forventes heller ikke at gøre det i den nærmeste fremtid. Desuden har Ungarn officielt afvist at deltage i det internationale "5G Clean Network Program", som støttes af USA og sigter mod at begrænse tilstedeværelsen af kinesiske leverandørers udstyr i 5G-kernenet.

(1) Beslutning 18-8496 af 20.10.2020 om betingelserne for auktion af frekvensbåndene 3,5 GHz og 2,3 GHz.

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

(3) Østrigs telekommunikationslov.

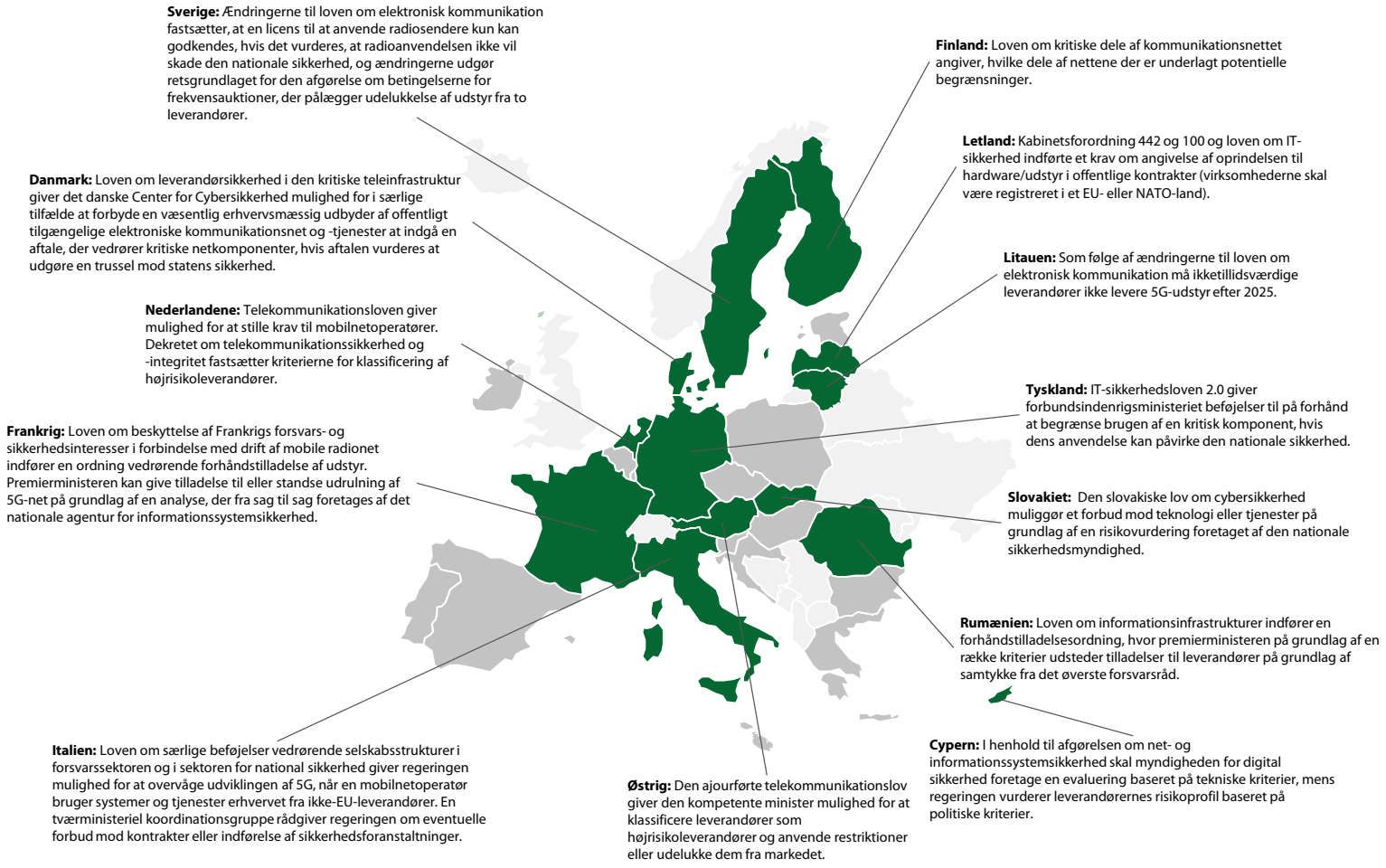
(4) https://www.euractiv.com/section/5g/news/austria-to-also-rely-on-huawei-in-5g-rollout/

(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 Siden værktøjskassens vedtagelse er der sket fremskridt med hensyn til at styrke sikkerheden i 5G-net, og de fleste medlemsstater anvender eller er ved at indføre restriktioner over for højrisikoleverandører. Ved udgangen af 2021 havde 13 medlemsstater vedtaget eller ændret national lovgivning om 5G-sikkerhed. Disse lovgivningsmæssige foranstaltninger tager hensyn til kriterierne i værktøjskassen, men anvender forskellige tilgange (jf. ***figur 6***). Andre medlemsstater er i færd med at udarbejde lovgivning. I de kommende år kan dette føre til mere ensartede tilgange til højrisikoleverandører af 5G-udstyr, i hvert fald i de medlemsstater, der har vedtaget relevant lovgivning.

Figur 6 - Medlemsstater med love, som muliggør forbud mod brug af udstyr fra højrisikoleverandører i deres net - oktober 2021



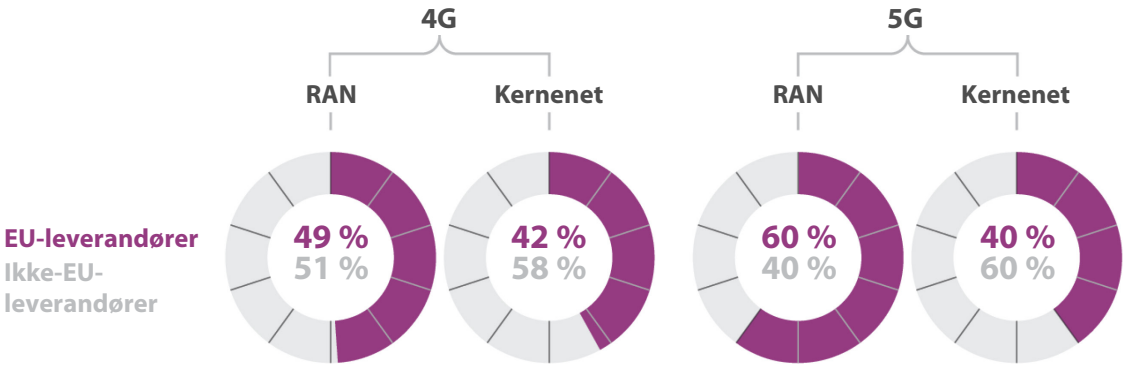
Kilde: Revisionsretten, baseret på data fra Europa-Kommissionen.

76 Indtil videre har Kommissionen ikke vurderet, hvilke konsekvenser anvendelsen af forskellige tilgange kan få, hvis en medlemsstat opbygger sine 5G-net med udstyr fra en leverandør, der i en anden medlemsstat betragtes som en højrisikoleverandør. Dette kan påvirke enten den grænseoverskridende sikkerhed eller konkurrencen mellem mobilnetoperatørerne på EU's indre marked.

Kommissionen er for nylig begyndt at behandle spørgsmålet om udenlandske subsidier, der fordrejer det indre marked

77 I december 2020 var over halvdelen af det samlede 4G- og 5G-udstyr i EU indkøbt fra ikke-EU-leverandører (jf. ***figur 7***).

Figur 7 - Andelen af mobilnetoperatører, der bruger udstyr fra EU-leverandører/ikke-EU-leverandører*



* *Herunder leverandører fra Nordamerika, Asien og Australien.*

Kilde: Revisionsretten, baseret på BEREC, "Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)". BoR (20) 227.

78 Ved udgangen af 2019 brugte nærmere bestemt 286 millioner kunder i EU-27 (64 % af den samlede befolkning) telekommunikationsnet baseret på 4G-udstyr fra kinesiske leverandører[59]. I oktober 2020 gav en gruppe medlemmer af Europa-Parlamentet udtryk for bekymring over for medlemsstaternes telekommunikations- og handelsministre samt Kommissionen, idet en af årsagerne til de kinesiske leverandørers store markedsandel efter deres opfattelse er, at de har en urimelig økonomisk fordel, fordi de modtager offentlige subsidier, som i henhold til EU's

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

statsstøtteregler ikke er tilgængelige for EU-leverandører[60]. I en nylig analyse fremhævede vi nogle relaterede risici[61]. Sådanne subsidier kan fordreje det indre marked, så 5G-leverandørerne ikke har lige vilkår, hvilket kan få sikkerhedsmæssige konsekvenser. Med henblik på at løse dette problem fremsatte Kommissionen i maj 2021 forslag til en ny forordning[62], der fastsætter procedurer for undersøgelse af sådanne subsidier og for afhjælpning af de relaterede konkurrencefordrejninger.

Kommissionen har ikke tilstrækkelige oplysninger om mulige omkostninger til udskiftning af kinesiske leverandørers udstyr

79 Ifølge en rapport fra juni 2020[63] vil anvendelse af restriktioner over for en væsentlig leverandør af 5G-infrastruktur i EU øge de samlede investeringsomkostninger med næsten 2,4 milliarder euro om året i det næste årti (dvs. 24 milliarder euro i alt). Ifølge en anden undersøgelse[64] står de europæiske operatører allerede over for at skulle opgradere de 4G-net, der blev bygget mellem 2012 og 2016, fordi det er almindelig forretningspraksis at gennemgå og modernisere netværksudstyr, der er mere end tre-fire år gammelt. I undersøgelsen anslås det, at de samlede omkostninger til udskiftning af opgraderbart udstyr erhvervet fra kinesiske leverandører siden 2016 vil beløbe sig til ca. 3 milliarder euro.

80 Eftersom en stor andel af udstyret i de europæiske net kommer fra kinesiske leverandører, og disse kan blive kategoriseret som højrisikoleverandører i visse medlemsstater, kan mobilnetoperatører skulle afholde milliarder i udskiftningsomkostninger, hvis de er nødt til at fjerne og erstatte udstyr fra kinesiske leverandører uden en overgangsperiode (jf. punkt ***77***-***79***). I princippet kan der ikke ydes statsstøtte til at kompensere operatører for omkostninger forbundet med opfyldelse af retlige forpligtelser, medmindre medlemsstaterne kan godtgøre over for Kommissionen, at de nødvendige betingelser er opfyldt (f.eks. at der er en tilskyndelsesvirkning). Vi konstaterede under vores analyse ét tilfælde, hvor den

---

[60] Brev fra MEP'er til EU's telekommunikations- og handelsministre og til EU-kommissærerne Thierry Breton, Margrethe Vestager og Valdis Dombrovskis, 14.10.2020.

[61] Revisionsrettens analyse nr. 03/2020:"EU's reaktion på Kinas statsdrevne investeringsstrategi".

[62] Forslag til forordning om udenlandske subsidier, der fordrejer det indre marked, COM(2021) 223 final af 5.5.2021.

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

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

nationale lovgivning eventuelt kan tillade national offentlig støtte til dækning af udskiftningsomkostninger (jf. den finske lov om elektroniske kommunikationstjenester[65]). Medlemsstaterne skal underrette Kommissionen om enhver form for statsstøtte, der ydes for at kompensere mobilnetoperatører for sådanne omkostninger. Kommissionen oplyste, at den endnu ikke er blevet kontaktet af nogen medlemsstat eller interessent med henblik på at drøfte statsstøtte til dækning af omkostninger vedrørende udskiftning af udstyr. Den manglende klarhed om medlemsstaternes behandling af sådanne omkostninger - og de eventuelle forskelle mellem medlemsstaterne - skaber ifølge de interessenter fra industrien, der blev interviewet under revisionen, usikkerhed for erhvervslivet og kan påvirke den rettidige udrulning af 5G.

[65] Lov om elektroniske kommunikationstjenester 1207/2020 af 30.12.2020, artikel 301.

Konklusioner og anbefalinger

81 Samlet set viste vores revision, at der trods Kommissionens støtte er betydelige forsinkelser i medlemsstaternes udrulning af 5G-net, og at der er behov for en yderligere indsats for at håndtere sikkerhedsspørgsmål vedrørende 5G-udrulning.

82 I sin 5G-handlingsplan fra 2016 opfordrede Kommissionen til 5G-dækning i alle byområder og langs større transportveje senest i 2025, og i marts 2021 opfordrede den til fuld dækning senest i 2030. Ved udgangen af 2020 havde 23 medlemsstater lanceret kommercielle 5G-tjenester og nået delmålet om, at der i mindst én stor by skulle være adgang til sådanne tjenester. Vi konstaterede imidlertid, at ikke alle medlemsstater henviser til Kommissionens mål i deres nationale 5G-strategier eller bredbåndsplaner. Hertil kommer, at flere lande endnu ikke har gennemført den europæiske kodeks for elektronisk kommunikation i national ret, og at tildelingen af 5G-frekvenser er forsinket. Forsinkelserne i frekvenstildelingen har forskellige årsager: svag efterspørgsel fra mobilnetoperatørerne, problemer vedrørende koordinering med ikke-EU-lande langs de østlige grænser, covid-19's indvirkning på auktionskalenderne og usikkerhed om håndteringen af sikkerhedsspørgsmål. Ifølge Kommissionen er det kun sandsynligt, at 11 medlemsstater når 2025-målet (jf. punkt ***22***-***43***).

83 Kommissionen har støttet medlemsstaternes gennemførelse af 5G-handlingsplanen fra 2016 med initiativer, vejledning og finansiering af 5G-relateret forskning. Kommissionen har dog ikke defineret den forventede servicekvalitet i 5G-nettene, f.eks. med præstationskrav vedrørende minimumshastighed og maksimal latenstid. Det har medført, at udtrykket "5G-kvalitet" forstås forskelligt af medlemsstaterne. Vi bemærkede, at medlemsstaterne har forskellige tilgange til udrulning af 5G-tjenester, så f.eks. kun to medlemsstater har fastsat krav vedrørende minimumshastighed og maksimal latenstid. I sidste ende skaber disse forskellige tilgange en risiko for uligheder i adgangen til og kvaliteten af 5G-tjenester i EU og for, at den "digitale kløft" mellem forskellige medlemsstater og regioner dermed bliver større i stedet for mindre (jf. punkt ***22***-***31***).

Anbefaling 1 - Fremme en jævn og rettidig udrulning af 5G-net i EU

Kommissionen bør:

a) sammen med medlemsstaterne udvikle en fælles definition på den forventede servicekvalitet i 5G-nettene, f.eks. med præstationskrav vedrørende minimumshastighed og maksimal latenstid

b) tilskynde medlemsstaterne til ved de næste ajourføringer af deres 5G-strategier, digitale strategier eller bredbåndsplaner at medtage 2025- og 2030-målene for 5G-udrulning og de foranstaltninger, der er nødvendige for at nå dem

c) støtte medlemsstaterne i deres håndtering af problemer vedrørende frekvenskoordinering med nabolande uden for EU, f.eks. ved at opfordre til at sætte emnet på dagsordenen for hvert relevant møde.

Tidsramme: december 2022

84 Sikkerhedsaspekterne ved 5G-net blev først for nylig et væsentligt bekymringspunkt på EU-plan. Behovet for en indsats på EU-plan blev i 2019 fremhævet af Det Europæiske Råd, som opfordrede til en fælles tilgang og til samarbejde mellem medlemsstaterne om dette grænseoverskridende emne. Kommissionen reagerede sammen med medlemsstaterne hurtigt på nye 5G-sikkerhedsbekymringer. I 2020 vedtog NIS-samarbejdsgruppen en EU-værktøjskasse til 5G-cybersikkerhed, som angiver en række strategiske foranstaltninger, tekniske foranstaltninger og støttetiltag vedrørende håndtering af sikkerhedstrusler mod 5G-net og identificerer de aktører, der er ansvarlige for de enkelte foranstaltninger. Flere af foranstaltningerne adresserer spørgsmålet om højrisikoleverandører af 5G-udstyr. Denne værktøjskasse er efterfølgende blevet godkendt af Kommissionen og Det Europæiske Råd (jf. punkt ***45***-***47***). Da værktøjskassen er et soft law-instrument, er disse foranstaltninger ikke bindende for medlemsstaterne. I den nye europæiske strategi for fremme af intelligente, rene og sikre forbindelser i digitale systemer i hele verden omtales EU-værktøjskassen til 5G-cybersikkerhed som et retningsgivende værktøj for investeringer i digital infrastruktur (jf. punkt ***50***).

85 Kriterierne i værktøjskassen skaber en operationel ramme, der er nyttig til på en koordineret måde at vurdere leverandørernes risikoprofil i samtlige medlemsstater. Gennemførelsen af denne vurdering forbliver dog et nationalt ansvar (jf. punkt ***54***).

86 Siden værktøjskassens vedtagelse er der sket fremskridt med hensyn til at styrke sikkerheden i 5G-net, og de fleste medlemsstater anvender eller er ved at indføre restriktioner over for højrisikoleverandører. Under hensyntagen til denne ramme havde 13 medlemsstater i oktober 2021 vedtaget eller ændret lovgivning om 5G-sikkerhed. Andre medlemsstater er i færd med at udarbejde lovgivning, der tager hensyn til kriterierne i værktøjskassen (jf. punkt ***54*** og ***75***).

87 Værktøjskassen blev vedtaget i en tidlig fase af 5G-udrulningen, men en række mobilnetoperatører havde allerede valgt deres leverandører af 5G-udstyr (jf. punkt ***52***). Manglende adressering af sikkerhedsbekymringer ved udformningen af en politik kan indvirke negativt på politikgennemførelsen, så de forventede fordele (f.eks. vækst i BNP) kan udhules af omkostninger forbundet med håndtering af trusler (f.eks. omkostninger ved cyberkriminalitet) (jf. punkt ***02*** og ***04***).

88 Værktøjskassen tager hensyn til nationale kompetencer og relevante landespecifikke faktorer. Vores revision viste, at medlemsstaterne indtil videre har anvendt forskellige tilgange til brug af udstyr fra højrisikoleverandører og til omfanget af restriktioner (så de f.eks. kun gælder 5G-kernenettet og dets kritiske dele eller kun gælder Radio Access Network (RAN) eller en del af det) (jf. punkt ***74*** og ***75***).

89 I de kommende år kan den lovgivning om 5G-sikkerhed, som medlemsstaterne har indført på grundlag af værktøjskassen, føre til mere ensartede tilgange til højrisikoleverandører af 5G-udstyr. Ingen af de foranstaltninger, der indgår i værktøjskassen, er imidlertid juridisk bindende, så Kommissionen har ikke beføjelser til at kræve dem indført. Der er derfor en risiko for, at værktøjskassen ikke i sig selv kan garantere, at medlemsstaterne behandler sikkerhedsaspekter på en samordnet måde (jf. punkt ***49***-***75***).

90 Mange 5G-leverandører har hjemsted uden for EU og opererer således inden for rammerne af tredjelandes lovgivning, som kan adskille sig meget fra EU's standarder, f.eks. med hensyn til effektiv beskyttelse af borgernes data og mere generelt med hensyn til, hvordan domstolenes uafhængighed er sikret ved hjælp af lovgivningsmæssige eller demokratiske kontrolforanstaltninger. Det forhold, at 5G-net i overvejende grad er softwaredrevne, kan give anledning til særlige sikkerhedsbekymringer, hvis kontrolcentrene for denne type software placeres i ikke-EU-lande, og EU-borgere dermed potentielt underlægges disse tredjelandes lovgivning. Kommissionen er begyndt at adressere disse bekymringer og har den holdning, at alle virksomheder, der leverer tjenester til EU-borgere, skal acceptere og respektere EU's

regler og værdier. Den har også indledt dialog med flere lande for at sikre en stærk beskyttelse af privatlivets fred og af personoplysninger (jf. punkt ***56***-***62***).

91 Trods 5G-sikkerhedsbekymringernes grænseoverskridende karakter mangler der offentlige oplysninger om medlemsstaternes tilgang til sikkerhedsspørgsmål og deres afhængighed af højrisikoleverandører. Kommissionen overvåger og rapporterer om implementeringen af EU-værktøjskassen. Dens rapporter indeholder imidlertid ikke detaljerede og sammenlignelige oplysninger om, hvordan medlemsstaterne håndterer 5G-sikkerhedsbekymringer. I september 2021 var der desuden ingen planer om fremtidig rapportering. Denne mangel på oplysninger begrænser udvekslingen af viden mellem medlemsstaterne og muligheden for at anvende samordnede foranstaltninger. Den begrænser også Kommissionens mulighed for at foreslå forbedringer af sikkerheden i 5G-net (jf. punkt ***68***-***73***).

Anbefaling 2 - Fremme en samordnet tilgang til 5G-sikkerhed blandt medlemsstaterne

Kommissionen bør:

a) give yderligere vejledning eller støtte tiltag vedrørende centrale elementer i EU-værktøjskassen til 5G-cybersikkerhed, f.eks. kriterier for vurdering af 5G-leverandører og klassificering af højrisikoleverandører, samt vedrørende databeskyttelseshensyn

Tidsramme: december 2022

b) fremme gennemsigtighed vedrørende medlemsstaternes tilgange til 5G-sikkerhed ved at overvåge og rapportere om gennemførelsen af sikkerhedsforanstaltningerne i EU-værktøjskassen til 5G-cybersikkerhed. Dette bør gøres på grundlag af et fælles sæt nøgleresultatindikatorer

Tidsramme: december 2022

c) sammen med medlemsstaterne vurdere, hvilke aspekter af 5G-netsikkerhed der bør underlægges krav, som det er muligt at håndhæve, og tage initiativ til lovgivning, hvor det er relevant.

Tidsramme: december 2022

92 Kommissionen er begyndt at behandle påstandene om unfair økonomiske fordele som følge af udenlandske subsidier. Sådanne subsidier kan fordreje det indre marked, så 5G-leverandørerne ikke har lige vilkår, hvilket kan få sikkerhedsmæssige konsekvenser (jf. punkt ***78***).

93 Kommissionen har ikke tilstrækkelige oplysninger om medlemsstaternes behandling af de potentielle udskiftningsomkostninger, der skal afholdes, hvis mobilnetoperatører er nødt til at fjerne højrisikoleverandørers udstyr i EU-net uden en overgangsperiode. Forskelle i behandlingen kan skabe usikkerhed for erhvervslivet og påvirke den rettidige udrulning af 5G (jf. punkt ***79*** og ***80***). Samtidig kan medlemsstaternes tilgange til 5G-sikkerhed, og navnlig manglen på en samordnet tilgang i EU, påvirke det indre markeds effektive funktion. Kommissionen har endnu ikke vurderet dette spørgsmål (jf. punkt ***74***-***76***).

Anbefaling 3 - Overvåge medlemsstaternes tilgange til 5G-sikkerhed og vurdere, hvordan forskellene påvirker det indre markeds effektive funktion

Kommissionen bør:

a) tilskynde medlemsstaterne til at anvende en gennemsigtig og konsekvent tilgang til behandling af mobilnetoperatørers omkostninger til udskiftning af 5G-udstyr, der er indkøbt fra højrisikoleverandører, idet den regelmæssigt overvåger og rapporterer om dette spørgsmål vedrørende implementeringen af EU-værktøjskassen til 5G-cybersikkerhed

b) vurdere, hvilke konsekvenser det kan få for det indre marked, hvis en medlemsstat opbygger sine 5G-net med udstyr fra en leverandør, der i en anden medlemsstat betragtes som en højrisikoleverandør.

Tidsramme: december 2022

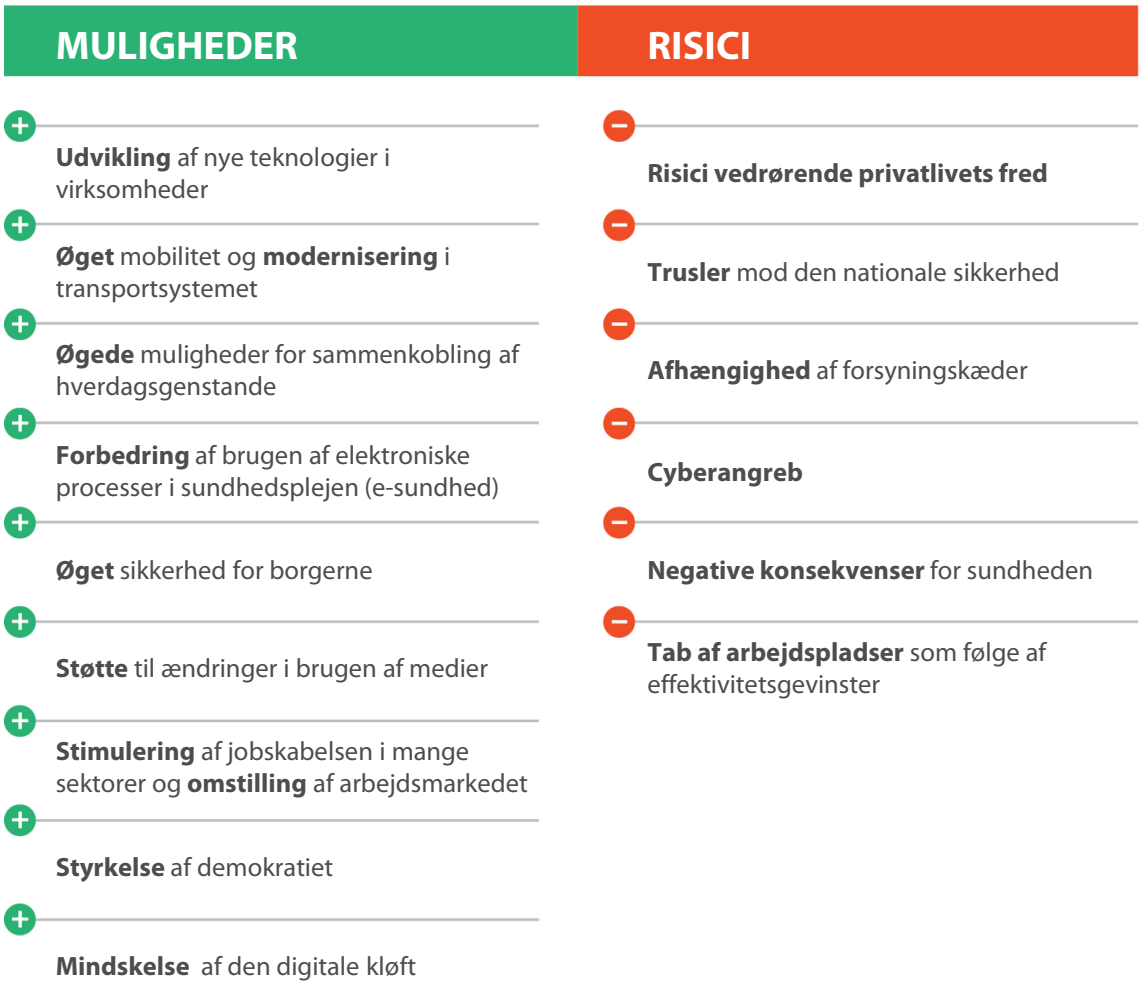
Vedtaget af Afdeling II, der ledes af Iliana Ivanova, medlem af Revisionsretten, i Luxembourg den 15. december 2021.

På Revisionsrettens vegne

Klaus-Heiner Lehne
Formand

Bilag

Bilag I - De væsentligste muligheder og risici i forbindelse med 5G



Kilde: Revisionsretten, baseret på Europa-Parlamentets Forskningstjeneste - European Science-Media hub.

Bilag II - Eksempler på konsekvenser af forstyrrelser i telekommunikationsnet og cybersikkerhedshændelser

Nedbrud på Frankrigs alarmnumre[66, 67]

01 Den 3. juni 2021 forhindrede en netafbrydelse hos Orange, det største franske teleselskab, nødopkald i en periode på flere timer. Det er blevet udelukket, at nedbruddet skyldtes et cyberangreb, men hændelsen viser, hvor store konsekvenser forstyrrelser i kritisk netinfrastruktur potentielt kan få.

Ransomwareangreb mod Irlands offentlige sundhedsvæsen[68, 69, 70]

02 I maj 2021 lukkede det irske sundhedsvæsen (Health Service Executive) alle sine IT-systemer på grund af et ransomwareangreb. Angrebet påvirkede alle aspekter af patientbehandlingen, da det besværliggjorde adgangen til patientjournaler og dermed øgede risikoen for forsinkelser og fejl. Den irske forvaltning mener ikke, at patientdata blev kompromitteret, men lækningen af journaler kunne have ført til alle tænkelige typer forbrydelser såsom svig og afpresning. Ifølge generaldirektøren for Health Service Executive vil genopretningsomkostningerne formentlig beløbe sig til 500 millioner euro (600 millioner USD).

---

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 er et amerikansk selskab, der udvikler software til at hjælpe virksomheder samt statslige og føderale myndigheder med at styre netværk, systemer og IT-infrastruktur. I starten af 2020 var Solarwinds udsat for et softwareangreb. Det lykkedes hackerne at føre angrebet videre ud til Solarwinds' kunder via softwareopgraderinger, der indeholdt skadelig kode. Disse opgraderinger åbnede bagdøre på kundernes platforme og gav let adgang for angreb og installation af yderligere malware og spyware.

[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

Bilag III - Retlig og politisk ramme

Europa-Kommissionen

Det Europæiske Råd EU-Rådet

Lovgivning

NIS-samarbejds-gruppen

2016 NIS-direktivet, juli 2016 - Med bestemmelser om retlige foranstaltninger, der skal styrke det samlede cybersikkerhedsniveau i EU.

2016 5G-handlingsplanen, september 2016 - Med et mål om lancering af 5G-tjenester i alle medlemsstater inden udgangen af 2020 og hurtig opbygning for at sikre uafbrudt 5G-dækning i byområder og langs større transportveje senest i 2025.

2018 Kodeksen for elektronisk kommunikation, december 2018 - Med et mål om at skabe et indre marked for elektroniske kommunikationsnet og -tjenester.

2019 Det Europæiske Råds konklusioner, marts 2019 - Med en anmodning til Kommissionen om at udstede en henstilling om en fælles tilgang til 5G-nets sikkerhed.

2019 Henstillingen om 5G-cybersikkerhed, marts 2019 - Med et mål om, at medlemsstaterne kan vurdere de cybersikkerhedsrisici, der påvirker 5G-net på nationalt plan, og træffe de nødvendige sikkerhedsforanstaltninger.

2019 Rådets konklusioner om betydningen af 5G for den europæiske økonomi, december 2019 - Med fremhævelse af, at en hurtig og sikker udrulning af 5G-net er afgørende for at styrke EU's konkurrenceevne og kræver en koordineret tilgang i EU.

2020 Værktøjskassen til 5G-cybersikkerhed, januar 2020 - Med et forslag til fælles foranstaltninger, der kan begrænse de væsentligste cybersikkerhedsrisici ved 5G-net.

2020 En EU-værktøjskasse til udrulning af sikre 5G-net i EU, januar 2020 - Med Europa-Kommissionens støtte til værktøjskassen og fastlæggelse af de næste skridt (f.eks. en gennemførelsesrapport senest i juni 2020).

2020 Rådets konklusioner om Europas digitale fremtid i støbeskeen, juni 2020 - Med understregelse af behovet for at sikre og gennemføre en koordineret tilgang til at afbøde de største risici vedrørende udrulning af sikre 5G-net i EU.

2020 Det Europæiske Råds konklusioner, oktober 2020 - Med støtte til værktøjskassen til 5G-cybersikkerhed og opfordring til at anvende de relevante restriktioner over for højrisikoleverandører.

2020 Henstilling om [...] adgang til 5G-radiofrekvenser, september 2020 - Med retningslinjer for udvikling af bedste praksis vedrørende fremme af konnektiviteten og sikring af rettidig og investeringsvenlig adgang til 5G-radiofrekvenser.

2020 EU's strategi for cybersikkerhed for det digitale årti, december 2020 - Et soft law-dokument med angivelse af Kommissionens prioriteter og planlagte tiltag vedrørende cybersikkerhed generelt, herunder i 5G-net.

2020 Forslag til NIS 2-direktiv, december 2020 - Med et mål om at modernisere og udvide det nuværende direktivs anvendelsesområde og dække 5G-cybersikkerhed mere eksplicit.

2020 Forslag til direktiv om kritiske enheders modstandsdygtighed, december 2020 - Med et mål om at mindske sårbarhederne i de kritiske infrastrukturer, der er afgørende for, at EU's samfund og økonomi kan fungere.

2020 Det digitale kompas 2030: Europas kurs i det digitale årti, marts 2021 - Med kortlægning af en klar vej mod en fælles vision og en fælles indsats, der vil gøre Europa i stand til at klare sig i det digitale årti.

2021 Rådets konklusioner om EU's strategi for cybersikkerhed for det digitale årti, marts 2021 - Med støtte til de næste skridt, der skal tages med hensyn til 5G-nets cybersikkerhed, som fastsat i Kommissionens strategi for cybersikkerhed.

Bilag IV - Eksempler på projekter medfinansieret af EFSI

5G-relaterede EFSI-projekter

De to EFSI-projekter, vi gennemgik, vedrørte investeringer i forskning, udvikling og innovation med henblik på udvikling af 5G-produktporteføljer. De omfattede udvikling af hardware og software til både Radio Access Network og kernenettet. Begge projekter bidrog til at opnå større tæthed i udrulningen af celler, støttede standardisering og muliggjorde vigtige teknologiske eksperimenter.

Projekterne startede i 2018 og sluttede i december 2020. De omfattede tilsammen investeringsomkostninger på 3,9 milliarder euro, hvoraf 1 milliard euro kom fra EFSI.

Bilag V - Eksempler på Horisont 2020- og EFRU-projekter

5G-relateret Horisont 2020-projekt

Dette projekt anvender udstyr fra alle de tre største 5G-leverandører (Ericsson, Huawei og Nokia) til at teste 5G-teknologier i den grænseoverskridende korridor, der forbinder byerne Metz (Frankrig), Merzig (Tyskland) og Luxembourg. Projektet startede i november 2018 og forventedes at vare 31 måneder. EU ydede 12,9 millioner euro til dækning af de samlede budgetterede omkostninger på 17,1 million euro.

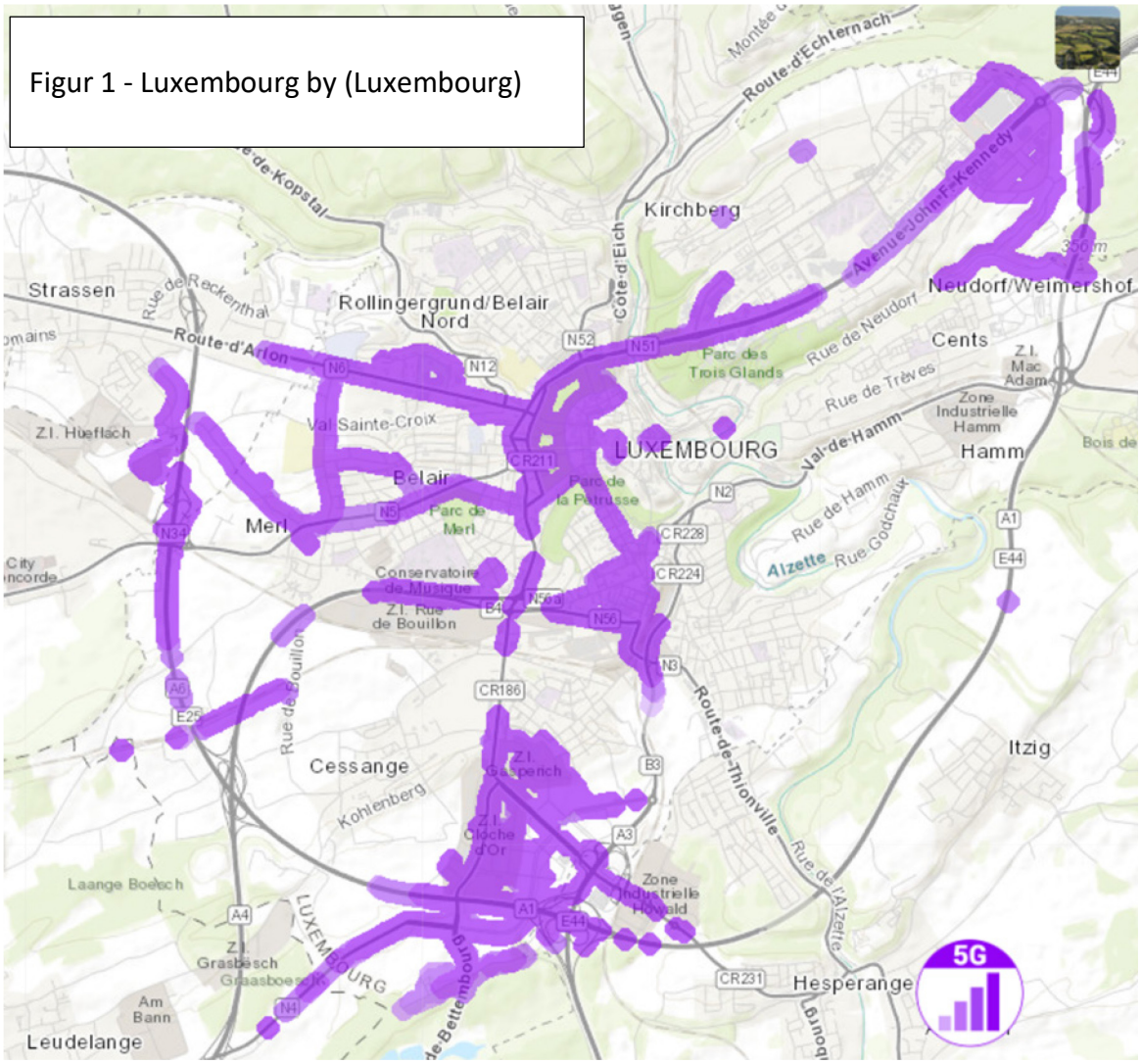
5G-relateret EFRU-projekt

Formålet med dette spanske projekt er at skaffe viden om udrulning af 5G-net. Det omfatter eksperimentering med netværksadministrationsteknikker baseret på 5G-teknologi, f.eks. network virtualisation, edge computing, dynamic network service allocation og network slicing samt udvikling af cases vedrørende 5G-brug. Projektet startede i 2019 og forventedes at vare 30 måneder. EU-bidraget udgør 2,2 millioner euro til dækning af de samlede forventede omkostninger på 7,1 million euro.

Bilag VI - 5G-dækning i udvalgte byer

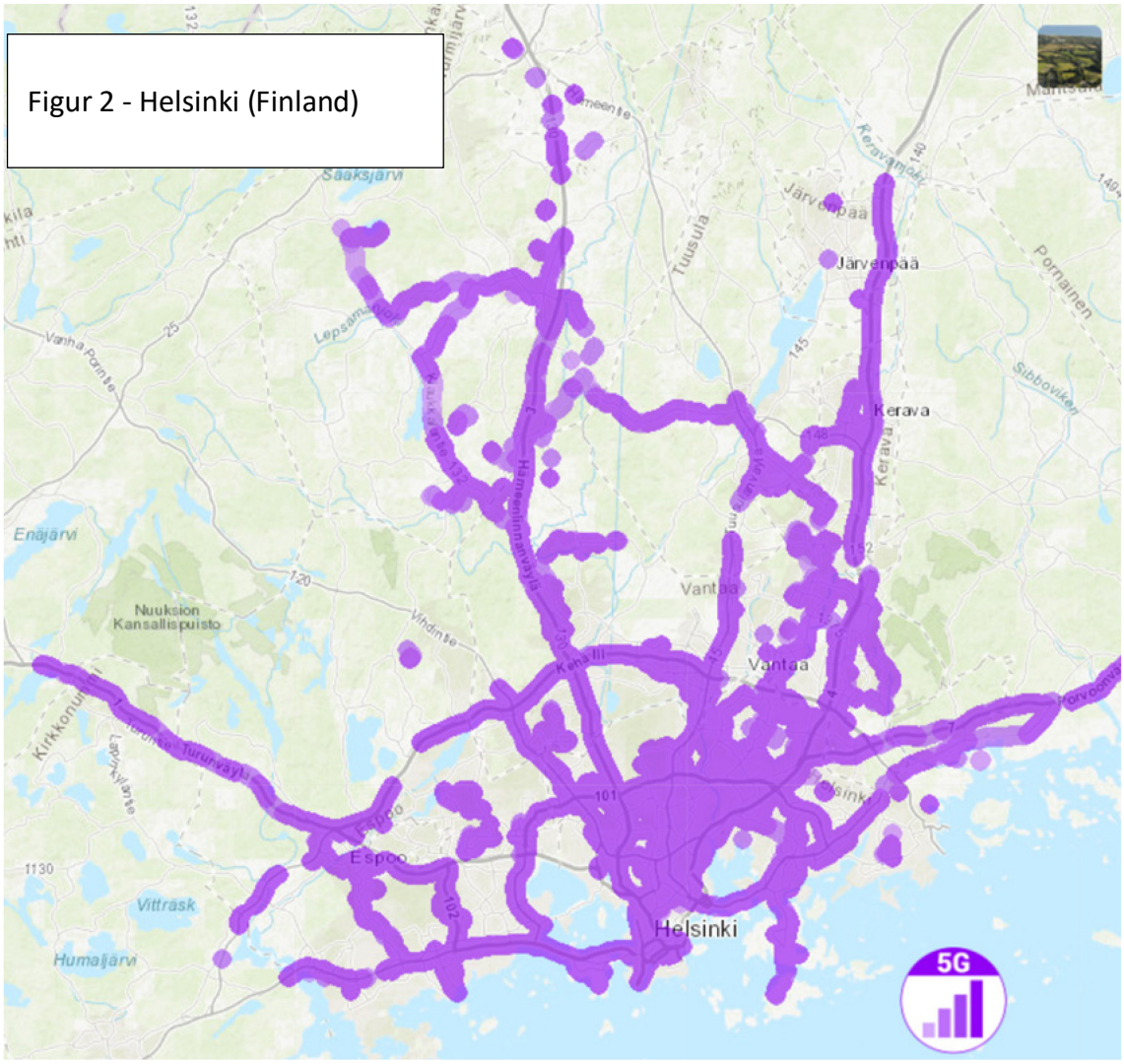
Nedenstående figurer er baseret på data for mobilbredbåndsforbindelser indsamlet fra test udført af brugere af Nperf-appen. De områder, hvor 5G er blevet påvist, er ikke nødvendigvis kommercielt åbne. Da nettenes præstationer afhænger af de enkelte mobilnetoperatører, viser disse kort - udtrukket den 4. oktober 2021 - kun dækningen og ikke præstationer med hensyn til f.eks. hastighed og latenstid.

Figur 1 - Luxembourg by (Luxembourg)

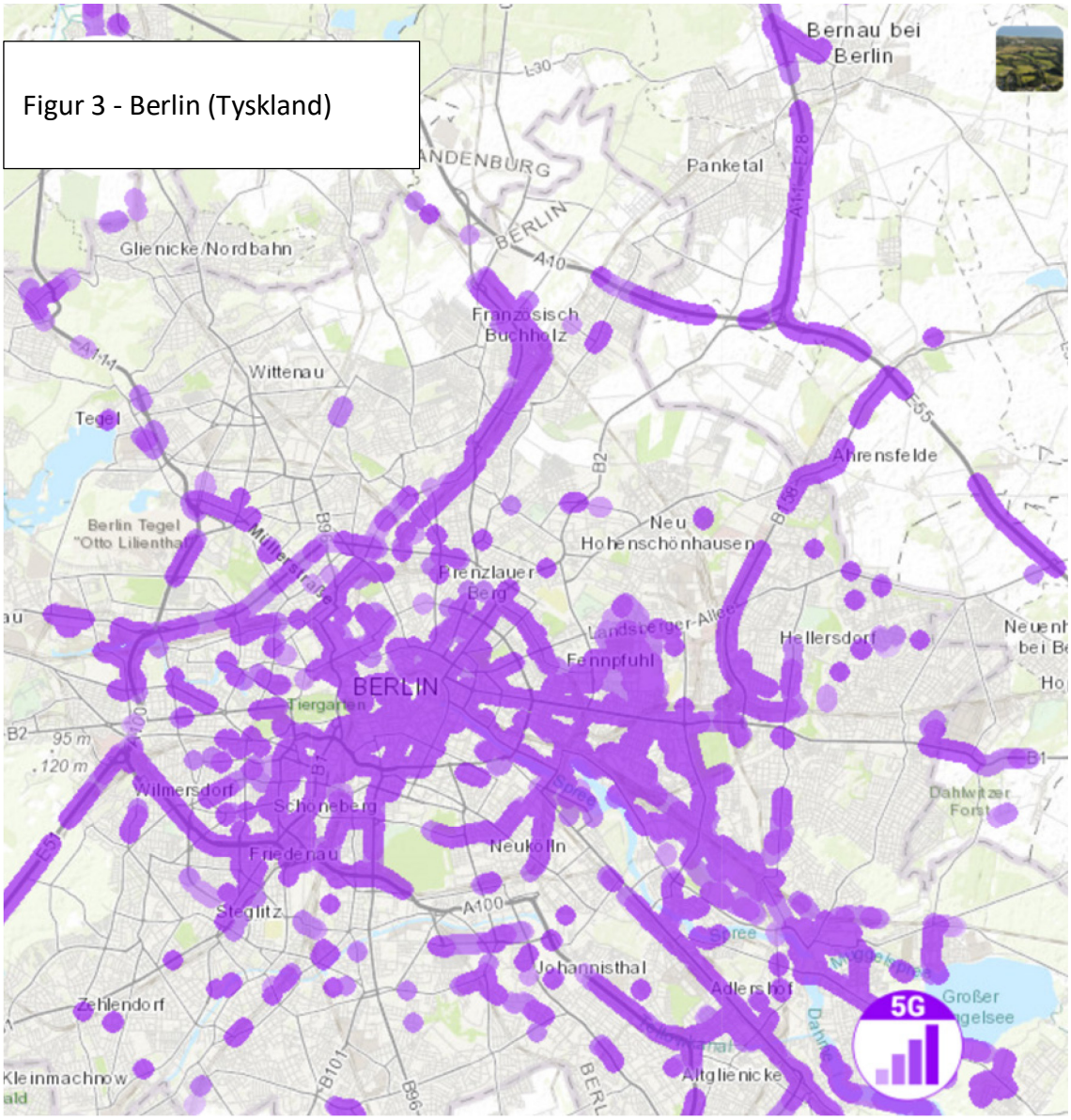


© nPerf.

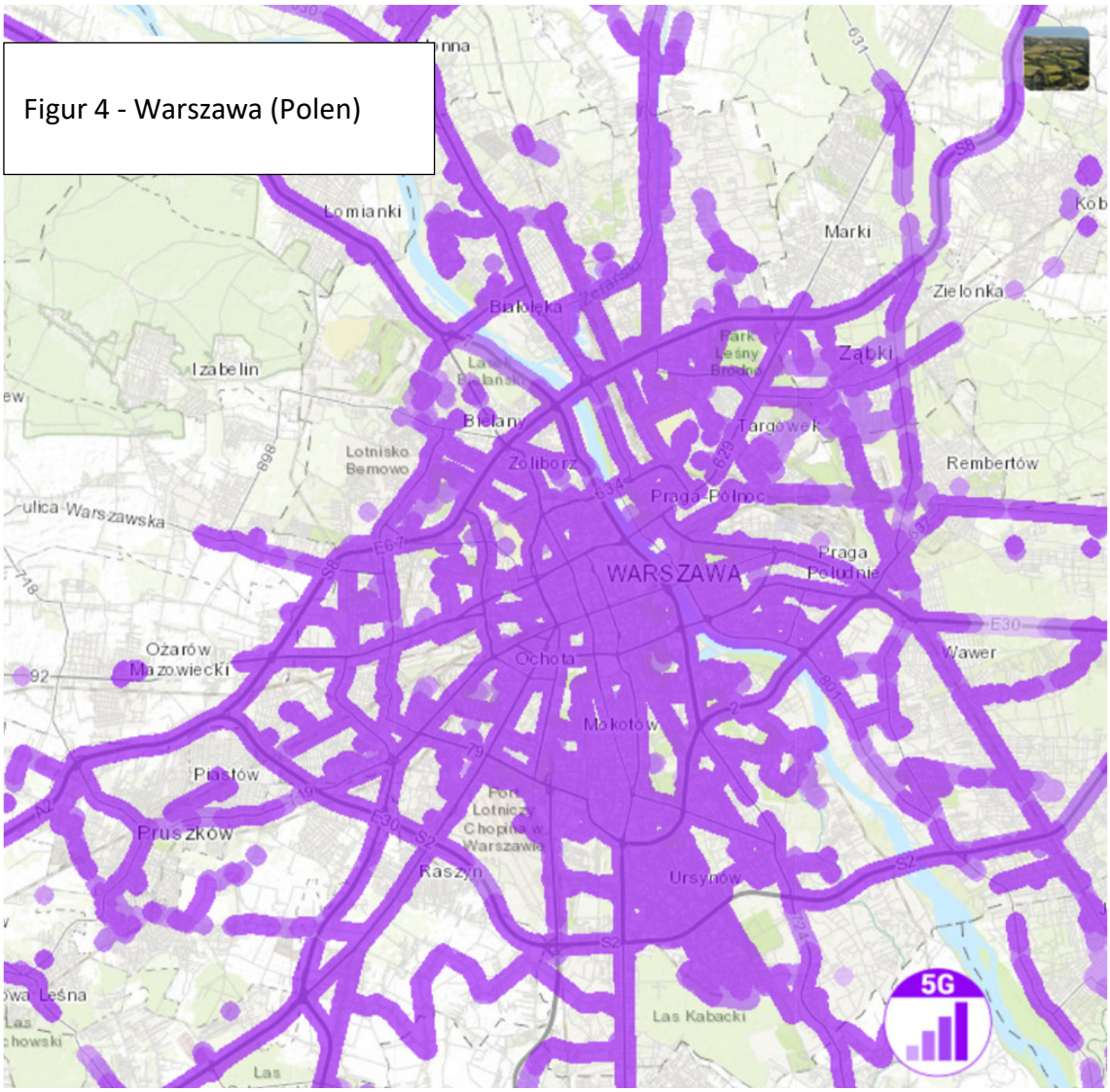
Figur 2 - Helsinki (Finland)



© nPerf.

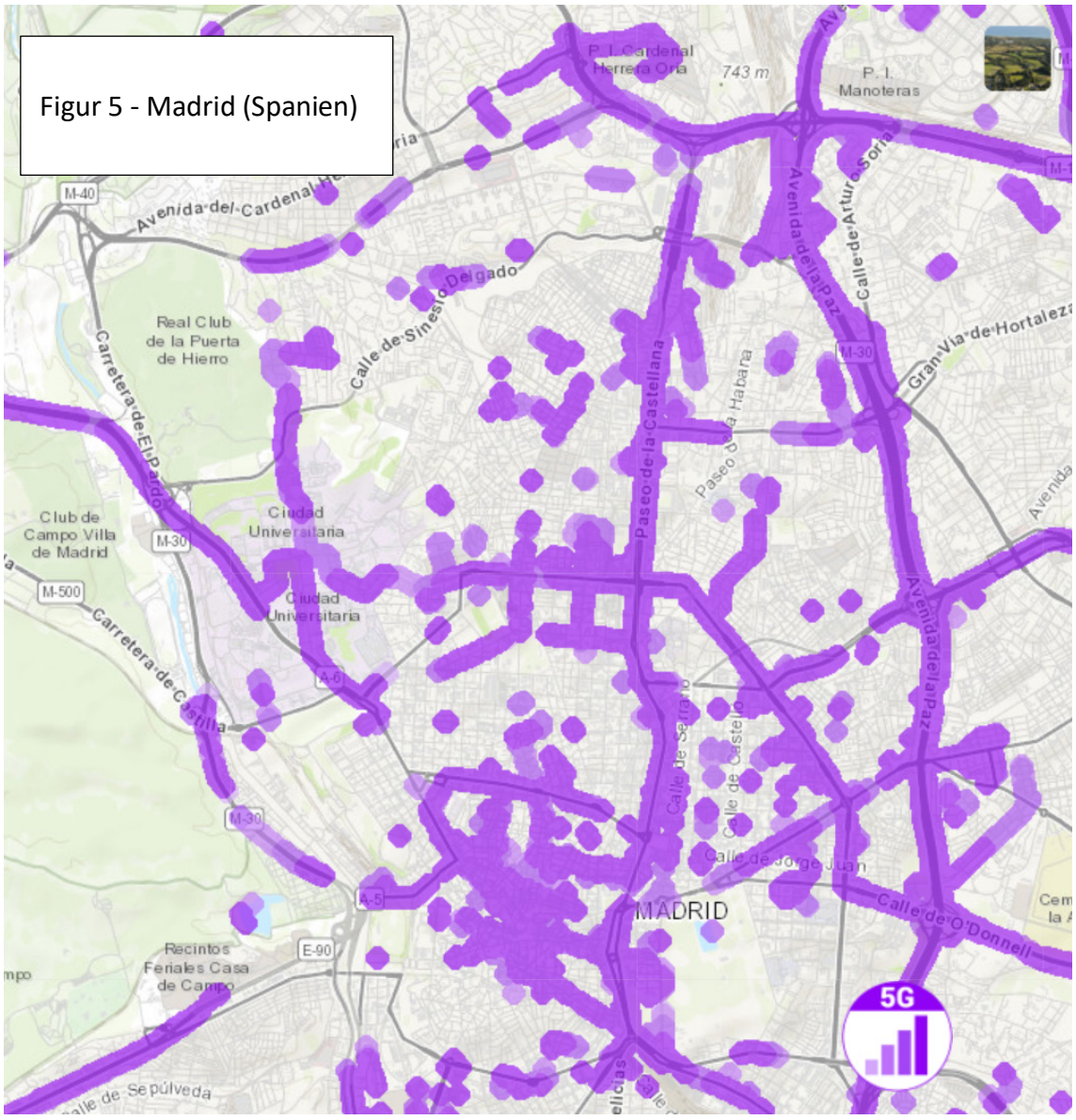


Figur 3 - Berlin (Tyskland)



Figur 4 - Warszawa (Polen)

© nPerf.



Figur 5 - Madrid (Spanien)

© nPerf.

Bilag VII - EU-værktøjskassen til 5G-cybersikkerhed

EU-værktøjskassen til 5G-cybersikkerhed, der er vedtaget af NIS-samarbejdsgruppen og godkendt af Kommissionen, omfatter tre typer ikkebindende foranstaltninger (strategiske foranstaltninger, tekniske foranstaltninger og støttetiltag), der skal gennemføres af forskellige aktører, som angivet nedenfor.

Foranstaltninger	Relevante aktører				
	Medlems-staternes myndigheder	Mobilnet-operatører	Europa-Kommissionen	ENISA	Interessenter (inkl. leverandører)
Strategiske foranstaltninger					
SF01 - Styrkelse af de nationale myndigheders rolle	✓	✓			
SF02 - Audit af operatører og krav om oplysninger	✓	✓			
SF03 - Vurdering af leverandørernes risikoprofil og anvendelse af restriktioner over for leverandører, der vurderes at udgøre en høj risiko - herunder nødvendige udelukkelser for effektivt at begrænse risiciene - i forbindelse med centrale aktiver	✓	✓			
SF04 - Kontrol med brugen af tjenesteudbydere og udstyrsleverandørers tredjelinjesupport	✓	✓			
SF05 - Sikring af de enkelte mobilnetoperatørers leverandørdiversificering gennem hensigtsmæssige flerleverandørstrategier	✓	✓			
SF06 - Styrkelse af modstandsdygtigheden på nationalt plan	✓	✓			
SF07 - Identifikation af centrale aktiver og fremme af et diversificeret og bæredygtigt 5G-økosystem i EU	✓		✓		
SF08 - Opretholdelse og opbygning af diversificering og EU-kapacitet i fremtidige netteknologier	✓		✓		✓
Tekniske foranstaltninger					
TF01 - Sikring af, at der anvendes grundlæggende sikkerhedskrav (sikkert netdesign og sikker netarkitektur)	✓	✓			
TF02 - Sikring og evaluering af gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder	✓	✓			✓

Foranstaltninger	Relevante aktører				
	Medlems-staternes myndigheder	Mobilnet-operatører	Europa-Kommissionen	ENISA	Interessenter (inkl. leverandører)
TF03 - Sikring af strenge adgangskontroller	✓	✓			
TF04 - Forøgelse af sikkerheden af virtualiserede netfunktioner	✓	✓			
TF05 - Sikring af sikker styring, drift og overvågning af 5G-net	✓	✓			
TF06 - Styrkelse af den fysiske sikkerhed	✓	✓			
TF07 - Styrkelse af softwareintegritet og -opdatering samt styring af rettelser	✓	✓			
TF08 - Forbedring af sikkerhedsstandarderne i leverandørernes processer gennem robuste indkøbsbetingelser	✓	✓			✓
TF09 - Anvendelse af EU-certificering for 5G-netkomponenter, kundeudstyr og/eller leverandørers processer	✓	✓	✓	✓	✓
TF10 - Anvendelse af EU-certificering for andre ikke-5G-specifikke IKT-produkter og -tjenester (tilsluttede enheder og cloudtjenester)	✓		✓	✓	✓
TF11 - Styrkelse af planer for modstandsdygtighed og kontinuitet	✓	✓			✓
Støttetiltag					
ST01 - Revision eller udarbejdelse af retningslinjer og bedste praksis for netsikkerhed	✓	✓		✓	
ST02 - Styrkelse af test- og auditkapaciteten på nationalt plan og EU-plan	✓		✓	✓	
ST03 - Støtte til og udformning af 5G-standarder	✓	✓	✓	✓	✓
ST04 - Udvikling af retningslinjer for gennemførelsen af sikkerhedsforanstaltninger i eksisterende 5G-standarder	✓			✓	
ST05 - Sikring af, at der anvendes tekniske og organisatoriske standardsikkerhedsforanstaltninger gennem en specifik EU-certificeringsordning	✓			✓	✓
ST06 - Udveksling af bedste praksis for gennemførelsen af strategiske foranstaltninger, navnlig nationale rammer for vurdering af leverandørernes risikoprofil	✓				
ST07 - Forbedring af koordineringen af beredskabs- og krisestyring	✓			✓	

Foranstaltninger	Relevante aktører				
	Medlems-staternes myndigheder	Mobilnet-operatører	Europa-Kommissionen	ENISA	Interessenter (inkl. leverandører)
ST08 - Gennemførelse af audit af indbyrdes afhængighed mellem 5G-net og andre kritiske tjenester	✓				
ST09 - Styrkelse af mekanismerne for samarbejde, koordinering og informationsudveksling	✓			✓	
ST10 - Sikring af 5G-projekter, der modtager offentlig støtte, under hensyntagen til cybersikkerhedsrisici	✓		✓		

Kilde: EU-værktøjskassen til 5G-cybersikkerhed.

Akronymer og forkortelser

BEREC: Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation

BNP: Bruttonationalprodukt

EECC: Den europæiske kodeks for elektronisk kommunikation

EFRU: Den Europæiske Fond for Regionaludvikling

EFSI: Den Europæiske Fond for Strategiske Investeringer

EIB: Den Europæiske Investeringsbank

ENISA: Den Europæiske Unions Agentur for Net- og Informationssikkerhed

NIS: Net- og informationssystem

RAN: Radio Access Network

Glossar

Bredbånd: Simultan højhastighedstransmission af forskellige informationstyper (f.eks. data, tale og video).

Den Europæiske Fond for Strategiske Investeringer: En mekanisme til investeringsstøtte lanceret af Den Europæiske Investeringsbank (EIB) og Kommissionen som led i investeringsplanen for Europa med det formål at mobilisere private investeringer i projekter af strategisk betydning for EU.

Den Europæiske Unions Agentur for Cybersikkerhed: Et EU-agentur, der er oprettet med henblik på at udvikle og opretholde et højt niveau af net- og informationssikkerhed på alle områder i det private og offentlige liv.

Exabyte: Et mål for digital lagringskapacitet svarende til 1 milliard gigabyte.

Frekvenspolitikgruppen: Rådgivende gruppe på højt plan, der består af repræsentanter for medlemsstaterne, og som bistår og rådgiver EU-institutionerne om udviklingen af det indre marked for trådløse produkter og tjenester.

Global System for Mobile Communications Association (GSMA): En brancheorganisation, der repræsenterer mobiloperatører i hele verden samt produktions- og servicevirksomheder og -organisationer med en interesse i mobilinfrastruktur.

Latenstid: I computernet den tid, det tager et sæt data at rejse mellem to punkter.

Mobilnetoperatør: Et teleselskab, der leverer trådløs tale- og datakommunikation til mobiltelefonbrugere med abonnement.

Nationale bredbåndsplaner: Medlemsstaternes dokumenter med strategiske mål for opfyldelse af EU's bredbåndsmål.

Radio Access Network: Et væsentligt element i moderne telekommunikationsteknologi, som forbinder enheder med andre dele af et net via radioforbindelser.

Radiofrekvenser: Den del af det elektromagnetiske spektrum, der består af radiofrekvenser.

Ransomware: Malware, der nægter offeret adgang til et computersystem eller gør datafilerne ulæselige med det formål at tvinge offeret til at betale en løsesum for genetablering af adgangen.

Samarbejdsgruppen for net- og informationssystemer (NIS-samarbejdsgruppen): NIS-samarbejdsgruppen blev oprettet ved NIS-direktivet med henblik på at sikre samarbejde og informationsudveksling mellem medlemsstaterne og består af repræsentanter for EU-medlemsstaterne, Europa-Kommissionen og EU's Agentur for Cybersikkerhed.

Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation: Et organ bestående af repræsentanter for medlemsstaternes nationale tilsynsmyndigheder, som bistår disse myndigheder og Kommissionen ved gennemførelsen af EU's retlige ramme med henblik på at skabe et indre marked for elektronisk kommunikation.

Tingenes internet: Fysiske objekter med indbyggede sensorer, software og andre teknologier, som sætter dem i stand til trådløst at forbinde sig og udveksle data med andre enheder og systemer.

Kommissionens svar

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

Tidsplan

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

Revisionsholdet

Revisionsrettens særberetninger præsenterer resultaterne af dens revisioner vedrørende EU-politikker og -programmer eller forvaltningsspørgsmål i forbindelse med specifikke budgetområder. Med henblik på at opnå maksimal effekt udvælger og udarbejder Revisionsretten sine revisionsopgaver under hensyntagen til de risici, der knytter sig til forvaltningens resultatopnåelse eller regeloverholdelsen, de pågældende indtægters eller udgifters omfang, den fremtidige udvikling samt den politiske og offentlige interesse.

Denne forvaltningsrevision blev udført af Revisionsafdeling II - Investering i samhørighed, vækst og inklusion, der ledes af Iliana Ivanova, medlem af Revisionsretten. Revisionsarbejdet blev ledet af Annemie Turtelboom, medlem af Revisionsretten, med støtte fra kabinetschef Florence Fornaroli, attaché Celil Ishik, ledende administrator Niels-Erik Brokopp, opgaveansvarlig Paolo Pesce og revisorerne Jussi Bright, Rafal Gorajski, Zuzana Gullová, Alexandre Tan, Aleksandar Latinov og Nils Westphal.

Annemie Turtelboom

Florence Fornaroli

Celil Ishik

Niels-Erik Brokopp

Paolo Pesce

Jussi Bright

Rafal Gorajski

Zuzana Gullová

Aleksandar Latinov

Nils Westphal

PDF	ISBN 978-92-847-7405-0	ISSN 1977-5636	doi:10.2865/81	QJ-AB-21-029-DA-N
HTML	ISBN 978-92-847-7377-0	ISSN 1977-5636	doi:10.2865/54704	QJ-AB-21-029-DA-Q

5G forventes at ville øge det europæiske BNP med op til 1 billion euro mellem 2021 og 2025 og have potentiale til at skabe eller omdanne op til 20 millioner arbejdsspladser i alle sektorer af økonomien. Vi konstaterede, at forsinkelser betyder, at EU's mål for 5G-udrulning måske ikke kan nås, og at der er behov for en yderligere indsats for at håndtere sikkerhedsspørgsmål. I denne beretning fremsætter vi en række anbefalinger til Kommissionen med henblik på at fremme en rettidig og samordnet implementering af sikre 5G-net i EU.

Særberetning fra Revisionsretten udarbejdet i medfør af artikel 287, stk. 4, andet afsnit, TEUF.

DEN EUROPÆISKE REVISIONSRET

Den Europæiske Unions Publikationskontor

DEN EUROPÆISKE REVISIONSRET
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tlf. +352 4398-1

Kontakt: eca.europa.eu/da/Pages/ContactForm.aspx
Websted: eca.europa.eu
Twitter: @EUAuditors