

Posebno poročilo

Uvajanje omrežij 5G v EU:

zamude pri uvajanju omrežij in varnostna
vprašanja, ki ostajajo nerešena



EVROPSKO
RAČUNSKO
SODIŠČE

Vsebina

	Odstavek
Povzetek	I–IX
Uvod	01–16
Narava in pomembnost 5G	01–03
Pomisleki glede varnosti	04–07
Pobude 5G, sprejete na ravni EU	08
Vloge in odgovornosti	09–10
Stroški uvajanja omrežij 5G in s tem povezana finančna podpora EU	11–16
Skupni stroški uvajanja omrežij 5G v vseh državah članicah bi lahko znašali do 400 milijard EUR	11
V obdobju 2014–2020 je EU razvoj 5G podprla z več kot 4 milijardami EUR	12–15
Z mehanizmom za okrevanje in odpornost bo zagotovljeno dodatno financiranje EU za uvajanje omrežij 5G v naslednjih letih	16
Obseg revizije in revizijski pristop	17–20
Opažanja	21–80
Zaradi zamud pri uvajanju omrežij 5G je ogroženo doseganje ciljev EU do leta 2025 in 2030	21–43
Pri uvajanju omrežij 5G v državah članicah prihaja do zamud	22–27
Pri podpori, ki jo je Komisija zagotovila državam članicam, so bile nekatere pomanjkljivosti	28–33
Države članice morajo še vedno odstraniti ključne ovire za hitro uvajanje omrežij 5G	34–43
Za obravnavanje varnostnih vprašanj pri uvajanju omrežij 5G so potrebna nadaljnja prizadevanja	44–80
Ko je varnost omrežij 5G postala pomembno vprašanje na ravni EU, se je Komisija hitro odzvala	45–47
Z naborom orodij EU za kibernetško varnost tehnologije 5G iz leta 2020 so bili prvič oblikovani ukrepi za obravnavo groženj za varnost na ravni EU, ki pa niso predpisovalni	48–67

Države članice pri uvajanju omrežij 5G varnostnih vidikov še ne obravnavajo usklajeno	68–80
--	-------

Zaključki in priporočila	81–93
---------------------------------	--------------

Priloge

Priloga I – Glavne priložnosti in tveganja v zvezi s 5G

**Priloga II – Primeri posledic motenj telekomunikacijskih omrežij
in kibernetских incidentov**

Priloga III – Pravni okvir in okvir politik

Priloga IV – Primeri projektov, sofinanciranih iz sklada EFSI

Priloga V – Primeri projektov programa Obzorje 2020 in ESRR

Priloga VI – Pokritost 5G v izbranih mestih

**Priloga VII – Nabor orodij EU za kibernetisko varnost tehnologije
5G**

Kratice

Glosar

Odgovori Komisije

Časovni okvir

Revizijska ekipa

Povzetek

I Peta generacija telekomunikacijskih sistemov (5G) je novi svetovni brezžični standard, ki ima veliko večjo podatkovno zmogljivost in hitrost prenosa. Storitve 5G so bistvene za najrazličnejše inovativne načine uporabe, s katerimi se lahko preobrazijo številni sektorji naših gospodarstev in izboljša vsakdanje življenje državljanov, zato je 5G strateško pomemben za celotni enotni trg.

II Komisija je v svojem akcijskem načrtu za 5G iz leta 2016 predstavila cilj, da bodo imela mestna področja in glavne prometne poti neprekinjeno pokritost 5G do leta 2025. Marca 2021 je cilj razširila na pokritost vseh naseljenih območij z omrežji 5G do leta 2030.

III Tehnologija 5G ima sicer potencial, da omogoči številne priložnosti za rast, vendar so z njo povezana tudi tveganja. Komisija je v priporočilu o kibernetiski varnosti omrežij 5G, ki ga je dala leta 2019, opozorila, da bi bile zaradi odvisnosti številnih kritičnih storitev od omrežij 5G posledice močno razširjene motnje še posebej resne. Poleg tega čezmejna narava s tem povezanih groženj pomeni, da bi morebitne pomembne šibke točke ali kibernetiski incidenti v eni državi članici vplivali na EU kot celoto. Eden od izidov priporočila Komisije je nabor orodij EU za kibernetisko varnost tehnologije 5G (nabor orodij), ki je bil sprejet januarja 2020.

IV Skupni stroški uvajanja omrežij 5G v celotni EU bi lahko dosegli 400 milijard EUR. V obdobju 2014–2020 je EU za projekte v zvezi z omrežji 5G zagotovila financiranje v višini več kot 4 milijard EUR.

V Sodišče je preučilo, ali je Komisija uspešno podpirala države članice pri doseganju ciljev EU glede uvajanja omrežij 5G v njih in obravnavi varnostnih pomislekov v zvezi s 5G na usklajen način. Sodišče je preučilo vidike v zvezi z uvajanjem omrežij 5G, za katerega je bilo ključno leto 2020, ter njihovo varnostjo. Namen tega poročila je zagotoviti uvide in priporočila za pravočasno uvajanje varnih omrežij 5G v vseh državah članicah EU. Revizija je bila osredotočena na Komisijo, vendar je Sodišče preučilo tudi vlogo nacionalnih uprav in drugih akterjev.

VI Iz revizije Sodišča je razvidno, da pri uvajanju omrežij 5G v državah članicah prihaja do zamud. Do konca leta 2020 je 23 držav članic uvedlo komercialne storitve 5G in doseglo vmesni cilj, da ima do omrežij 5G dostop vsaj eno veliko mesto. Vendar se nekatere države članice v svojih nacionalnih strategijah za 5G ali načrtih za širokopasovne povezave ne sklicujejo na cilja EU za leti 2025 in 2030. Poleg tega več držav še ni preneslo Evropskega zakonika o elektronskih komunikacijah v nacionalno zakonodajo, pri dodelitvi spektra 5G pa je prišlo do zamud. Zamude pri dodelitvi spektra je mogoče pripisati različnim razlogom, in sicer slabemu povpraševanju operaterjev mobilnih omrežij, težavam pri čezmejnem usklajevanju z državami nečlanicami EU ob vzhodnih mejah, vplivu COVID-19 na časovne načrte dražb in negotovosti glede obravnave varnostnih vprašanj. Države članice pri uvajanju omrežij 5G zaostajajo v tolikšnem obsegu, da je ogroženo doseganje ciljev EU. Komisija je države članice pri izvajanju akcijskega načrta za 5G iz leta 2016 podpirala s pobudami trdega in mehkega prava, smernicami ter financiranjem raziskav, povezanih s 5G. Vendar Komisija ni jasno opredelila pričakovane kakovosti storitev 5G.

VII V okviru nabora orodij EU za kibernetско varnost tehnologije 5G so navedeni številni strateški, tehnični in podporni ukrepi za obravnavo groženj za varnost omrežij 5G, za vsakega od njih pa so opredeljeni tudi ustrezni akterji. Več ukrepov zadeva vprašanje visoko tveganih dobaviteljev opreme 5G. Ta nabor orodij sta odobrila Komisija in Evropski svet. Z merili iz nabora orodij je zagotovljen operativni okvir, ki je koristen za usklajeno ocenjevanje profila tveganja dobaviteljev v vseh državah članicah, hkrati pa je izvajanje te ocene še vedno v nacionalni pristojnosti. Nabor orodij je bil sicer sprejet v zgodnji fazi uvajanja omrežij 5G, vendar je več operaterjev mobilnih omrežij takrat že izbralo svoje dobavitelje. Od sprejetja nabora orodij je bil dosežen napredek pri krepitevi varnosti omrežij 5G, saj večina držav članic uporablja omejitve za visoko tvegane dobavitelje ali to namerava storiti. V prihodnjih letih bi lahko zakonodaja o varnosti omrežij 5G, ki bi jo na podlagi nabora orodij sprejele države članice, privedla do bolj usklajenih pristopov k visoko tveganim dobaviteljem 5G. Ker pa nobeden od predlaganih ukrepov ni pravno zavezujoč, Komisija nima pooblastil za njihovo izvrševanje. Zato obstaja tveganje, da zgolj z naborom orodij ne bo mogoče zagotoviti, da bi države članice varnostne vidike omrežij obravnavale usklajeno.

VIII Komisija je že začela obravnavati vprašanje tujih subvencij za dobavitelje 5G, ki lahko vplivajo na varnost, Komisija nima dovolj informacij glede tega, kako bi države članice obravnavale morebitne stroške nadomestitve, ki bi lahko nastali, če bi morali operaterji mobilnih omrežij brez prehodnega obdobja odstraniti opremo visoko tveganih dobaviteljev iz omrežij EU.

IX Sodišče priporoča, naj Komisija:

- spodbuja enakomerno in pravočasno uvajanje omrežij 5G v EU,
- spodbuja usklajen pristop držav članic k varnosti 5G in
- spremlja pristope držav članic k varnosti 5G in oceni učinek različnih pristopov na uspešno delovanje enotnega trga.

Uvod

Narava in pomembnost 5G

01 Peta generacija telekomunikacijskih sistemov (5G) je novi svetovni brezžični standard, ki ima v primerjavi z omrežji 3G in 4G veliko večjo podatkovno zmogljivost in hitrost prenosa. 5G vključuje nekatere omrežne elemente, ki temeljijo na prejšnjih generacijah mobilne in brezžične komunikacijske tehnologije, vendar ni naslednja stopnja v razvoju teh omrežij. Z njim je posameznim uporabnikom in povezanim napravam zagotovljena univerzalna in izredno širokopasovna povezljivost z nizko latenco (zakasnitvijo).

02 5G bo v internet stvari povezal največ naprav doslej. Po ocenah je bilo do konca leta 2018 po vsem svetu v uporabi 22 milijard povezanih naprav. To število se bo po napovedih do leta 2030 povečalo na okoli 50 milijard¹, tako da bo nastala obsežna mreža med sabo povezanih naprav, in sicer vse od pametnih telefonov do kuhinjskih aparatov. Svetovni mobilni podatkovni promet, ki je leta 2017 znašal 12 eksabajtov na mesec², se bo do leta 2030 po pričakovanjih povečal na več kot 5 000 eksabajtov³.

03 Storitve 5G so bistvene za najrazličnejše inovativne načine uporabe, s katerimi se lahko preobrazijo številni sektorji gospodarstva EU in izboljša vsakdanje življenje državljanov (glej [slika 1](#)). V študiji, ki je bila leta 2017 izvedena za Komisijo, se je pokazalo, da lahko koristi uvajanja 5G v štirih ključnih strateških industrijskih sektorjih (avtomobilskem, zdravstvenem, prometnem in energetske) znašajo do 113 milijard EUR na leto⁴. Po pričakovanjih iz študije bi se lahko z uvajanjem 5G ustvarilo tudi 2,3 milijona delovnih mest v državah članicah. Po ocenah iz študije iz leta 2021 bi se zaradi 5G evropski bruto domači proizvod (BDP) med letoma 2021 in

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.

2025 povečal za do 1 bilijon EUR, s potencialom za nastanek ali preobrazbo do 20 milijonov delovnih mest v vseh gospodarskih sektorjih⁵.

Slika 1 – Tehnologija 5G bo pokrivala vse vidike našega življenja



Vir: Evropska komisija

Pomisliki glede varnosti

04 Tehnologija 5G ima sicer potencial, da omogoči številne priložnosti za rast, vendar so z njo povezana tudi nekatera tveganja (glej [Prilogo I](#), v kateri so navedene glavne priložnosti in tveganja 5G). Eno od teh tveganj so grožnje za varnost. Telekomunikacijski sistemi so že od nekdaj ogroženi zaradi kibernetских napadov (glej [Prilogo II](#))⁶. Posebej zaskrbljujoča v zvezi s 5G so varnostna vprašanja, ker je 5G zaradi vrste tehnologije in zlasti svoje odvisnosti od programske opreme bolj dovzeten za napade kot telekomunikacijski sistemi 3G in 4G⁷.

05 Ker naj bi omrežja 5G postala temelj za najrazličnejše storitve in načine uporabe, bo njihova dostopnost velik varnostni izziv na nacionalni ravni in ravni EU. Če bi v katerega od omrežij 5G vdrla hekerji, bi lahko ogrozili njegove osnovne funkcije in s tem povzročili motnje v storitvah ali prevzeli nadzor nad kritično infrastrukturo (na primer

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

⁶ Pregled št. 02/2019: Izzivi za uspešno politiko EU za kibernetško varnost (informativni dokument); kompendij revizijskih poročil Odbora za stike iz leta 2020 – Kibernetška varnost v EU in njenih državah članicah in Evropsko vozlišče za znanstvene medije, ki ga upravlja služba Evropskega parlamenta za raziskave.

⁷ Skupina za sodelovanje na področju varnosti omrežij in informacij, *EU coordinated risk assessment of the cybersecurity of 5G networks*, 9. oktober 2019, točka 3.4.

energetskimi omrežji), ki ima v EU pogosto čezmejno razsežnost. Po ocenah v študijah bi lahko ekonomski učinek kibernetске kriminalitete znašal do 5 000 milijard EUR letno, kar je več kot 6 % svetovnega BDP v letu 2020⁸.

06 Še en varnostni izziv, povezan s 5G, je kritična vloga omejenega števila dobaviteljev pri gradnji in delovanju omrežij 5G. To v primeru odvisnosti od enega samega dobavitelja povečuje izpostavljenost morebitnim motnjam v dobavi – zlasti če ta dobavitelj pomeni visoko tveganje – na primer, če je pod vplivom tretje države. Skupina za sodelovanje na področju varnosti omrežij in informacij, ki jo sestavljajo predstavniki držav članic in organov EU, je leta 2019 opozorila na tveganje, da bi si lahko sovražni državni akterji zagotovili preprost dostop do enega od omrežij 5G, in sicer s privilegiranim dostopom, izvajanjem pritiska na dobavitelja ali sklicevanjem na nacionalne pravne zahteve⁹ (glej **okvir 1**). V tem okviru je začela EU razvijati pobude na področju varnosti 5G.

Okvir 1

Pomisliki glede varnosti v zvezi s sodelovanjem EU in Kitajske na področju 5G

- o EU je leta 2015 s Kitajsko podpisala skupno izjavo o strateškem sodelovanju na področju 5G, s katero sta se zavezali k vzajemnosti in odprtosti pri dostopu do financiranja raziskav o omrežjih 5G in trga¹⁰.
- o Kitajska je leta 2017 sprejela zakon o državnih obveščevalnih dejavnostih, v skladu s katerim morajo vse kitajske organizacije in državljani sodelovati z nacionalno obveščevalno službo in o tem ohraniti tajnost¹¹. V odziv so ZDA leta 2018 sprejele ukrepe za omejitev operacij več kitajskih družb, vključno z družbo Huawei, ki je eden od ključnih dobaviteljev 5G.

⁸ Svetovni gospodarski forum, *Wild Wide Web – Consequences of Digital Fragmentation*, 2021.

⁹ Skupina za sodelovanje na področju varnosti omrežij in informacij, *EU coordinated risk assessment of the cybersecurity of 5G networks*, 9. oktober 2019.

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

¹¹ Resolucija Evropskega parlamenta z dne 12. marca 2019; zakon Ljudske republike Kitajske o državnih obveščevalnih dejavnostih, člen 14. Glej tudi angleški prevod zakona na naslovu <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>.

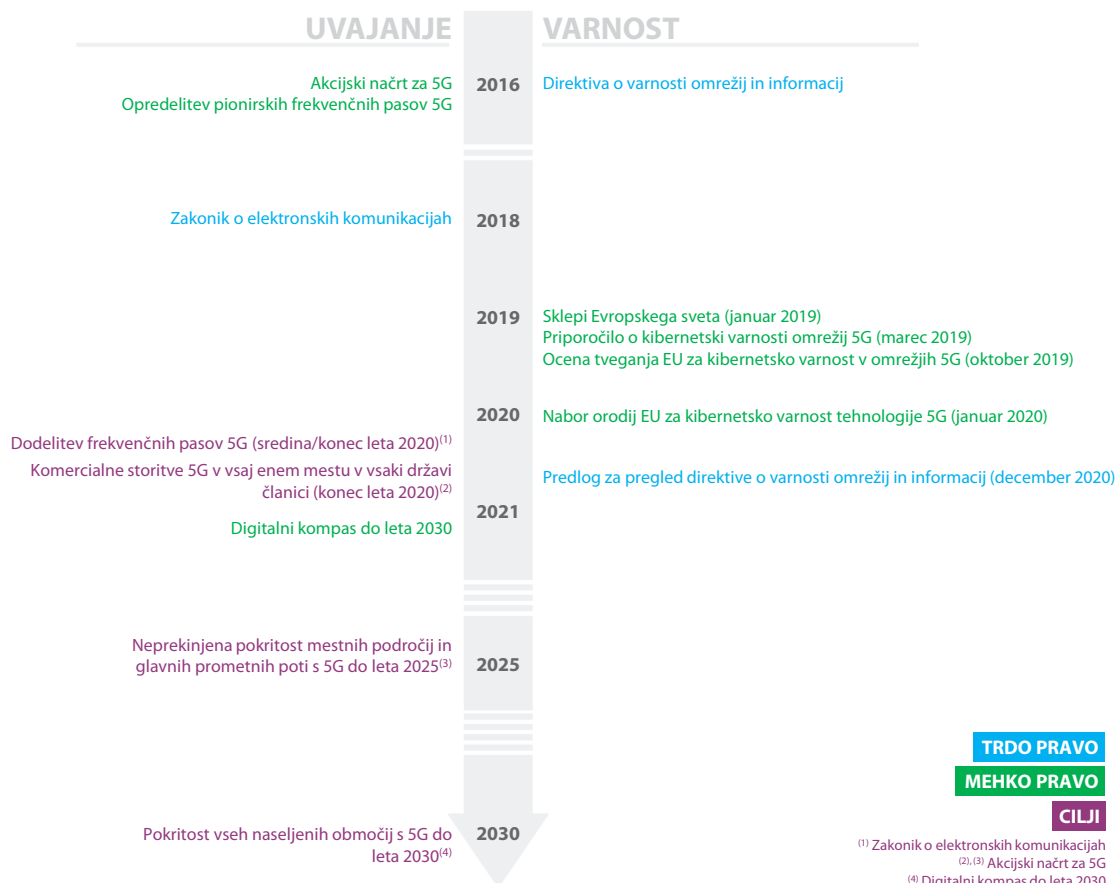
Marca 2019 je tudi Evropski parlament izrazil pomisleke glede tega, da bi lahko kitajski dobavitelji 5G zaradi zakonov v svoji matični državi pomenili varnostno tveganje za EU.

07 Ogroženi sta lahko tudi zaupnost in zasebnost, saj telekomunikacijski operaterji svoje podatke pogosto prenesejo v zunanje podatkovne centre. Obstaja tveganje, da bi bili ti podatki shranjeni na napravah dobaviteljev 5G v državah nečlanicah EU, ki imajo drugačne ravni pravnega varstva in varstva podatkov kot EU.

Pobude 5G, sprejete na ravni EU

08 Okvir politike, povezan s 5G in njegovo varnostjo, sestavljata trdo pravo, ki je pravno zavezujoče in izvršljivo (na primer uredbe), in mehko pravo, ki ni zavezujoče (na primer sporočila Komisije). V *Prilogi III* sta predstavljena pravni okvir in okvir politike. Na *sliki 2* so glavni dokumenti politike in ključni cilji.

Slika 2 – Glavni dokumenti politike in ključni cilji, povezani z uvajanjem in varnostjo omrežij 5G



Vir: Evropsko računsko sodišče

Vloge in odgovornosti

09 Za varno uvajanje omrežij 5G z opremo, pridobljeno od tehnoloških dobaviteljev, so sicer odgovorni operaterji mobilnih omrežij, za nacionalno varnost pa države članice, vendar je varnost omrežij 5G strateško pomembno vprašanje za celotni enotni trg in tehnološko suverenost EU¹². Pri tehničnih in varnostnih vidikih omrežij 5G zato ukrepe držav članic podpirajo in usklajujejo Komisija in agencije EU.

10 V **tabeli 1** so nadalje pojasnjene glavne vloge in odgovornosti na področju omrežij 5G.

Tabela 1 – Vloge in odgovornosti

	Komisija in agencije EU	Organi držav članic	Operaterji mobilnih omrežij in dobavitelji 5G
Razporeditev in dodelitev pionirskih frekvenčnih pasov 5G		✓	
Opredelitev politike EU za 5G	✓	✓	
Uvajanje omrežij 5G			✓
Naložbe in financiranje	✓	✓	✓
Nacionalna varnost		✓	
Varnost omrežij 5G		✓	✓
Podpora in usklajevanje ukrepov držav članic	✓		

Vir: Evropsko računsko sodišče

Stroški uvajanja omrežij 5G in s tem povezana finančna podpora EU

Skupni stroški uvajanja omrežij 5G v vseh državah članicah bi lahko znašali do 400 milijard EUR

11 Leta 2021 je bilo ocenjeno, da bodo skupni stroški uvajanja omrežij 5G v vseh državah članicah EU do leta 2025 znašali med 281 milijardami EUR in 391 milijardami EUR, kar je enakomerno porazdeljeno med gradnjo nove

¹² https://ec.europa.eu/commission/presscorner/detail/sl/IP_20_12.

infrastrukture 5G in nadgradnjo fiksne infrastrukture na gigabitne hitrosti¹³. Večino teh naložb morajo financirati operaterji mobilnih omrežij.

V obdobju 2014–2020 je EU razvoj 5G podprla z več kot 4 milijardami EUR

12 V obdobju 2014–2020 je EU razvoj 5G podprla z več kot 4 milijardami EUR, in sicer neposredno iz proračuna EU in s financiranjem Evropske investicijske banke (EIB). Iz proračuna EU so se financirali projekti, povezani izključno z raziskavami, s sredstvi EIB pa so se podpirali raziskave in uvajanje.

13 EIB prispeva največ financiranja EU za projekte, povezane s 5G. Do avgusta 2021 je zagotovila posojila v skupni vrednosti 2,5 milijarde EUR za devet projektov 5G v petih državah članicah¹⁴, v proračunu EU pa je bilo za obdobje 2014–2020 na voljo 1,9 milijarde EUR. V **tabeli 2** so povzeti glavni viri finančne podpore, ki jo je EU namenila za 5G.

Tabela 2 – Financiranje EU za 5G (2014–2020)

Financiranje EU	Znesek
EIB	2,485 milijarde EUR ¹
Evropski sklad za strateške naložbe (EFSI)	1 milijarda EUR ²
Obzorje 2020	755 milijonov EUR ³
ESRR	vsaj 147 milijonov EUR ⁴

(1) [Seznam projektov EIB.](#)

(2) [Seznam projektov sklada EFSI.](#)

(3) [Podatkovni portal programa Obzorje 2020.](#)

(4) [Nabor podatkov o projektih, sofinanciranih iz ESRR med obdobjem večletnega finančnega okvira 2014–2020.](#)

Vir: Evropsko računsko sodišče

¹³ Ocena Komisije na podlagi podatkov EIB, Analysys, združenja GSMA in sporočil podjetij ter Združenja evropskih operaterjev telekomunikacijskih omrežij ETNO, *Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All*, marec 2021.

¹⁴ [Seznam projektov EIB.](#)

14 S skladom EFSI (ki ga upravlja EIB) sta bila podprta dva projekta, namenjena gostejši postavitvi celic in podpiranju standardizacije. Skupni stroški naložb za ta projekta so znašali 3,9 milijarde EUR, vključno s financiranjem iz sklada EFSI v višini 1 milijarde EUR (glej *Prilogo IV*).

15 Komisija je od leta 2014 tudi neposredno sofinancirala več kot 100 projektov s področja 5G, in sicer s sredstvi iz programa Obzorje 2020, v manjši meri pa tudi iz ESRR. Primeri teh projektov so navedeni v *Prilogi V*.

Z mehanizmom za okrevanje in odpornost bo zagotovljeno dodatno financiranje EU za uvajanje omrežij 5G v naslednjih letih

16 Z mehanizmom za okrevanje in odpornost bo zagotovljen dopolnilen vir financiranja EU za uvajanje omrežij 5G v naslednjih letih. Po podatkih iz septembra 2021 je uvajanje omrežij 5G z mehanizmom za okrevanje in odpornost nameravalo financirati 16 držav članic, deset pa se jih za to ni odločilo. Informacije iz preostale države članice še niso bile na voljo.

Obseg revizije in revizijski pristop

17 Sodišče je s to revizijo ocenilo, ali Komisija države članice uspešno podpira pri:

- doseganju ciljev EU glede uvajanja omrežij 5G v državah članicah do leta 2025 in 2030 ter
- usklajenem obravnavanju pomislekov glede varnosti 5G.

Na teh področjih je Sodišče preučilo tudi ukrepe in dejavnosti držav članic.

18 Izraz varnost 5G se v tem poročilu nanaša na kibernetско varnost in varnost strojne/programske opreme. Sodišče je preučilo varnost in uvajanje omrežij 5G, za kar je bilo leto 2020 ključno (glej [sliko 2](#)). Namen tega poročila je zagotoviti uvide in priporočila za pravočasno uvajanje varnih omrežij 5G v EU.

19 Revizija zajema obdobje od leta 2016 do maja 2021. Kolikor je bilo mogoče, so vključene tudi dodatne najnovejše informacije. Sodišče je v okviru svojega revizijskega dela:

- pregledalo zakonodajo EU, pobude Komisije in drugo ustrezno dokumentacijo,
- opravilo razgovore s predstavniki Komisije, EIB, Organa evropskih regulatorjev za elektronske komunikacije (BEREC), Agencije Evropske unije za varnost omrežij in informacij (ENISA), združenj za telekomunikacije, operaterjev mobilnih omrežij, dobaviteljev 5G in mednarodnih organizacij ter s strokovnjaki na terenu, da bi pridobilo uvide, pa tudi s predstavniki organov na Finskem, v Nemčiji, na Poljskem in v Španiji. Države članice so bile izbrane na podlagi meril, kot je znesek sredstev EU, namenjenih za projekte 5G, in stanje uvajanja omrežij 5G, ter ob upoštevanju geografske uravnoteženosti,
- izvedlo anketo med vsemi 27 nacionalnimi regulativnimi organi za telekomunikacije v EU, da bi pridobilo širši pregled nad izzivi v zvezi s 5G v državah članicah, in
- pregledalo deset projektov v zvezi s 5G, ki jih je sofinancirala EU (sklad EFSI, ESRR in Obzorje 2020), izbranih za ponazoritev.

20 Poleg tega se je Sodišče oprlo tudi na svoj nedavni pregled odziva EU na državno vodeno naložbeno strategijo Kitajske¹⁵ ter druga poročila, npr. o širokopasovnih povezavah¹⁶, pobudi za digitalizacijo evropske industrije¹⁷ in politiki EU za kibernetško varnost¹⁸.

¹⁵ Pregled št. 03/2020: Odziv EU na državno vodeno naložbeno strategijo Kitajske.

¹⁶ Posebno poročilo št. 12/2018: Širokopasovne povezave v državah članicah EU: kljub napredku vsi cilji strategije Evropa 2020 ne bodo doseženi.

¹⁷ Posebno poročilo 19/2020: Digitalizacija evropske industrije: ambiciozna pobuda, katere uspeh je odvisen od stalne zavezanosti EU, vlad in podjetij.

¹⁸ Pregled št. 02/2019: Izzivi za uspešno politiko EU za kibernetško varnost (informativni dokument).

Opažanja

Zaradi zamud pri uvajanju omrežij 5G je ogroženo doseganje ciljev EU do leta 2025 in 2030

21 V zvezi s pravočasnim uvajanjem omrežij 5G je Sodišče preučilo, ali:

- so države članice pri uvajanju omrežij 5G na dobri poti,
- je Komisija državam članicam zagotovila ustrezno podporo,
- so države članice odstranile ključne ovire za hitro uvajanje omrežij 5G.

Pri uvajanju omrežij 5G v državah članicah prihaja do zamud

Komisija je roke za uvajanje omrežij 5G določila v svojem akcijskem načrtu za 5G iz leta 2016

22 Komisija je v svojem akcijskem načrtu za 5G iz leta 2016 predlagala roke za uvajanje omrežij 5G v EU, in sicer bi morale države članice zgodnja omrežja 5G vzpostaviti do konca leta 2018, popolnoma komercialne storitve 5G v vsaj enem velikem mestu do konca leta 2020, neprekinjeno pokritost mestnih področij in glavnih prometnih poti s 5G pa do leta 2025.

23 Marca 2021 je dodala še rok za pokritost vseh naseljenih območij z omrežji 5G do leta 2030¹⁹.

Do konca leta 2020 je komercialne storitve 5G uvedlo 23 držav članic

24 Do konca leta 2020 je cilj glede dostopa do storitev 5G v vsaj enem velikem mestu doseglo 23 držav članic. Cilja niso dosegli samo Ciper, Litva, Malta in Portugalska. Konec oktobra 2021 storitev 5G v nobenem mestu nista imeli samo še Litva in Portugalska.

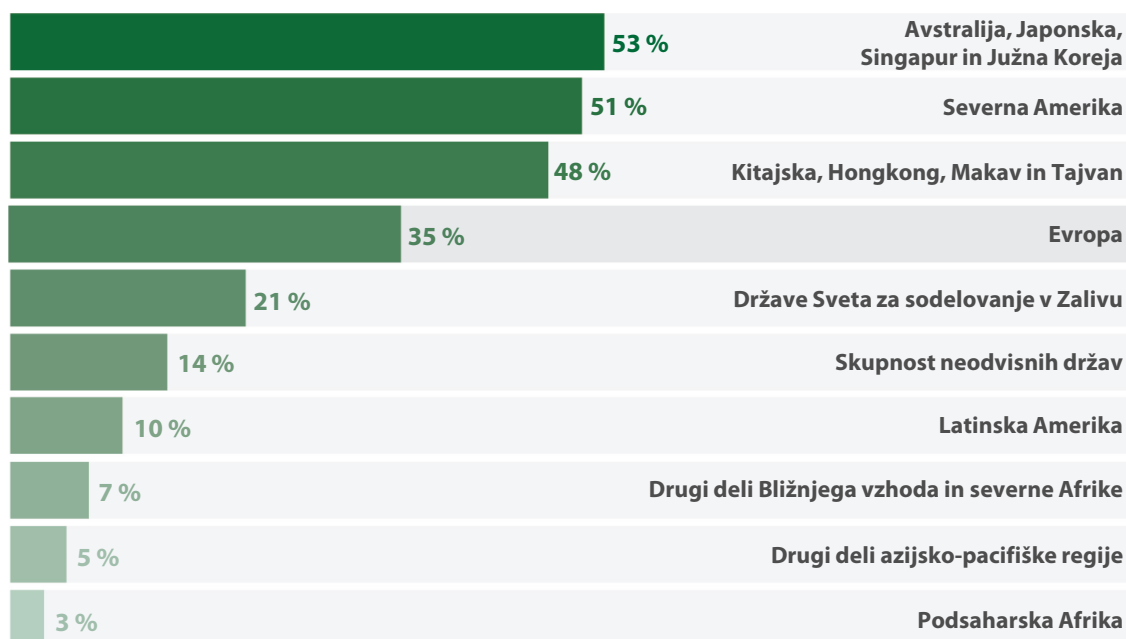
¹⁹ Evropska komisija, [Digitalni kompas do leta 2030: evropska pot v digitalno desetletje](#), COM(2021) 118 final.

Obstaja tveganje, da bo večina držav članic zamudila roka za leto 2025 in leto 2030

25 Pri nedavni študiji Komisije se je pokazalo, da bo neprekinjeno pokritost vseh mestnih področij in glavnih kopenskih prometnih poti s 5G do leta 2025 verjetno doseglo samo 11 držav članic²⁰. Za preostalih 16 držav članic Komisija meni, da je verjetnost, da bodo dosegle cilj, srednja (Avstrija, Češka, Estonija, Nemčija, Irska, Poljska, Litva in Slovenija) ali majhna (Belgija, Bolgarija, Hrvaška, Ciper in Grčija).

26 Panožna organizacija Global System for Mobile Communications Association (GSMA) je leta 2021 navedla, da uvajanje omrežij 5G v EU napreduje z drugačno hitrostjo kot drugje po svetu. Na primer, do leta 2025 naj bi po ocenah v Severni Ameriki na 5G temeljilo 51 % vseh mobilnih povezav, v Evropi (vključno z državami nečlanicami EU) pa samo 35 % (glej [slika 3](#)).

Slika 3 – Povezave 5G kot delež vseh mobilnih povezav do leta 2025



Vir: GSMA, *The Mobile Economy 2021*

27 Pri trenutni hitrosti uvajanja obstaja veliko tveganje, da roka za leto 2025 – in torej tudi roka za leto 2030 glede pokritosti vseh naseljenih območij – večina držav članic ne bo dosegla. Sodišče je glede na navedeno preučilo, ali je Komisija države članice uspešno podpirala pri doseganju ciljev EU za 5G za leti 2025 in 2030 na področju uvajanja omrežij 5G.

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

Pri podpori, ki jo je Komisija zagotovila državam članicam, so bile nekatere pomanjkljivosti

Komisija ni opredelila pričakovane kakovosti storitev omrežij 5G

28 Komisija doslej še ni opredelila pričakovane kakovosti storitev omrežij 5G, na primer glede minimalne hitrosti in maksimalne latence. Poleg tega je Komisija države članice v akcijskem načrtu iz leta 2016 pozvala, naj do konca leta 2020 v Evropi uvedejo popolnoma komercialne storitve 5G, vendar teh konceptov glede kakovosti ni opredelila.

29 Zaradi nejasnosti glede pričakovane kakovosti storitev obstaja tveganje, da si bodo države članice te pojme razlagale različno. Sodišče je odkrilo primere razlik v pristopih držav članic k uvajanju omrežij 5G (glej [okvir 2](#)).

Okvir 2

Primeri razlik pri pristopih k uvajanju omrežij 5G

Hitrost in latenca sta ključna vidika zmogljivosti storitev, za katere se uporablja 5G. Na primer, za kirurgijo na daljavo ali industrijsko avtomatizacijo prek omrežja 5G sta potrebni zelo velika hitrost in nizka latenca. Doslej sta zahteve glede najmanjše hitrosti in največje latence določili samo dve državi članici (Nemčija in Grčija)²¹.

Države članice si cilj, naj ima do konca leta 2020 vsaj eno veliko mesto v vsaki državi članici dostop do storitev 5G, razlagajo različno, zato za mesto z dostopom do storitev 5G veljata tako Luxembourg, kjer je pokritih le nekaj ulic, kot Helsinki, kjer je pokrito skoraj celotno mesto. V [Prilogi VI](#) so navedeni primeri pokritosti v izbranih mestih.

30 Če se bodo te razmere nadaljevale, lahko vodijo do neenakosti pri kakovosti storitev 5G v EU in dostopu do njih (digitalni razkorak), kar pomeni, da bi imeli ljudje v delu EU kakovostnejše storitve 5G in boljši dostop do njih kot drugi. Digitalni razkorak bi lahko vplival tudi na potencial za gospodarski razvoj, saj se lahko zaradi 5G sektorji, kot sta zdravstvo in izobraževanje, ter delovna sila korenito spremenijo samo, če bodo imela omrežja 5G ustrezno zmogljivost.

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

31 Jasnost glede pričakovane zmogljivosti omrežij 5G je potrebna tudi zaradi pobude Komisije za večjo transparentnost kakovosti storitev gostovanja, ki jih zagotavljajo operatorji mobilnih omrežij. O tem je Komisija nedavno predstavila zakonodajni predlog²².

Četrtletno poročanje Komisije o uvajanju omrežij 5G včasih ni zanesljivo

32 Komisija raven uvajanja omrežij 5G v državah članicah EU spremlja v okviru [opazovalnice 5G](#). Ta vsako četrletje zagotovi informacije o uvajanju omrežij 5G in strategijah držav članic za 5G, vendar je Sodišče ugotovilo, da za dve od štirih držav, vključenih v pregled, informacije v teh poročilih včasih niso zanesljive. Na primer, v četrtnem poročilu št. 10, ki vsebuje informacije do konca decembra 2020, je bilo navedeno število občin s 5G na Finskem veliko nižje od dejanskega (40 namesto 70), informacije o preložitvi dražbe spektra 5G na Poljskem pa niso bile vključene (glej odstavek [42](#)).

Komisija je šele nedavno izkoristila proces evropskega semestra za spremljanje napredka držav članic pri uvajanju omrežij 5G

33 Sodišče je ugotovilo, da je Komisija v zadnjih dveh letih bolj uporabljala proces evropskega semestra, da bi spodbudila napredek držav članic pri uvajanju omrežij 5G. Priporočila za posamezne države, neposredno povezana s 5G, so bila leta 2019 namenjena dvema državam članicama, leta 2020 pa že sedmim (glej [slika 4](#)).

²² Evropska komisija, [predlog uredbe Evropskega parlamenta in Sveta o gostovanju v javnih mobilnih komunikacijskih omrežjih v Uniji \(prenovitev\)](#), COM(2021) 85 final z dne 24. februarja 2021.

Slika 4 – Priporočila za posamezne države v zvezi s 5G

Leta 2020:

1. Avstrija
2. Belgija
3. Bolgarija
4. Hrvaška
5. Češka
6. Slovenija
7. Švedska

Leta 2019:

1. Belgija
2. Francija



Vir: Evropsko računsko sodišče na podlagi [priporočil za posamezne države](#)

Države članice morajo še vedno odstraniti ključne ovire za hitro uvajanje omrežij 5G

34 Da bi države članice izpolnile cilja EU za leti 2025 in 2030 na področju uvajanja omrežij 5G, morajo izpolniti tri glavne pogoje: strateškega, tako da zagotovijo, da sta ta cilja upoštevana v njihovih nacionalnih strategijah za 5G ali nacionalnih načrtih za širokopasovne povezave²³, zakonodajnega, tako da v svojo zakonodajo prenesejo Evropski zakonik o elektronskih komunikacijah iz leta 2018²⁴, in poslovnega, tako da dodelijo spekter²⁵. **Tabela 3** vsebuje pregled napredka držav članic pri doseganju teh treh elementov.

²³ Študija Komisije [Study on National Broadband Plans in the EU-27](#).

²⁴ Direktiva (EU) 2018/1972 o Evropskem zakoniku o elektronskih komunikacijah.

²⁵ Sporočilo Evropske komisije, [Varna uvedba tehnologije 5G v EU - izvajanje nabora orodij EU](#), COM(2020) 50 final.

Tabela 3 – Stanje glede izpolnjevanja pogojev za uresničitev cilja za leto 2025

Država članica	Nacionalni načrt za širokopasovne povezave v skladu s cilji za leto 2025	Prenos Evropskega zakonika o elektronskih komunikacijah	Pionirski frekvenčni pasovi 5G (avgust 2021)			Verjetnost doseganja cilja
			700 MHz	3,6 GHz začasna uporaba	26 GHz	
Belgija						majhna
Bolgarija		✓		✓		majhna
Češka	✓	✓	✓	✓		srednja
Danska		✓	✓	✓	✓	velika
Nemčija	✓	✓	✓	✓	✓	srednja
Estonija						srednja
Irska				✓		srednja
Grčija	✓	✓	✓	✓	✓	majhna
Španija	✓		✓	✓		velika
Francija	✓	✓	✓	✓		velika
Hrvaška			✓	✓	✓	majhna
Italija			✓	✓	✓	velika
Ciper	✓		✓	✓		majhna
Litva	✓					srednja
Latvija				✓		velika
Luksemburg			✓	✓		velika
Madžarska	✓	✓	✓	✓		velika
Malta		✓				srednja
Nizozemska	✓		✓			srednja
Avstrija	✓	✓	✓	✓		srednja
Poljska	✓					srednja
Portugalska				začasna uporaba		srednja do velika
Romunija						velika
Slovenija	✓		✓	✓	✓	srednja
Slovaška			✓			velika
Finska	✓	✓	✓	✓	✓	velika
Švedska	✓		✓	✓		velika

Vir: Študija Komisije [Study on National Broadband Plans in the EU-27](#), opazovalnica 5G in RSPG

Cilja glede uvajanja omrežij 5G do leta 2025 in 2030 je v svoje nacionalne strategije za 5G vključilo malo držav članic

35 Države članice svojo politiko o 5G opredelijo z namenskimi nacionalnimi strategijami za 5G ali posodobitvijo obstoječih nacionalnih načrtov za širokopasovne povezave. Komisija je v študiji o nacionalnih načrtih za širokopasovne povezave iz leta 2021²⁶ navedla, da je cilj EU glede neprekinjene pokritosti 5G do leta 2025 na vseh mestnih območjih in vseh glavnih kopenskih prometnih poteh v svojo nacionalno strategijo za 5G ali posodobitev širokopasovnih načrtov vključilo samo 14 držav članic (glej [tabelo 3](#)). Vključitev cilja je ključna za podpiranje uspešnega izvajanja politike.

Večina držav članic do konca leta 2020 ni prenesla direktive o Evropskem zakoniku o elektronskih komunikacijah

36 Evropski zakonik o elektronskih komunikacijah – direktivo, v kateri so določene naloge nacionalnih regulativnih in drugih pristojnih organov ter roki za dodelitev pionirskih pasov 5G – bi morale države članice prenesti do 21. decembra 2020. Do konca februarja 2021 so le tri države članice (Finska, Grčija in Madžarska) navedle, da so sprejele vse potrebne ukrepe za prenos direktive, zato je Komisija proti preostalem 24 državam članicam začela postopke za ugotavljanje kršitev²⁷.

37 Konec novembra 2021 je še vedno potekalo 23 postopkov za ugotavljanje kršitev. Komisija sicer pričakuje, da bo postopke za ugotavljanje kršitev v zvezi s šestimi državami članicami (Avstrijo, Bolgarijo, Češko, Francijo, Nemčijo in Malto) kmalu zaključila, zadeve v zvezi s preostalimi 17 državami članicami pa bo morda morala posredovati Sodišču Evropske unije²⁸ (glej [tabelo 3](#)).

Zaostajanje pri dodelitvi pionirskih frekvenčnih pasov 5G

38 Komisija in države članice so leta 2016 opredelile tri pionirske frekvenčne pasove, ki se bodo uporabljali za storitve 5G:

- o frekvenčni spekter 700 MHz: brezžični signali v tem spektru lažje prodirajo v stavbe, operaterji pa lahko z njim zagotovijo širšo pokritost (več sto kvadratnih kilometrov), vendar sta hitrost in latenca omrežja 5G le malo boljša od omrežja 4G (250 namesto 150 megabitov na sekundo),

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

²⁷ Sporočilo Komisije za medije IP/21/2016 z dne 4. februarja 2021.

²⁸ Sporočilo Komisije za medije IP/21/4612 z dne 23. septembra 2021.

- o srednji frekvenčni spekter 3,6 GHz: ta spekter lahko prenaša velike količine podatkov (do 900 megabitov na sekundo) čez znatne razdalje (večkilometrski radij),
- o visoki frekvenčni spekter 26 GHz: ta spekter omogoča velike hitrosti od 1 do 3 gigabitov na sekundo na kratke razdalje (manj kot 2 km), vendar je bolj občutljiv za motnje.

39 Države članice naj bi uporabo nizkega frekvenčnega spektra zagotovile do 30. junija 2020²⁹, uporabo srednjega in visokega frekvenčnega spektra pa do 31. decembra 2020³⁰. vendar so do konca leta 2020 dodelile manj kot 40 % vseh razpoložljivih pionirskih frekvenčnih pasov (glej *tabelo 4*):

- o pas 700 MHz je bil dodeljen v 13 državah članicah,
- o pas 3,6 GHz je bil dodeljen v 17 državah članicah (vključno z dvema državama članicama, ki sta ga dodelili v začasno uporabo),
- o pas 26 GHz je bil dodeljen v štirih državah članicah.

Do konca oktobra 2021 se je stopnja dodelitve povečala na 53 %³¹.

²⁹ Sklep (EU) 2017/899 o uporabi frekvenčnega pasu 470–790 MHz v Uniji.

³⁰ Direktiva (EU) 2018/1972 o Evropskem zakoniku o elektronskih komunikacijah.

³¹ Opazovalnica 5G in RSPG.

Tabela 4 – Stanje glede dodelitve pionirskih frekvenčnih pasov 5G decembra 2020

Država članica	700 MHz	3,6 GHz	26 GHz
Belgija		začasna uporaba	
Bolgarija			
Češka	✓	✓	
Danska	✓	✓	✓
Nemčija	✓	✓	✓
Estonija		–	
Irska		✓	
Grčija	✓	✓	✓
Španija		✓	
Francija	✓	✓	
Hrvaška			
Italija		✓	✓
Ciper	✓	✓	
Latvija		✓	
Litva			
Luksemburg	✓	✓	
Madžarska	✓	✓	
Malta			
Nizozemska	✓		
Avstrija	✓	✓	
Poljska			
Portugalska		začasna uporaba	
Romunija			
Slovenija			
Slovaška	✓	✓	
Finska	✓	✓	✓
Švedska	✓	✓	

Vir: [Opazovalnica 5G](#) in [RSPG](#)

Do zamud pri dodelitvi pionirskih frekvenčnih pasov prihaja iz različnih razlogov

40 Sodišče je ugotovilo, da je razlog za zamude pri dodelitvi pasov 26 GHz predvsem slabo povpraševanje operaterjev mobilnih omrežij. V Španiji je na primer v pasu 26 GHz za uporabo 5G na voljo le skupno 1,5 GHz, vendar pas še ni bil dodeljen operaterjem, ker po podatkih z javnega posvetovanja, končanega julija 2019, po njem ni povpraševanja. Do konca leta 2021 je načrtovano novo javno posvetovanje z namenom, da bi pas dodelili na dražbi v drugem četrtletju leta 2022. Tudi operaterji mobilnih omrežij na Finskem so navedli, da za pas 26 GHz še ni veliko zanimanja ali poslovnih potreb.

41 K zamudam pri dodelitvi spektra 5G prispevajo tudi težave pri čezmejnem usklajevanju z državami nečlanicami EU ob vzhodnih mejah (Belorusijo, Rusijo in Ukrajino), ki v skladu z veljavnimi mednarodnimi sporazumi pas 700 MHz uporabljajo za razširjanje televizijskih programov, pas 3,6 GHz pa za vojaške satelitske storitve. Ta težava prizadeva predvsem baltske države (Estonijo, Latvijo in Litvo) ter Poljsko. Komisija navaja, da je v zvezi z Ukrajino in Belorusijo prišlo do napredka in da naj bi državi pas 700 MHz sprostili do konca leta 2022. V dvostranskih pogovorih z Rusijo napredka še ni. Glede na razmere sta Estonija in Poljska zaprosili za možnost odstopanja od rokov za dodelitev pasu 700 MHz do sredine leta 2022.

42 Poleg tega so bile na Poljskem in v Španiji dražbe spektra 5G med pandemijo COVID-19 preložene (glej [okvir 3](#)).

Okvir 3

Primeri zamud pri dodelitvi spektra 5G zaradi COVID-19

- Poljska je marca 2020 napovedala dražbo v zvezi s pasom 3,6 GHz, ki naj bi bil dodeljen do 30. junija 2020. Po izbruhu pandemije so se poljski organi odločili, da bodo začasno ustavili vse upravne postopke, dokler se pandemija ne konča. Do septembra 2021 proces za dodelitev tega pasu na dražbi še ni bil zaključen,
- v Španiji je bila dražba v zvezi s pasom 700 MHz sprva načrtovana marca 2020, vendar je po navedbah španskih organov zaradi pandemije COVID-19 prišlo do zamud pri sprostitvi tega pasu, ki se uporablja za digitalno televizijo. Dražba je bila najprej prestavljena na maj 2020, potem pa na prvo četrtnetje 2021. Po spremembi španske zakonodaje aprila 2021, s katero je bilo trajanje licenc usklajeno z Evropskim zakonikom o elektronskih komunikacijah, je bila dražba prestavljena na poletje 2021, pas 700 MHz pa končno dodeljen julija 2021.

43 Poleg tega zamude pri dodelitvi pionirskih frekvenčnih pasov 5G povzročajo tudi različni pristopi držav članic k varnosti 5G in zamude pri sprejemanju zakonov o varnosti 5G, kar vodi v poslovno negotovost (glej odstavka **74** in **75**):

- o v Španiji so pravila za dražbo pionirskih frekvenčnih pasov vključevala splošno klavzulo, v skladu s katero morajo imetniki javnih koncesij izpolnjevati vse obveznosti v zvezi z varnostjo omrežij 5G, ki bi bile kadar koli v prihodnosti določene z evropskimi ali španskimi predpisi. Španski operater mobilnega omrežja, s katerim je Sodišče opravilo razgovor, je menil, da je moral zaradi te klavzule odločitve o strategijah in nakupih sprejemati v negotovih razmerah. Poudaril je tudi, da nacionalni organi niso bili pripravljeni pojasniti nekaterih ključnih pogojev, kot je možnost nadomestila, če bi moral operater zaradi prihodnje zakonodaje, ki naj bi bila sprejeta do konca leta 2022, zamenjati opremo,
- o na Poljskem je bila dodelitev spektra 5G med drugim odložena tudi zato, ker je bilo treba počakati na zakon o varnostnih zahtevah za omrežja 5G.

Za obravnavanje varnostnih vprašanj pri uvajanju omrežij 5G so potrebna nadaljnja prizadevanja

44 V zvezi z varnostnimi vidiki omrežij 5G je Sodišče preučilo:

- o ali je Komisija sprejela potrebne ukrepe za spodbujanje dobre zasnove varnostnega okvira in državam članicam zagotovila ustrezno podporo ter
- o ali države članice varna omrežja 5G uvajajo na usklajen način, sprejemajo blažilne ukrepe iz nabora orodij EU za kibernetško varnost tehnologije 5G in posodablajo svojo zakonodajo.

Ko je varnost omrežij 5G postala pomembno vprašanje na ravni EU, se je Komisija hitro odzvala

45 Akcijski načrt za 5G iz leta 2016 ne vsebuje varnostnih pomislekov. Varnost omrežij 5G in pretirana odvisnost od dobaviteljev iz tretjih držav, zlasti Kitajske, sta bili marca 2019 opredeljeni kot ena od kritičnih težav. Evropski parlament je v svoji resoluciji z dne 12. marca 2019³² izrazil pomisleke glede dobaviteljev 5G iz držav nečlanic EU, ki bi lahko zaradi zakonov v svoji matični državi pomenili varnostno tveganje za EU. Isti dan je Komisija v svoji strateški viziji o odnosu med EU in Kitajsko poudarila, da je potreben skupen pristop EU k varnosti omrežij 5G, da bo zagotovljena zaščita pred morebitnimi resnimi posledicami za varnost kritične digitalne infrastrukture³³. Evropski svet je v sklepih z dne 21. in 22. marca 2019 pozval Komisijo, naj pripravi priporočilo o usklajenem pristopu k varnosti omrežij 5G³⁴.

46 Nekaj dni pozneje je Komisija objavila takšno priporočilo, in sicer s sklopom ukrepov na nacionalni ravni (na primer ocena tveganja omrežij 5G) in ravni EU (na primer usklajena ocena tveganja), namenjenih zagotavljanju visoke ravni kibernetске varnosti omrežij 5G v EU³⁵.

47 Do roka v juliju 2019 so nacionalne ocene tveganja dokončale skoraj vse države članice³⁶. Skupina za sodelovanje na področju varnosti omrežij in informacij je oktobra 2019 izdala poročilo o usklajeni oceni EU glede tveganja za kibernetско varnost v omrežjih 5G, januarja 2020 pa je bil objavljen [nabor orodij EU za kibernetско varnost tehnologije 5G](#)³⁷ (glej [Prilogo VII](#)), ki sta ga Komisija in Evropski svet hitro odobrila³⁸.

³² Resolucija Evropskega parlamenta z dne 12. marca 2019 (2019/2575(RSP)).

³³ JOIN(2019) 5 final z dne 12. marca 2019. EU-Kitajska – strateška vizija.

³⁴ Sklepi Evropskega sveta z dne 21. in 22. marca 2019.

³⁵ Priporočilo Komisije (EU) 2019/534 z dne 26. marca 2019 – Kibernetška varnost omrežij 5G.

³⁶ Sporočilo za medije z dne 19. julija 2019.

³⁷ *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*, Skupina za sodelovanje na področju varnosti omrežij in informacij, januar 2020.

³⁸ Sporočilo Evropske komisije, *Varna uvedba tehnologije 5G v EU - izvajanje nabora orodij EU*, COM(2020) 50 final, in Sklepi Evropskega sveta z dne 1. in 22. marca 2019 (EUCO 13/20).

Z naborom orodij EU za kibernetško varnost tehnologije 5G iz leta 2020 so bili prvič oblikovani ukrepi za obravnavo groženj za varnost na ravni EU, ki pa niso predpisovalni

Če se varnost omrežij 5G obravnava kot vprašanje nacionalne varnosti v nacionalni pristojnosti, so možnosti Komisije za ukrepanje omejene

48 V Pogodbah EU³⁹ je opredeljeno področje ukrepanja glede obravnave izzivov, kot so izzivi, povezani z uvajanjem varnih omrežij 5G na ravni EU. Področje uporabe je široko ter Komisiji in državam članicam omogoča manevrski prostor za razlago (glej [okvir 4](#)).

Okvir 4

Pristojnosti EU v zvezi z omrežji 5G: deljena pristojnost ali vprašanje nacionalne varnosti?

Omrežja 5G načeloma spadajo v okvir pristojnosti EU za enotni trg (deljena pristojnost), in sicer kot storitev (storitev, ki jo zagotavljajo operaterji mobilnih omrežij) in kot blago (oprema 5G, ki jo operaterji mobilnih omrežij kupijo za gradnjo omrežij 5G). V okviru deljene pristojnosti lahko EU (Komisija in druge institucije EU) sprejme pravno zavezujoče ukrepe (zakonodajo), da bi zagotovila vzpostavitev svojega enotnega trga in spodbujala njegovo pravilno delovanje. Varnost omrežij 5G bi lahko razumeli tudi širše, in sicer kot vprašanje, povezano s področji svobode, varnosti in pravice v EU. V tem smislu se lahko varnost razume kot splošen pojem, povezan s preprečevanjem kriminala in bojem proti njemu. Tudi s tega vidika gre za deljeno pristojnost, v zvezi s katero lahko EU sprejme pravno zavezujoče ukrepe.

Po drugi strani se lahko z ožjo razlago varnosti pojem omeji na grožnje za nacionalno varnost držav članic. V tem primeru gre izključno za nacionalno pristojnost, zato je EU omejena na sprejemanje podpornih ukrepov za pomoč prizadevanjem držav članic na nacionalni ravni, da bi zagotovile varnost svojih omrežij 5G.

³⁹ Pogodba o delovanju Evropske unije.

49 Za varnost omrežij 5G, ki je povezana tudi z nacionalno varnostjo, so pristojne tako države članice kot tudi EU. Ker si Komisija varnost omrežij 5G razlaga v smislu groženj za nacionalno varnost, se je odločila za ukrepe mehkega prava. To pomeni, da EU ne more sprejeti pravno zavezujočih ukrepov, s katerimi bi države članice prisilila k uporabi enotnih ukrepov za zmanjševanje tveganja ali uvedbi izvršljivih zahtev. Namesto tega lahko Komisija izdaja nezavezujoča priporočila in sporočila, pomaga pri razširjanju najboljših praks in usklajuje nacionalne ukrepe držav članic. Vendar je mogoč tudi drugačen pristop. Tak primer je direktiva o varnosti omrežij in informacij⁴⁰ – zakonski akt EU, v katerem je obravnavana varnost omrežij in informacijskih sistemov v Uniji. Predlagala jo je Komisija, sprejeta pa je bila na pravni podlagi enotnega trga, čeprav so za kibernetiko varnost v glavnem pristojne države članice⁴¹.

Nabor orodij EU za kibernetiko varnost 5G je bil sicer sprejet v zgodnji fazi uvajanja omrežij 5G, vendar so nekateri operaterji mobilnih omrežij takrat že izbrali svoje dobavitelje

50 Skupina za sodelovanje na področju varnosti omrežij in informacij je januarja 2020 sprejela nabor orodij EU za kibernetiko varnost tehnologije 5G, v okviru katerega so navedeni številni strateški, tehnični in podporni ukrepi za obravnavo groženj za varnost omrežij 5G, za vsakega od njih pa so opredeljeni tudi ustrezni akterji. Ta nabor orodij, ki sta ga odobrila Komisija in Evropski svet, je bil sprejet samo devet mesecev po tem, ko sta Evropski parlament in Svet prvič izrazila pomisleke glede varnosti omrežij 5G. Nedavno je bil nabor orodij EU za kibernetiko varnost 5G omenjen v novi evropski strategiji za spodbujanje pametnih, čistih in varnih povezav v digitalnih sistemih po vsem svetu kot orodje za usmerjanje naložb v digitalno infrastrukturo⁴². Pristop mehkega prava, ki ga je sprejela Komisija, je prispeval k hitremu zagonu ukrepov za obravnavo groženj za varnost tudi na ravni EU in za lažje sodelovanje držav članic pri tem čezmejnem vprašanju. Za primerjavo, od predloga Komisije⁴³ do sprejetja direktive o varnosti omrežij in informacij⁴⁴ so minila več kot tri leta, do

⁴⁰ Direktiva (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

⁴¹ Pregled št. 02/2019: Izzivi za uspešno politiko EU za kibernetiko varnost (informativni dokument), odstavek 36.

⁴² Skupno sporočilo Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru, Odboru regij in Evropski investicijski banki – Strategija Global Gateway, JOIN(2021) 30 final z dne 1. decembra 2021.

⁴³ COM(2013) 48 final z dne 7. februarja 2013.

⁴⁴ Direktiva (EU) 2016/1148.

sprejetja direktive o Evropskem zakoniku o elektronskih komunikacijah⁴⁵ pa več kot dve leti. Še dlje je trajalo, da sta bili direktivi preneseni v nacionalne pravne sisteme držav članic (glej tudi odstavka 36 in 37).

51 Nabor orodij EU za kibernetško varnost tehnologije 5G je bil sprejet štiri leta po tem, ko je bila v akcijskem načrtu za 5G predstavljena politika za 5G, in v letu, ko bi morali biti doseženi vmesni mejniki uvajanja, določeni v tem akcijskem načrtu. Glede na to so predstavniki ministrstev držav članic, nacionalnih regulativnih organov in operaterjev mobilnih omrežij, s katerimi so bili opravljeni razgovori za to revizijo, menili, da so se ukrepi v zvezi z varnostnimi vidiki omrežij 5G začeli prepozno.

52 Poleg tega je bila večina držav članic v času objave nabora orodij v zgodnji fazi uvajanja omrežij 5G in priprave načrtov za 5G. Večina pogodb med dobavitelji in operaterji za opremo 5G je bila sklenjena v letih 2020 in 2021. Vendar so po podatkih Združenja evropskih operaterjev telekomunikacijskih omrežij (ETNO) številni operaterji mobilnih omrežij v času objave nabora orodij EU za kibernetško varnost 5G svoje dobavitelje že izbrali.

Z naborom orodij EU za kibernetško varnost 5G je bil zagotovljen okvir za ocenjevanje profila tveganja dobaviteljev, vendar so pomanjkljivosti ostale

Nekatere države članice in nacionalni organi menijo, da del meril za razvrstitev dobaviteljev med visoko tvegane ni dovolj jasen

53 Ena od ključnih značilnosti nabora orodij EU za kibernetško varnost tehnologije 5G je to, da države članice ocenijo dobavitelje in pri tistih, razvrščenih med visoko tvegane, uporabijo omejitve za ključna sredstva, ki so opredeljena kot kritična. Države članice bi morale to oceno izvesti na podlagi neizčrpnega seznama meril iz usklajene ocene EU glede tveganja. Ta merila so na primer:

- verjetnost, da je dobavitelj pod vplivom države nečlanice EU, na primer zaradi močne povezave med dobaviteljem in vlado države nečlanice EU ali zaradi zakonodaje države nečlanice EU, zlasti če ta država nima zakonodajnega ali demokratičnega sistema zavor in ravnovesij ali če med njo in EU niso bili sklenjeni sporazumi o varnosti ali varstvu podatkov,
- sposobnost dobavitelja, da zagotovi dobavo, ter

⁴⁵ COM(2016) 590 final/2 z dne 12. oktobra 2016 in Direktiva (EU) 2018/1972 o Evropskem zakoniku o elektronskih komunikacijah.

- o splošna kakovost dobaviteljevih proizvodov in praks kibernetike varnosti.

54 Zbirka orodij je bila razvita za preprečevanje razdrobljenosti in spodbujanje doslednosti na notranjem trgu. Z merili iz nabora orodij je zagotovljen operativni okvir, ki je koristen za usklajeno ocenjevanje profila tveganja dobaviteljev v vseh državah članicah. Poleg tega se lahko Komisija na podlagi nabora orodij skupaj z državami članicami hitro odzove na nove pomisleke glede varnosti 5G. Za uporabo teh meril pri ocenjevanju tveganj, povezanih z določenimi dobavitelji, pa so še vedno pristojni nacionalni organi. Do oktobra 2021 je zakonodaja o varnosti 5G ob upoštevanju tega okvira sprejelo ali spremenilo 13 držav članic (glej odstavek **75** in **sliko 6**).

55 Vendar so predstavniki dveh od štirih ministrstev držav članic, s katerimi je Sodišče opravilo razgovore za to revizijo, menili, da je nekatera od teh meril za razvrščanje dobaviteljev 5G mogoče različno razlagati in da bi jih bilo treba dodatno pojasniti. Komisijo so tudi pozvali, naj zagotovi dodatno podporo in smernice v zvezi z razvrstitvijo visoko tveganih dobaviteljev. Predstavniki držav članic, s katerimi je Sodišče opravilo razgovore, so navedli tudi, da zaradi te situacije obstaja tveganje, da bi države članice visoko tvegane dobavitelje obravnavale različno (glej tudi odstavek **74** in **75** ter **okvir 5**). 11 nacionalnih regulativnih organov, ki so odgovorili na anketo Sodišča in ki na področju varnosti 5G delujejo v različnem obsegu, je izrazilo podobne pomisleke.

Matična država dobaviteljev 5G vpliva na oceno varnostnega tveganja

56 Dobavitelji 5G se razlikujejo glede na lastnosti njihovih podjetij in prihajajo iz držav z različnimi vezmi z EU. Na **sliki 5** so za glavne dobavitelje 5G in njihove matične države prikazane nekatere skupne točke in razlike, zlasti na področjih, za katere je v naboru orodij navedeno, da bodo verjetno vplivala na oceno profila tveganja (glej odstavek **53**).

Slika 5 – Dobavitelji 5G in njihove matične države – skupne točke in razlike



Vir: Evropsko računsko sodišče na podlagi seznama članic STO, seznama članic OECD, indeksa omejevanja neposrednih tujih naložb OECD, nabora podatkov Svetovne banke o svetovnih kazalnikih upravljanja za leto 2019, nabora podatkov WEF o svetovni konkurenčnosti, lestvica za leto 2018, sklepov o ustreznosti, analize platforme Statista: *Who is leading the 5G patent race?*, podatkov o podjetju Ericsson, podatkov o podjetju Nokia, podatkov o podjetju Qualcomm, podatkov o podjetju Sharp, podatkov o podjetju LG, podatkov o podjetju Samsung, podatkov o podjetju Huawei in podatkov o podjetju ZTE (upoštevani so podatki iz leta 2019, razen če je drugače navedeno).

57 Eden od dejavnikov tveganja je skladnost matične države dobavitelja s temeljnimi političnimi in gospodarskimi vrednotami EU. Dejavniki, specifični za državo, kot so pravna država, neodvisnost sodstva, odprtost za tuje naložbe in obstoj sporazumov o varstvu podatkov, se lahko razumejo kot raven pravnega varstva podjetja pred poseganjem države ter zaščita, ki jo lahko podjetje zagotovi svojim strankam.

58 Dobavitelja s sedežem v državah članicah EU sta zavezana spoštovati standarde in pravne zahteve EU, to pa ne velja za šest glavnih dobaviteljev s sedežem v državah nečlanicah EU, ki delujejo v okviru zakonodaj tretjih držav (glej [sliko 5](#)). Te zakonodaje se lahko znatno razlikujejo od standardov EU, na primer glede varstva podatkov, ki so ga deležni državljani, in njegove uspešnosti ali bolj na splošno, kako se z zakonodajnim in/ali demokratičnim sistemom zavor in ravnesij zagotavlja neodvisnost sodstva. Na področju neodvisnosti sodstva imajo ZDA in Japonska višjo oceno od drugih matičnih držav dobaviteljev 5G, ki niso članice EU, na področju pravne države pa ima med državami nečlanicami EU najvišjo oceno Južna Koreja.

59 Omrežja 5G delujejo predvsem na podlagi programske opreme. Delovanje nekaterih dobaviteljev v okviru zakonodaje tretjih držav je še zlasti skrb vzbujajoče, če so tudi centri za nadzor programske opreme v državah nečlanicah EU, zaradi česar bi lahko za državljane EU veljala zakonodaja tretjih držav.

60 Komisija je začela obravnavati te pomisleke, saj meni, da bi moralo vsako podjetje, ki zagotavlja storitve državljanom EU, spoštovati pravila in vrednote EU⁴⁶. Z več državami je začela dialoge, da bi zagotovila močno varstvo zasebnosti osebnih podatkov⁴⁷. Na [sliki 5](#) je vidno tudi, da je Komisija ustreznost sistemov varstva podatkov že priznala za Japonsko (in v preteklosti za ZDA). Vendar je treba opozoriti, da je sklepe o ustreznosti mogoče izpodbijati in da so pod strogim sodnim nadzorom. Na primer, Sodišče Evropske unije je leta 2015 razveljavilo takrat veljavni pravni instrument za izmenjavo podatkov z ZDA (sporazum o varnem pristanu)⁴⁸, leta 2020 pa je odločilo, da z zasebnostnim ščitom EU-ZDA, ki je nadomestil sporazum o varnem pristanu, državljanom EU ni bila zagotovljena ustrezna zaščita⁴⁹. Zato sklepa o ustreznosti za ZDA trenutno ni. Na splošno je poleg obstoja sistema varstva podatkov

⁴⁶ Sporočilo Evropske komisije, [Oblikovanje digitalne prihodnosti Evrope](#), COM(2020) 67 final.

⁴⁷ EU-Kitajska – strateška vizija.

⁴⁸ Sodba v zadevi C-362/14 in <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117sl.pdf>.

⁴⁹ Sodba v zadevi C-311/18 in <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091sl.pdf>.

pomembno upoštevati tudi širši pravni in institucionalni okvir, med drugim na primer spoštovanje pravne države in način zagotavljanja neodvisnosti sodstva.

61 Na [sliki 5](#) je vidno tudi, da so med dobavitelji 5G bistvene razlike v smislu deleža patentov 5G, prihodka in števila zaposlenih, kar vpliva na vire, ki jih imajo na voljo, to pa ima lahko posledice za njihovo odpornost in sposobnost zagotavljanja nemotene dobave. Na primer, Samsung in Huawei sta dobavitelja z največjim deležem patentov 5G, najvišjimi korporativnimi prihodki in največjim številom zaposlenih.

62 V naboru orodij je kot eden od pomembnih dejavnikov za določanje profila tveganja dobavitelja opredeljena tudi verjetnost, da je dobavitelj pod vplivom vlade države nečlanice EU. V zvezi s tem ima pomembno vlogo lastništvo, saj lahko lastniki z velikim deležem delnic morda pritiskajo ali vplivajo na odločitve vodstva. Poleg tega šteje, da so podjetja v zasebni ali državni lasti manj odprta za javni nadzor v obliki revizij in odgovornosti kot delniške družbe, za katere veljajo celoletne stroge zahteve glede razkritja za potrebe splošnih vlagateljev in regulatorjev. Večina dobaviteljev 5G kotira na borzi v svoji matični državi ali tujini, kitajska dobavitelja pa je težje razvrstiti in zanju na splošno velja, da sta tesno povezana s kitajsko vlado⁵⁰.

Države članice so menile, da je bila podpora Komisije in agencije ENISA koristna za izvajanje nabora orodij EU za kibernetško varnost tehnologije 5G

63 Komisija je državam članicam zagotovila podporo, in sicer z izmenjavo najboljših praks v zvezi z nekaterimi ključnimi ukrepi iz nabora orodij EU za kibernetško varnost tehnologije 5G, vključno s praksami v zvezi z visoko tveganimi dobavitelji. Podporo, ki je bila pogosto zagotovljena v okviru skupine za sodelovanje na področju varnosti omrežij in informacij, so dopolnjevale posebne dejavnosti, ki jih je pripravila agencija ENISA, kot sta organizacija spletnih seminarjev in zagotovitev smernic o:

- izvajanju nabora orodij s poudarkom na tehničnih ukrepih in
- najboljše prakse v zvezi z varnostjo omrežij, zlasti glede:
 - narave groženj 5G⁵¹,

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

⁵¹ ENISA, *Threat Landscape for 5G Networks*, 14. december 2020.

- priprave nacionalnih ocen tveganja 5G in
- varnostnih ukrepov v okviru Evropskega zakonika o elektronskih komunikacijah⁵², vključno s posebnimi smernicami o varnosti 5G⁵³.

64 Komisija je agencijo ENISA zadolžila, naj za omrežja 5G pripravi certifikacijsko shemo EU za kibernetsko varnost, ki bo v pomoč pri obravnavi tveganj, povezanih s tehničnimi ranljivostmi omrežij, in s katero bo nadalje okrepljena kibernetska varnost⁵⁴. To certificiranje bi sicer lahko prispevalo k izboljšanju varnosti, vendar se z njim ne more preprečiti vgrajevanja groženj v sisteme s posodobitvami programske opreme.

65 Vsi predstavniki organov držav članic, s katerimi je Sodišče opravilo razgovore za to revizijo, so poudarili koristnost podpore Komisije in agencije ENISA za izvajanje nabora orodij EU za kibernetsko varnost tehnologije 5G. Poleg tega je večina nacionalnih regulativnih organov za telekomunikacije (15 od 21) navedla, da sta Komisija in/ali agencija ENISA nacionalne organe podpirali pri izmenjavi najboljših praks glede izvajanja ključnih strateških ukrepov.

Nabor orodij EU za kibernetsko varnost tehnologije 5G je bil sprejet prepozno, da bi se upošteval pri projektih, ki jih je EU sofinancirala v obdobju 2014–2020

66 Eden od ciljev nabora orodij EU za kibernetsko varnost tehnologije 5G je zagotoviti, da se pri projektih 5G, ki jih sofinancira EU, upoštevajo tveganja za kibernetsko varnost. Toda nabor orodij je bil sprejet šele januarja 2020. Vsi projekti, pregledani v okviru te revizije, so bili izbrani pred sprejetjem nabora orodij EU za kibernetsko varnost tehnologije 5G, zato ni mogoče pričakovati, da se je pri njih upošteval priporočeni pristop h kibernetski varnosti, vključno s pristopom k visoko tveganim dobaviteljem. Na primer, Sodišče je v svojem vzorcu opredelilo en projekt v okviru programa Obzorje 2020 in dva projekta v okviru ESRR v Španiji, pri katerih je bila uporabljena kitajska oprema 5G, ki je bila na Švedskem pozneje prepovedana (glej odstavek 15).

⁵² ENISA, *Guideline on Security Measures under the EECC*, 10. december 2020.

⁵³ ENISA, *Guideline on Security Measures under the EECC*, 7. julij 2021.

⁵⁴ Sporočilo za medije z dne 3. februarja 2021.

67 Za projekte, ki jih bo EU sofinancirala v obdobju 2021–2027, namerava Komisija spodbujati usklajen pristop k varnosti 5G, tako da bo zagotovila, da bo skladnost z naborem orodij eden od pogojev za financiranje EU, vendar bo to odvisno od načina izvajanja:

- o v programih, ki jih neposredno upravlja Komisija (na primer program Obzorje Evropa za obdobje 2021–2027), bo v primeru posredovanja vlade države nečlanice EU dovoljena izključitev dobaviteljev. Na ta način bo verjetno mogoče zagotoviti, da se pri projektih, ki jih financira EU, upoštevajo tveganja za kibernetško varnost, in preprečiti, da bi dobavitelj v eni državi članici prejel sofinanciranje EU, medtem ko bi v drugi državi članici štel za visoko tveganega in bil izključen,
- o za programe, ki se izvajajo v okviru deljenega upravljanja, zakonodaja ne vsebuje zahtev glede tveganj za kibernetško varnost. Komisija zato namerava spodbujati vključitev omembe nabora orodij v partnerske sporazume držav članic, da bi se pri financiranju projektov ESRR, povezanih s 5G, upoštevala tveganja za kibernetško varnost,
- o tudi v zvezi s programom InvestEU (ki bo nadomestil sklad EFSI)⁵⁵ ter mehanizmom za okrevanje in odpornost namerava Komisija spodbujati odgovorne organe, naj v sporazume o financiranju vključijo omembo nabora orodij EU.

Države članice pri uvajanju omrežij 5G varnostnih vidikov še ne obravnavajo usklajeno

Informacije o pristopu držav članic k vprašanju varnosti so nezadostne

68 Komisija spremlja napredek pri izvajanju nabora orodij EU za kibernetško varnost tehnologije 5G in o tem napredku poroča v okviru skupine za sodelovanje na področju varnosti omrežij in informacij, dvostranskih pogovorov z državami članicami in posredno prek medijev. Prvi rezultati tega spremljanja so bili objavljeni julija 2020⁵⁶. Decembra 2020 je Komisija objavila tudi poročilo o učinku svojega priporočila o

⁵⁵ Uredba (EU) 2021/523 o vzpostavitvi Programa InvestEU.

⁵⁶ *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*, julij 2020.

kibernetski varnosti omrežij 5G⁵⁷. Glede na stanje septembra 2021 nadaljnje poročanje ni bilo načrtovano.

69 Vendar zgoraj omenjeni poročili nimata skupnega nabora ključnih kazalnikov smotrnosti in primerljivega nabora podrobnih informacij o tem, kako države članice obravnavajo pomisleke glede varnosti 5G.

70 Poleg tega obstaja le malo javno dostopnih informacij o tem, kako države članice obravnavajo visoko tvegane dobavitelje, tj. kako jih prepoznavajo in ali jih izključujejo iz dobavljanja opreme 5G, pa tudi informacije, ki so na voljo, so si nasprotujoče in so nepopolne. Na primer:

- o v poročilu Komisije iz julija 2020 o napredku držav članic pri izvajanju nabora orodij (glej odstavek 68) je navedeno, da je približno polovica držav članic (14 od 27) ocenila profil tveganja dobaviteljev in za tiste, ki veljajo za visoko tvegane, uporabila omejitve,
- o v poročilu organa BEREC iz decembra 2020⁵⁸ je navedeno, da je take omejitve uvedlo samo devet držav članic, medtem ko sedem od 18 preostalih držav članic takih omejitev tudi v prihodnosti ne namerava izvajati.

71 Tudi v zakonodajah, ki so jih za obravnavo varnosti omrežij 5G sprejele države članice (glej tudi odstavek 75), še vedno ni razjasnjeno, kakšen pristop imajo te države članice k visoko tveganim dobaviteljem. Vsakršne konkretne odločitve bodo verjetno sprejete samo z izvedbenimi akti ali nejavnimi upravnimi ali komercialnimi odločitvami.

72 Deležniki in nosilci odločanja (na primer v Evropskem parlamentu), s katerimi je Sodišče opravilo razgovore, pravijo, da je malo tudi nejavnih informacij (na primer iz poročil Komisije ali skupine za sodelovanje na področju varnosti omrežij in informacij) o pristopu držav članic k visoko tveganim dobaviteljem, zato se morajo zanašati na medije in neuradne vire.

⁵⁷ *Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks*, SWD(2020) 357 final z dne 16. decembra 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. december 2020.

73 Kljub čezmejni naravi pomislekov glede varnosti 5G je o pristopih držav članic k vprašanju varnosti in zlasti visoko tveganim dobaviteljem na splošno na voljo le malo javnih informacij, kar ovira izmenjavo znanja med državami članicami in možnost uporabe usklajenih ukrepov, pa tudi možnost, da bi Komisija predlagala izboljšave varnosti omrežij 5G.

Mogoče je sklepati, da nekatere države članice uporabljajo različne pristope k dobaviteljem 5G

74 Nacionalni organi imajo široko diskrecijsko pravico pri izvajanju ključnih ukrepov v zvezi z varnostjo 5G (glej odstavka [48](#) in [49](#)). Pri zbirki orodij so upoštevane nacionalne pristojnosti in relevantni dejavniki, specifični za posamezno državo (ocena tveganja, ki jo opravijo nacionalne varnostne službe, časovni okvir uvajanja 5G, prisotnost dobaviteljev, zmogljivosti kibernetske varnosti). Doslej so bili pristopi držav članic k uporabi opreme določenih dobaviteljev ali obsegu omejitev za visoko tvegane dobavitelje različni (glej primere štirih držav članic v [okviru 5](#)).

Okvir 5

Primeri različnih pristopov držav članic h kitajskim dobaviteljem 5G

Vzpostavljeni okvir in omejitve, ki se uporabljajo⁽¹⁾

Švedski nacionalni regulativni organ za telekomunikacije (PTS) je oktobra 2020 za sodelovanje na dražbi spektra 5G določil naslednja pogoja:

- pri novih instalacijah in izvajanju osrednjih funkcij za radijsko uporabo v frekvenčnih pasovih se ne smejo uporabljati proizvodi kitajskih dobaviteljev,
- morebitno obstoječo infrastrukturo takih dobaviteljev je treba odstraniti najpozneje do 1. januarja 2025.

Vzpostavljeni okvir, ki se še ne uporablja^{(2), (3), (4)}

V Nemčiji je z zakonom o varnosti IT 2.0 iz maja 2021 določena obvezna certifikacija kritičnih komponent, preden se lahko odobri njihova uporaba. Nemškim operaterjem mobilnih omrežij, s katerimi so bili opravljeni razgovori, bi bil namesto morebitne množice nacionalnih certifikacij ljubši enoten evropski certifikacijski postopek pod okriljem agencije ENISA, ki bi delovala kot evropska točka vse na enem mestu. Na podlagi zakona lahko zvezno ministrstvo za notranje zadeve tudi prepove uporabo kritičnih komponent, če bi lahko pomenile grožnjo za nacionalno varnost.

V Avstriji lahko pristojni minister na podlagi posodobljenega zakona o telekomunikacijah, sprejetega konec oktobra 2021, dobavitelje opredeli kot visoko tvegane in uporabi omejitve ali dobavitelje izključi s trga. Po javno dostopnih informacijah iz oktobra 2021 namerava Avstrija razširiti svoje omrežje 5G z uporabo opreme kitajskega dobavitelja Huawei.

Okvir ni vzpostavljen^{(5), (6)}

Madžarska v zvezi z dobavitelji 5G do septembra 2021 ni sprejela omejitev in jih verjetno tudi v bližnji prihodnosti ne bo. Poleg tega je uradno zavrnila pridružitvev mednarodnemu programu za čista omrežja 5G (Clean Network), ki ga spodbujajo ZDA in je namenjen omejitvi prisotnosti kitajskih dobaviteljev v jedrnih omrežjih 5G.

(1) Sklep 18-8496 z dne 20. oktobra 2020 o pogojih za dražbo frekvenčnih pasov 3,5 GHz in 2,3 GHz

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

(3) Avstrijski zakon o telekomunikacijah

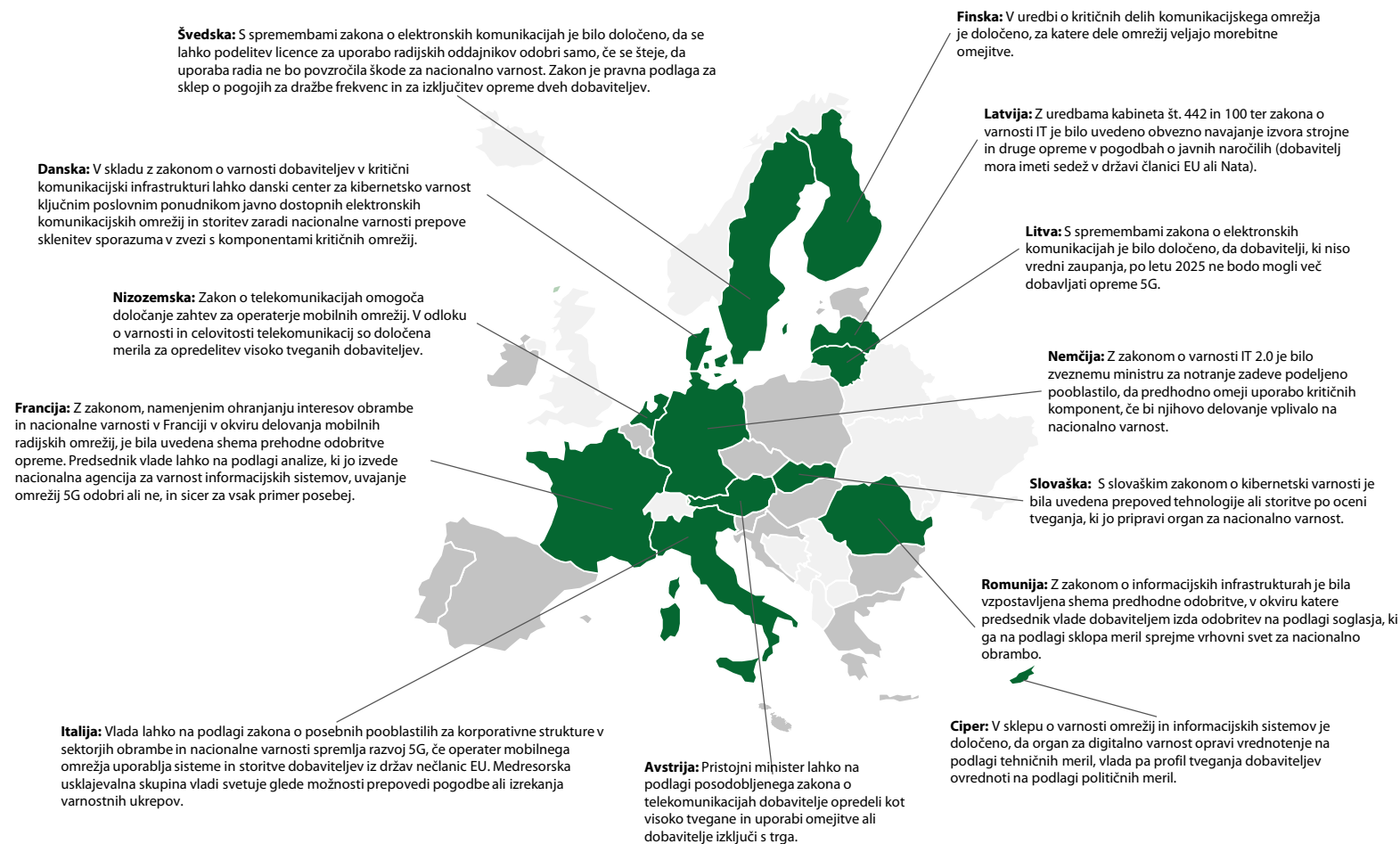
(4) <https://www.euractiv.com/section/5g/news/austria-to-also-rely-on-huawei-in-5g-rollout/>

(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 Od sprejetja nabora orodij je bil dosežen napredek pri krepitvi varnosti omrežij 5G, saj večina držav članic uporablja omejitve za visoko tvegane dobavitelje ali to namerava storiti. Do konca leta 2021 je nacionalne zakone o varnosti 5G sprejelo ali spremenilo 13 držav članic. Pri teh regulativnih ukrepih so upoštevana merila iz nabora orodij, vendar se zanje uporabljajo različni pristopi (glej [sliko 6](#)). Preostale države članice se pripravljajo na predložitev takšne zakonodaje. V prihodnjih letih bi to lahko privedlo do bolj usklajenih pristopov k visoko tveganim dobaviteljem 5G, vsaj med tistimi državami članicami, ki so takšno zakonodajo sprejele.

Slika 6 – Države članice, ki so do oktobra 2021 sprejele zakone, na podlagi katerih lahko iz svojih omrežij izključijo opremo visoko tveganih dobaviteljev



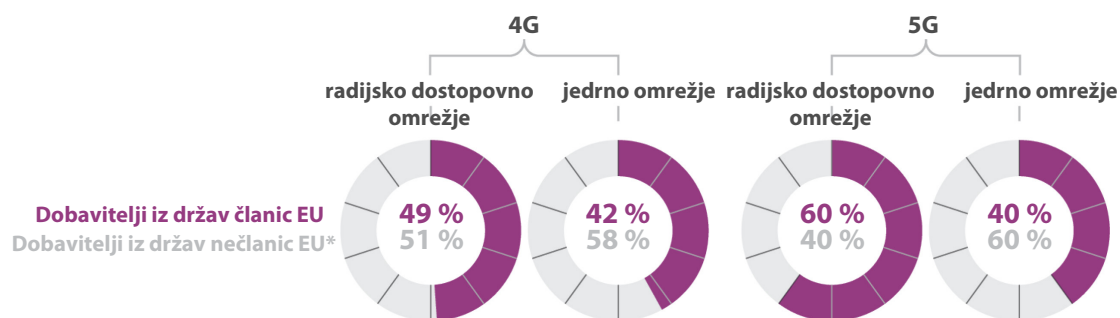
Vir: Evropsko računsko sodišče na podlagi podatkov Evropske komisije

76 Komisija doslej še ni ocenila, kakšen bi bil učinek takih različnih pristopov, in sicer če bi ena država članica svoja omrežja 5G gradila z uporabo opreme dobavitelja, ki v drugi državi članici šteje za visoko tveganega. To bi lahko vplivalo na čezmejno varnost ali konkurenco med operaterji mobilnih omrežij, ki delujejo na enotnem trgu EU.

Komisija je nedavno začela obravnavati vprašanje tujih subvencij, ki izkrivljajo notranji trg

77 Do decembra 2020 je bila več kot polovica celotne opreme 4G in 5G v EU pridobljena od dobaviteljev iz držav nečlanic EU (glej [sliko 7](#)).

Slika 7 – Delež operaterjev mobilnih omrežij, ki uporabljajo opremo dobaviteljev iz držav članic/nečlanic EU*



* Dobavitelji iz držav nečlanic EU vključujejo dobavitelje iz Severne Amerike, Azije in Avstralije.

Vir: Evropsko računsko sodišče na podlagi poročila organa BEREC z naslovom *Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)*, št. dokumenta BoR (20) 227

78 Ob koncu leta 2019 je [telekomunikacijska](#) omrežja, ki temeljijo na opremi 4G kitajskih dobaviteljev, uporabljalo 286 milijonov odjemalcev v 27 državah članicah EU (64 % vsega prebivalstva)⁵⁹. Skupina poslancev Evropskega parlamenta je oktobra 2020 ministrom držav članic za telekomunikacije in trgovino ter Komisiji poslala dopis, v katerem je izrazila zaskrbljenost glede tega, da je tržni delež kitajskih dobaviteljev visok tudi zato, ker imajo nepošteno ekonomsko prednost, saj so prejeli javne subvencije, ki dobaviteljem EU v skladu s pravili EU o državni pomoči niso na voljo⁶⁰. Sodišče je v

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

⁶⁰ Dopis poslancev Evropskega parlamenta ministrom EU za telekomunikacije in trgovino ter evropskim komisarjem Thierryju Bretonu, Margrethe Vestager in Valdisu Dombrovskisu z dne 14.10.2020.

nedavnem pregledu opozorilo na podobna tveganja v zvezi s tem⁶¹. S takimi subvencijami se lahko izkrivlja notranji trg in s tem povzroči neenaki konkurenčni pogoji za dobavitelje 5G, kar ima lahko posledice za varnost. Komisija je maja 2021 za obravnavo tega problema predlagala novo uredbo⁶², v kateri bi bili določeni postopki za preiskavo takih subvencij in odpravo z njimi povezanih izkrivljanj trga.

Komisija nima dovolj informacij o morebitnih stroških nadomestitve opreme, kupljene pri kitajskih dobaviteljih

79 Po podatkih v poročilu iz junija 2020⁶³ bi se z omejitvijo enega od ključnih dobaviteljev infrastrukture 5G v EU skupni naložbeni stroški v naslednjem desetletju povečali za skoraj 2,4 milijarde EUR na leto (tj. 24 milijard EUR). V neki drugi študiji⁶⁴ je navedeno, da evropske operaterje že čaka nadgradnja omrežij 4G, zgrajenih med letoma 2012 in 2016, saj prenova in posodobitev omrežne opreme, ki je stara več kot tri ali štiri leta, veljata za standardno poslovno prakso. Po oceni v tej študiji bodo skupni stroški odstranitve in nadomestitve nadgradljive opreme, kupljene pri kitajskih dobaviteljih od leta 2016 naprej, znašali približno 3 milijarde EUR.

80 Ker velik delež opreme prihaja od kitajskih dobaviteljev in ker bi lahko bili ti v nekaterih državah članicah razvrščeni med visoko tvegane, bi lahko v primeru obvezne odstranitve opreme kitajskih dobaviteljev iz evropskih omrežij in njene nadomestitve brez prehodnega obdobja operaterjem mobilnih omrežij nastali večmilijardni stroški nadomestitve (glej odstavke 77 do 79). Načeloma se državna pomoč operaterjem ne more dodeliti kot nadomestilo za izpolnjevanje pravnih obveznosti, razen če lahko države članice Komisiji dokažejo, da so izpolnjene potrebne zahteve (kot je spodbujevalni učinek). Pri analizi Sodišča je bil ugotovljen en primer nacionalne zakonodaje, na podlagi katere bi za povrnitev stroškov nadomestitve bilo mogoče uporabiti nacionalno javno financiranje (glej finski zakon o elektronskih komunikacijskih storitvah⁶⁵). Države članice morajo Komisiji priglasiti vsak primer državne pomoči za nadomestilo takih stroškov operaterjem mobilnih omrežij. Kot

⁶¹ Pregled Evropskega računskega sodišča št. 03/2020: Odziv EU na državno vodeno naložbeno strategijo Kitajske.

⁶² Predlog uredbe o tujih subvencijah, ki izkrivljajo notranji trg, COM(2021) 223 final z dne 5. maja 2021.

⁶³ Študija podjetja Oxford Economics z naslovom *Restricting competition in 5G network equipment throughout Europe*, ki jo je sponzoriralo podjetje Huawei, junij 2020.

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

⁶⁵ Zakon o elektronskih komunikacijskih storitvah 1207/2020 z dne 30. decembra 2020, člen 301.

navaja Komisija, je do zdaj v zvezi z državno pomočjo za stroške nadomestitve opreme ni kontaktirala še nobena država članica ali deležnik. Po mnenju deležnikov iz industrije, s katerimi so bili med revizijo opravljeni razgovori, negotovost glede obravnave takih stroškov v državah članicah in morebitne razlike med državami članicami ogrožajo poslovno varnost in pravočasno uvajanje omrežij 5G.

Zaključki in priporočila

81 Na splošno se je pri reviziji Sodišča pokazalo, da pri uvajanju omrežij 5G v državah članicah kljub podpori Komisije prihaja do znatnih zamud in da so potrebna nadaljnja prizadevanja za obravnavo varnostnih vprašanj pri uvajanju omrežij 5G.

82 Komisija je v svojem akcijskem načrtu za 5G iz leta 2016 pozvala k pokritosti vseh mestnih območij in vseh glavnih prometnih poti s 5G do leta 2025, marca 2021 pa k polni pokritosti do leta 2030. Do konca leta 2020 je komercialne storitve 5G uvedlo 23 držav članic in doseglo vmesni cilj, da ima do takih storitev dostop vsaj eno veliko mesto, vendar je Sodišče ugotovilo, da se nekatere države članice v svojih nacionalnih strategijah za 5G ali načrtih za širokopasovne povezave ne sklicujejo na cilja Komisije. Poleg tega več držav še ni preneslo Evropskega zakonika o elektronskih komunikacijah v nacionalno zakonodajo, pri dodelitvi spektra 5G pa je prišlo do zamud. Zamude pri dodelitvi spektra je mogoče pripisati različnim razlogom, in sicer slabemu povpraševanju operaterjev mobilnih omrežij, težavam pri čezmejnem usklajevanju z državami nečlanicami EU ob vzhodnih mejah, vplivu COVID-19 na časovne načrte dražb in negotovosti glede obravnave varnostnih vprašanj. Po navedbah Komisije bo cilj za leto 2025 verjetno doseglo samo 11 držav članic (glej odstavke [22](#) do [43](#)).

83 Komisija države članice pri izvajanju akcijskega načrta za 5G iz leta 2016 podpira s pobudami, smernicami in financiranjem raziskav, povezanih s 5G. Vendar doslej še ni opredelila pričakovane kakovosti storitev omrežij 5G, na primer glede minimalne hitrosti in maksimalne latence, zato si države članice pojem kakovost 5G razlagajo različno. Sodišče je opazilo, da imajo države članice različne pristope k uvajanju storitev 5G: najmanjšo hitrost in največjo latenco sta na primer opredelili le dve državi članici. Z različnimi pristopi je povezano tveganje za neenakosti glede kakovosti storitev 5G v EU in dostopa do njih, zaradi česar se lahko digitalni razkorak med državami članicami in regijami poveča, namesto da bi se zmanjšal (glej odstavke [22](#) do [31](#)).

Priporočilo 1 – Spodbujati enakomerno in pravočasno uvajanje omrežij 5G v EU

Komisija naj:

- (a) skupaj z državami članicami oblikuje skupno opredelitev pričakovane kakovosti storitev omrežij 5G, kot so zahteve glede zmogljivosti omrežij z vidika najmanjše hitrosti in največje latence;
- (b) spodbuja države članice, naj cilja glede uvajanja omrežij 5G do leta 2025 in leta 2030 ter ukrepe, potrebne za njuno uresničitev, vključijo v naslednjo posodobitev svojih strategij za 5G/digitalnih strategij ali načrtov za širokopasovne povezave, in
- (c) podpira države članice pri obravnavi težav z usklajevanjem spektra s sosednjimi državami nečlanicami EU, na primer s prizadevanji za vključitev vprašanja na dnevni red vsakega ustreznega srečanja.

Časovni okvir: december 2022.

84 Vidiki varnosti omrežij 5G so šele nedavno postali pomembno vprašanje na ravni EU. S tem povezano potrebo po ukrepanju na ravni EU je leta 2019 poudaril Evropski svet ter pozval k usklajenemu pristopu in sodelovanju držav članic pri tem čezmejnem vprašanju. Komisija se je skupaj z državami članicami hitro odzvala na nove pomisleke glede varnosti 5G. Skupina za sodelovanje na področju varnosti omrežij in informacij je leta 2020 sprejela nabor orodij EU za kibernetско varnost tehnologije 5G, v okviru katerega so navedeni številni strateški, tehnični in podporni ukrepi za obravnavo groženj za varnost omrežij 5G, za vsakega od njih pa so opredeljeni tudi ustrezni akterji. Več ukrepov zadeva vprašanje visoko tveganih dobaviteljev opreme 5G. Ta nabor orodij sta nato odobrila Komisija in Evropski svet (glej odstavke 45 do 47). Ker je zbirka orodij instrument mehkega prava, ti ukrepi za države članice niso zavezujoči. Nedavno je bil nabor orodij EU za kibernetско varnost 5G omenjen v novi evropski strategiji za spodbujanje pametnih, čistih in varnih povezav v digitalnih sistemih po vsem svetu kot orodje za usmerjanje naložb v digitalno infrastrukturo (glej odstavek 50).

85 Z merili iz nabora orodij je zagotovljen operativni okvir, ki je koristen za usklajeno ocenjevanje profila tveganja dobaviteljev v vseh državah članicah, hkrati pa je izvajanje te ocene še vedno v nacionalni pristojnosti (glej odstavek 54).

86 Od sprejetja nabora orodij je bil dosežen napredek pri krepitvi varnosti omrežij 5G, saj večina držav članic uporablja omejitve za visoko tvegane dobavitelje ali to namerava storiti. Do oktobra 2021 je zakonodajo o varnosti 5G ob upoštevanju tega okvira sprejelo ali spremenilo 13 držav članic. Preostale države članice se pripravljajo na predložitev zakonodaje, v kateri bodo upoštevana merila iz nabora orodij (glej odstavka [54](#) in [75](#)).

87 Nabor orodij je bil sicer sprejet v zgodnji fazi uvajanja omrežij 5G, vendar je več operaterjev mobilnih omrežij takrat že izbralo svoje dobavitelje opreme 5G (glej odstavke [52](#)). Če pomisleki glede varnosti niso obravnavani že pri oblikovanju politike, obstaja tveganje negativnega učinka na njeno izvajanje, npr. pričakovane koristi (npr. rast BDP) so zaradi stroškov, potrebnih za obravnavo groženj (npr. stroški kibernetске kriminalitete), lahko manjše ali izničene (glej odstavka [02](#) in [04](#)).

88 V zbirki orodij so upoštewane nacionalne pristojnosti in relevantni dejavniki, značilni za posamezne države. Pri reviziji Sodišča se je pokazalo, da so bili doslej pristopi držav članic k uporabi opreme visoko tveganih dobaviteljev ali obsegu omejitev različni (na primer, da veljajo samo za jedrne in kritične dele omrežij 5G ali za radijsko dostopovno omrežje ali njegov del) (glej odstavka [74](#) in [75](#)).

89 V prihodnjih letih bi lahko zakonodaja o varnosti omrežij 5G, ki bi jo na podlagi nabora orodij sprejele države članice, privedla do bolj usklajenih pristopov k visoko tveganim dobaviteljem 5G. Ker pa nobeden od ukrepov, določenih v tem naboru orodij, ni pravno zavezujoč, Komisija nima pooblastil za njihovo izvrševanje. Zato obstaja tveganje, da zgolj z naborom orodij ne bo mogoče zagotoviti, da bi države članice varnostne vidike obravnavale usklajeno (glej odstavke [49](#) do [75](#)).

90 Številni dobavitelji 5G imajo sedež v državah nečlanicah EU in delujejo v okviru zakonodaj tretjih držav, ki se lahko znatno razlikujejo od standardov EU, na primer glede uspešnega varstva podatkov, ki so ga deležni državljani, ali bolj na splošno glede tega, kako se z zakonodajnim ali demokratičnim sistemom zavor in ravnesij zagotavlja neodvisnost sodstva. Tudi to, da omrežja 5G delujejo predvsem na podlagi programske opreme, je lahko eden od večjih pomislekov glede varnosti, če so centri za nadzor te programske opreme v državah nečlanicah EU, zaradi česar bi lahko za državljane EU morda veljala zakonodaja tretjih držav. Komisija je začela obravnavati te pomisleke, saj meni, da bi morale vsako podjetje, ki zagotavlja storitve državljanom EU, spoštovati pravila in vrednote EU. Poleg tega je z več državami začela dialoge, da bi zagotovila močno varstvo zasebnosti osebnih podatkov (glej odstavke [56](#) do [62](#)).

91 Kljub čezmejni naravi pomislekov glede varnosti 5G je o pristopih držav članic k vprašanju varnosti in njihovi odvisnosti od visoko tveganih dobaviteljev na voljo le malo javnih informacij. Komisija spremlja izvajanje nabora orodij in poročila o tem izvajanju, vendar poročila ne vsebujejo podrobnih in primerljivih informacij o pristopih držav članic k pomislekom glede varnosti 5G. Poleg tega glede na stanje septembra 2021 nadaljnje poročanje ni bilo načrtovano. To pomanjkanje informacij ovira izmenjavo znanja med državami članicami in možnost uporabe usklajenih ukrepov, pa tudi možnost, da bi Komisija predlagala izboljšave varnosti omrežij 5G (glej odstavke [68](#) do [73](#)).

Priporočilo 2 – Spodbujati usklajen pristop držav članic k varnosti 5G

Komisija naj:

- (a) zagotovi nadaljnje smernice ali podporne ukrepe o ključnih elementih nabora orodij EU za kibernetško varnost tehnologije 5G, npr. o merilih za oceno dobaviteljev 5G in njihovo razvrstitev med visoko tvegane ter o pomislekih glede varstva podatkov;

Časovni okvir: december 2022.

- (b) spodbuja transparentnost pristopov držav članic k varnosti 5G s spremljanjem izvajanja varnostnih ukrepov iz nabora orodij EU za kibernetško varnost tehnologije 5G in poročanjem o tem izvajanju, in sicer s skupnim sklopom ključnih kazalnikov smotrnosti;

Časovni okvir: december 2022.

- (c) skupaj z državami članicami oceni, za katere vidike varnosti omrežij 5G je treba določiti izvršljive zahteve, in po potrebi uporabi pravico do zakonodajne pobude.

Časovni okvir: december 2022.

92 Komisija je začela obravnavati obtožbe o nepošteni ekonomski prednosti zaradi tujih subvencij. Z njimi se lahko izkrivlja notranji trg in s tem povzročijo neenaki konkurenčni pogoji za dobavitelje 5G, kar ima lahko posledice za varnost (glej odstavke [78](#)).

93 Komisija nima dovolj informacij glede tega, kako bi države članice obravnavale morebitne stroške nadomestitve, ki bi lahko nastali, če bi morali operaterji mobilnih omrežij brez prehodnega obdobja odstraniti opremo visoko tveganih dobaviteljev iz omrežij EU. Razlike v obravnavi lahko ogrozijo poslovno varnost in pravočasno uvajanje 5G (glej odstavka [79](#) in [80](#)). Poleg tega lahko pristopi držav članic k varnosti 5G in zlasti neusklajenost pristopov v EU vplivajo na uspešno delovanje enotnega trga. Komisija tega problema doslej še ni ocenila (glej odstavke [74](#) do [76](#)).

Priporočilo 3 – Spremljati pristope držav članic k varnosti 5G in oceniti učinek različnih pristopov na uspešno delovanje enotnega trga

Komisija naj:

- (a) spodbuja transparenten in dosleden pristop držav članic k obravnavi stroškov operaterjev mobilnih omrežij za nadomestitev opreme 5G, kupljene od visoko tveganih dobaviteljev, in sicer z rednim spremljanjem te tematike in poročanjem o njej v okviru izvajanja nabora orodij EU za kibernetско varnost 5G;
- (b) oceni, kakšen bi bil učinek, če bi ena država članica svoja omrežja 5G gradila z uporabo opreme dobavitelja, ki v drugi državi članici šteje za visoko tvegane.

Časovni okvir: december 2022.

To poročilo je sprejel senat II, ki ga vodi članica Evropskega računskega sodišča Iliana Ivanova, v Luxembourggu 15. decembra 2021.

Za Evropsko računsko sodišče

Klaus-Heiner Lehne
predsednik

Priloge

Priloga I – Glavne priložnosti in tveganja v zvezi s 5G

PRILOŽNOSTI	TVEGANJA
+	–
Razvoj novih tehnologij v podjetjih	Tveganja za zasebnost
+	–
Večja mobilnost in posodobitev prometnega sistema	Grožnje za nacionalno varnost
+	–
Nadaljnje omogočanje medsebojne povezljivosti vsakdanjih fizičnih predmetov	Odvisnost od dobavne verige
+	–
Izboljšanje uporabe elektronskih postopkov v zdravstvu (e-zdravje)	Kibernetski napadi
+	–
Povečanje varnosti državljanov	Negativni učinki na zdravje
+	–
Podpiranje sprememb družbe pri uporabi medijev	Izguba delovnih mest zaradi povečanja učinkovitosti
+	
Spodbujanje ustvarjanja delovnih mest v številnih sektorjih in preobrazba trga dela	
+	
Krepitev demokracije	
+	
Zmanjšanje digitalnega razkoraka	

Vir: Evropsko računsko sodišče na podlagi [Evropskega vozlišča za znanstvene medije](#), ki ga upravlja služba Evropskega parlamenta za raziskave

Priloga II – Primeri posledic motenj telekomunikacijskih omrežij in kibernetских incidentov

Nedelovanje številka za klic v sili v Franciji^{66,67}

01 Zaradi izpada omrežja Orange, največjega telekomunikacijskega podjetja v Franciji, so bili 3. junija 2021 več ur onemogočeni klici v sili. Čeprav je bilo izključeno, da bi do izpada prišlo zaradi kibernetiskega napada, incident kaže, kakšne bi lahko bile morebitne posledice motenj za kritično omrežno infrastrukturo.

Napadi z izsiljevalskim programjem na javne zdravstvene ustanove na Irskem^{68,69,70}

02 Irska zdravstvena služba (Health Service Executive) je maja 2021 zaradi napada z izsiljevalskim programjem izključila vse svoje sisteme IT. Napad je prizadel vse vidike oskrbe pacientov, saj je povzročil težave pri dostopu do evidenc pacientov, zato se je povečalo tveganje za zamude in napake. Irski uradniki sicer niso zaznali, da bi bili podatki pacientov ogroženi, če pa bi bile zdravstvene evidence razkrite, bi lahko to vodilo do različnih s tem povezanih kaznivih dejanj, kot sta goljufija in izsiljevanje. Generalni direktor zdravstvene službe je navedel, da bodo stroški sanacije sistemov po ocenah verjetno znašali 500 milijonov EUR (600 milijonov 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_DataBreachTodayinRSS-Syndication-in-299786a86ffeab5aec16d55392d94819.20210624.en.html

Solarwinds^{71,72,73}

03 Solarwinds je ameriško podjetje, ki razvija programsko opremo za lažje upravljanje omrežij, sistemov in infrastrukture informacijske tehnologije v podjetjih ter državnih in zveznih agencijah. V začetku leta 2020 je v podjetju prišlo do napada s programsko opremo. Hekerjem se je posrečilo, da so napadli tudi stranke podjetja, in sicer s programskimi nadgradnjami, ki so vsebovale zlonamerne kode, s katerimi so odprli stranska vrata na platformah strank in si tako zagotovili lahek dostop za napade ter namestitev dodatne zlonamerne in vohunske programske opreme.

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>.

Priloga III – Pravni okvir in okvir politik

 Evropska komisija

 Evropski svet
Svet EU

 Zakonodaja

 Skupina za
sodelovanje na
področju varnosti
omrežij in informacij



Priloga IV – Primeri projektov, sofinanciranih iz sklada EFSI

Projekta sklada EFSI, povezana s 5G

Projekta sklada EFSI, ki ju je pregledalo Sodišče, sta bila povezana z naložbami v raziskave, razvoj in inovacije za razvoj portfeljev proizvodov za omrežja 5G. Oba sta vključevala razvoj strojne in programske opreme za radijsko dostopovno omrežje in jedrno omrežje ter sta prispevala h gostejši postavitvi celic, podprla standardizacijo in olajšala ključne tehnološke preizkuse.

Začela sta se leta 2018, končala pa decembra 2020. Njuni skupni naložbeni stroški so znašali 3,9 milijarde EUR, vključno z 1 milijardo EUR financiranja iz sklada EFSI.

Priloga V – Primeri projektov programa Obzorje 2020 in ESRR

Projekt programa Obzorje 2020, povezan s 5G

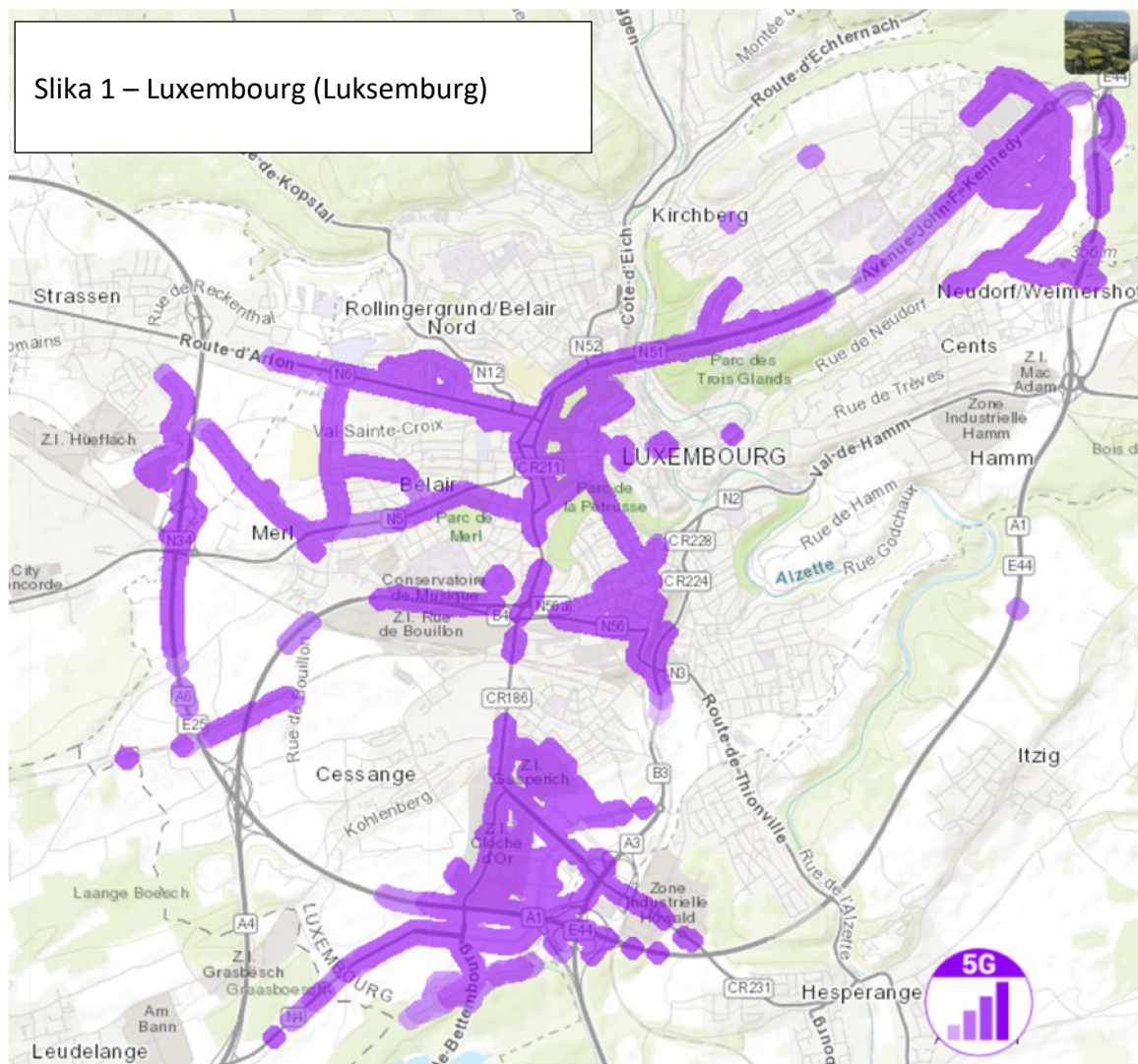
V okviru tega projekta, pri katerem se uporablja oprema vseh treh glavnih dobaviteljev 5G (podjetij Ericsson, Huawei in Nokia), se v čezmejnem koridorju, ki povezuje mesta Metz (Francija), Merzig (Nemčija) in Luxembourg, preizkušajo tehnologije 5G. Projekt se je začel izvajati novembra 2018 in naj bi trajal 31 mesecev. Skupni predvideni stroški znašajo 17,1 milijona EUR, EU pa je prispevala 12,9 milijona EUR.

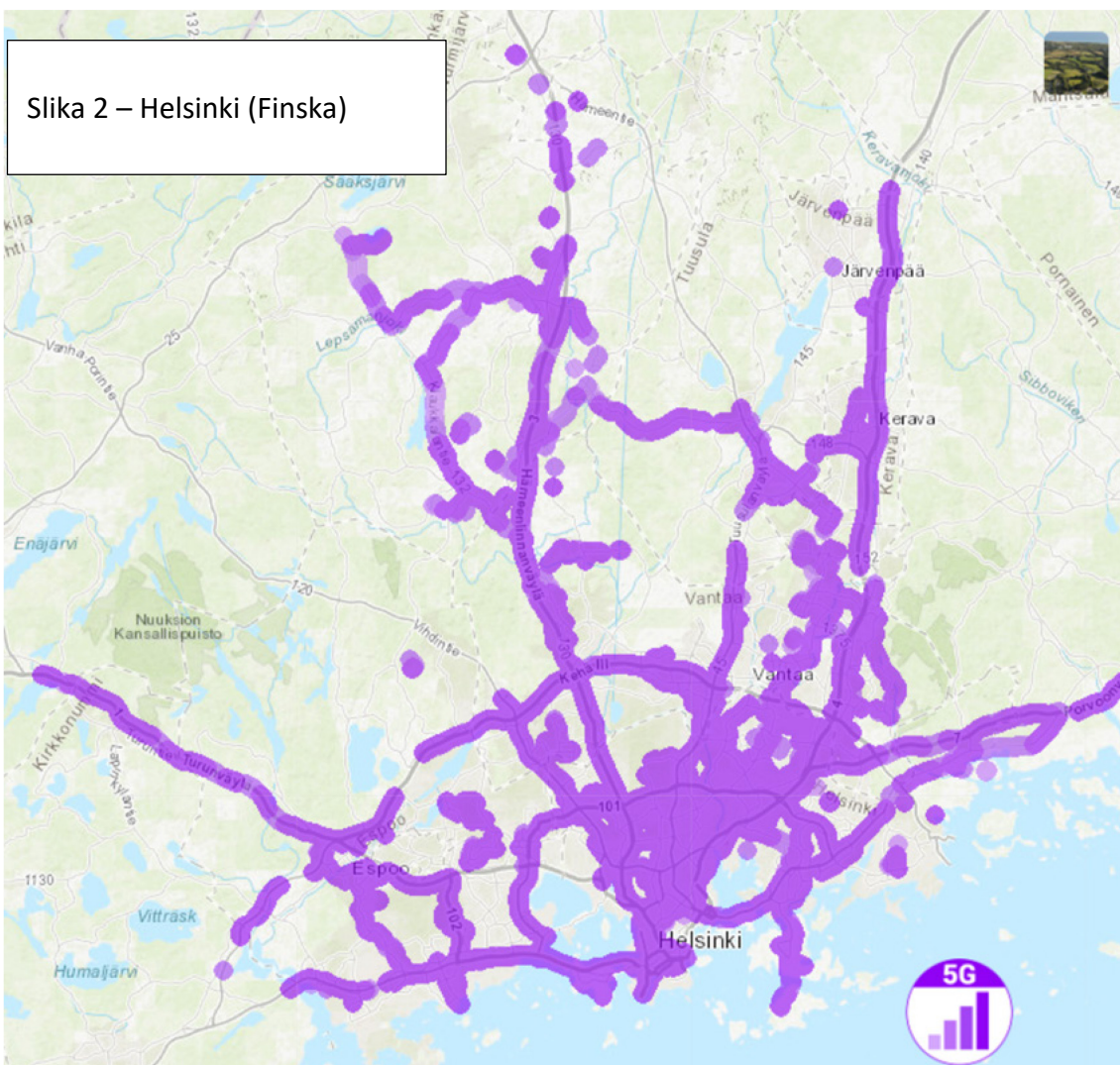
Projekt ESRR, povezan s 5G

Cilj tega projekta, ki se izvaja v Španiji, je zagotoviti uvide v uvajanje omrežij 5G, vključno s preizkušanjem metod upravljanja omrežja, ki jih omogoča tehnologija 5G, kot so virtualizacija omrežij, računalništvo na robu, dinamično dodeljevanje omrežnih storitev in omrežno rezinjenje, ter razvojem primerov uporabe 5G. Projekt se je začel izvajati leta 2019 in naj bi trajal 30 mesecev. Skupni predvideni stroški znašajo 7,1 milijona EUR, EU pa je prispevala 2,2 milijona EUR.

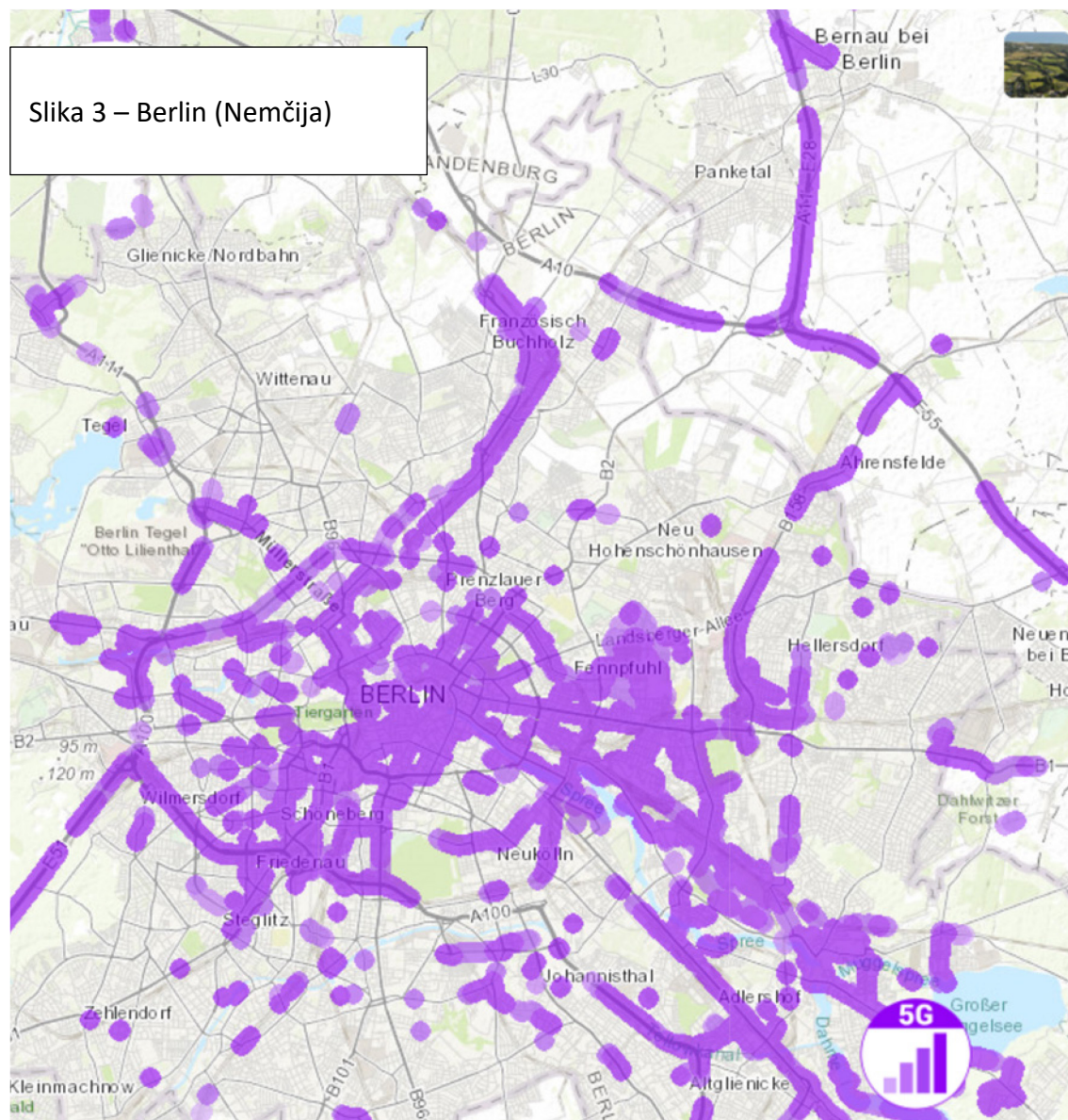
Priloga VI – Pokritost 5G v izbranih mestih

Spodnje slike temeljijo na podatkih o mobilni širokopasovni poveztivosti, zbranih s testi, ki so jih izvedli uporabniki aplikacije [Nperf](#). Območja, kjer je bila zaznana pokritost s 5G, morda niso komercialno odprta. Ker je zmogljivost omrežij odvisna od posameznega operaterja mobilnega omrežja, je na naslednjih zemljevidih, pridobljenih 4. oktobra 2021, prikazana samo pokritost, ne pa tudi vidiki zmogljivosti, kot sta hitrost in latenca.



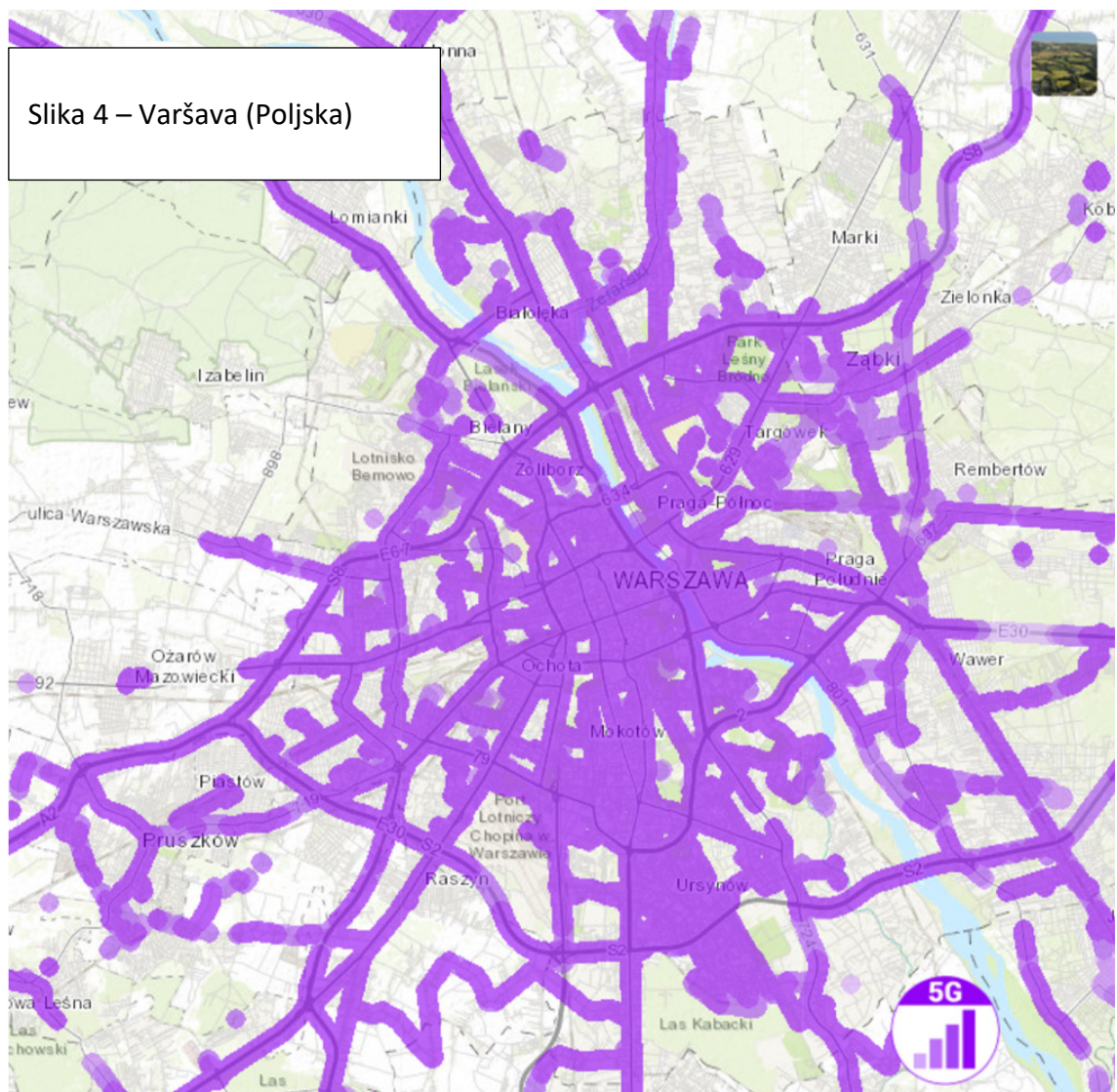


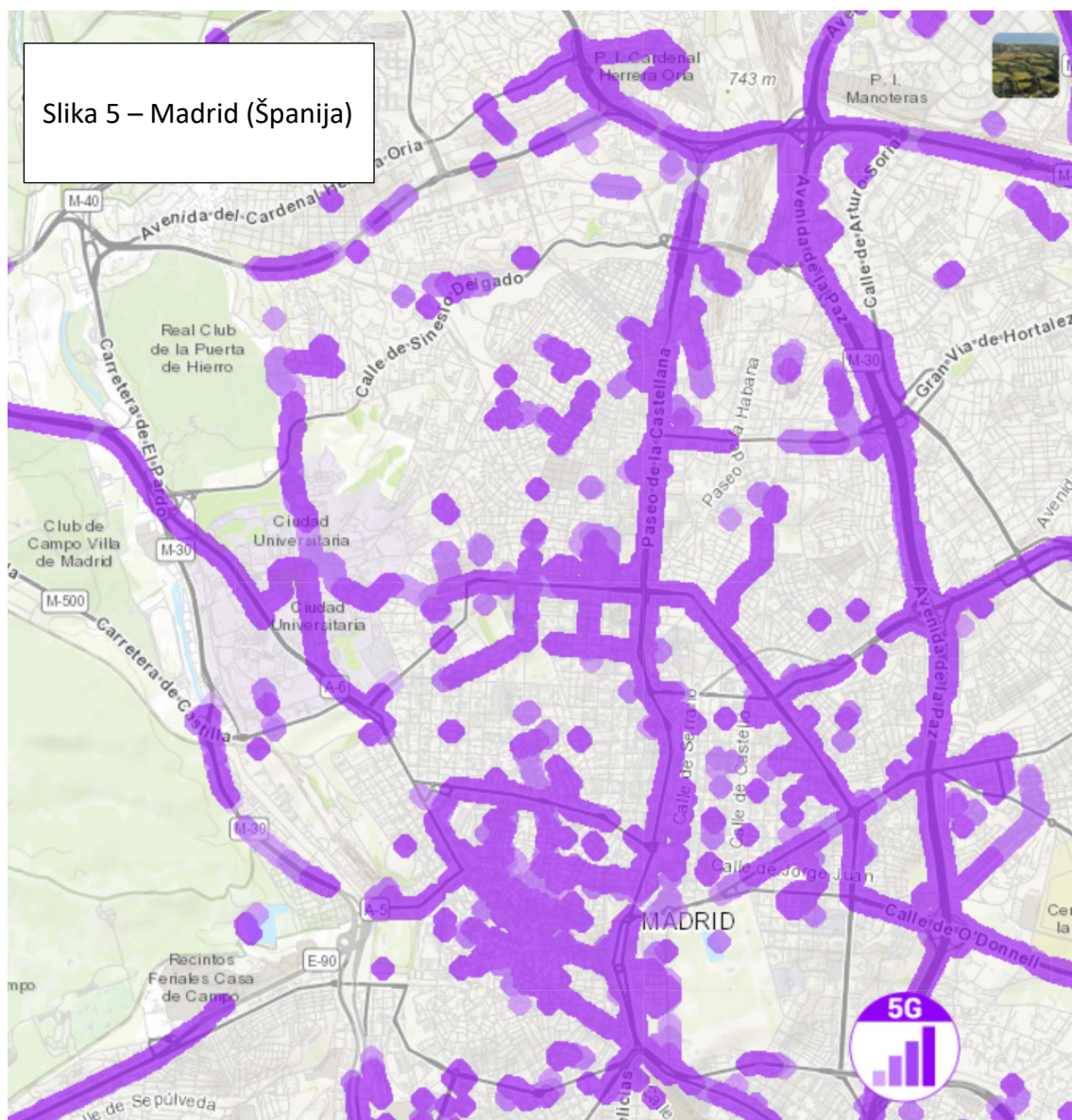
Slika 3 – Berlin (Nemčija)



© nPerf

Slika 4 – Varšava (Poljska)





Priloga VII – Nabor orodij EU za kibernetско varnost tehnologije 5G

Nabor orodij EU za kibernetско varnost tehnologije 5G, ki ga je sprejela skupina za sodelovanje na področju varnosti omrežij in informacij ter odobrila Komisija, vključuje tri vrste nezavezujočih ukrepov (strateške, tehnične in podporne ukrepe), ki jih morajo izvesti različni akterji, kot je povzeto v nadaljevanju.

Ukrepi	Ustrezni akterji				
	Organi držav članic	Operaterji mobilnih omrežij	Evropska komisija	ENISA	Deležniki (vključno z dobavitelji)
Strateški ukrepi					
SU01 – Okrepitev vloge nacionalnih organov	✓	✓			
SU02 – Izvajanje revizij operaterjev in zahtevanje informacij	✓	✓			
SU03 – Ocena profila tveganja dobaviteljev in uporaba omejitev za dobavitelje, ki se štejejo za visoko tvegane, vključno s potrebnimi izključitvami za učinkovito blaženje tveganj, za ključna sredstva	✓	✓			
SU04 – Nadziranje uporabe ponudnikov upravljanih storitev in podpore dobaviteljev opreme na tretji ravni	✓	✓			
SU05 – Zagotavljanje raznolikosti dobaviteljev za posamezne operaterje mobilnih omrežij z ustreznimi strategijami za več dobaviteljev	✓	✓			
SU06 – Okrepitev odpornosti na nacionalni ravni	✓	✓			
SU07 – Opredelitev ključnih sredstev ter spodbujanje raznoliškega in trajnostnega ekosistema 5G v EU	✓		✓		
SU08 – Ohranjanje in krepitev raznolikosti in zmogljivosti EU v prihodnjih omrežnih tehnologijah	✓		✓		✓
Tehnični ukrepi					
TU01 – Zagotavljanje uporabe osnovnih varnostnih zahtev (varna zasnova in arhitektura omrežij)	✓	✓			
TU02 – Zagotavljanje in vrednotenje izvajanja varnostnih ukrepov pri obstoječih standardih 5G	✓	✓			✓
TU03 – Zagotavljanje strogega nadzora nad dostopom	✓	✓			
TU04 – Povečanje varnosti funkcij virtualiziranega omrežja	✓	✓			

Ukrepi	Ustrezni akterji				
	Organi držav članic	Operaterji mobilnih omrežij	Evropska komisija	ENISA	Deležniki (vključno z dobavitelji)
TU05 – Zagotavljanje varnega upravljanja, delovanja in spremljanja omrežij 5G	✓	✓			
TU06 – Okrepitev fizične varnosti	✓	✓			
TU07 – Okrepitev celovitosti, posodabljanja in upravljanja popravkov programske opreme	✓	✓			
TU08 – Zvišanje standardov varnosti v procesih dobaviteljev s strogimi pogoji javnega naročanja	✓	✓			✓
TU09 – Uporaba certifikacije EU za komponente omrežij 5G, opremo odjemalcev in/ali procese dobaviteljev	✓	✓	✓	✓	✓
TU10 – Uporaba certifikacije EU za druge izdelke in storitve IKT, ki niso značilni samo za 5G (povezane naprave, storitve v oblaku)	✓		✓	✓	✓
TU11 – Okrepitev odpornosti in načrtov neprekinjenega poslovanja	✓	✓			✓
Podporni ukrepi					
PU01 – Pregled ali razvoj smernic in najboljših praks za varnost omrežij	✓	✓		✓	
PU02 – Okrepitev zmogljivosti testiranja in izvajanja revizij na nacionalni ravni in ravni EU	✓		✓	✓	
PU03 – Podpiranje in usmerjanje standardizacije 5G	✓	✓	✓	✓	✓
PU04 – Razvoj smernic za izvajanje varnostnih ukrepov pri obstoječih standardih 5G	✓			✓	
PU05 – Zagotavljanje uporabe standardnih tehničnih in organizacijskih varnostnih ukrepov s posebno vseevropsko shemo certificiranja	✓			✓	✓
PU06 – Izmenjava najboljših praks za izvajanje strateških ukrepov, zlasti nacionalnih okvirov za ocenjevanje profila tveganja dobaviteljev	✓				
PU07 – Izboljšanje usklajevanja pri odzivanju na incidente in kriznem upravljanju	✓			✓	
PU08 – Izvajanje revizij medsebojne odvisnosti med omrežji 5G in drugimi kritičnimi storitvami	✓				
PU09 – Okrepitev mehanizmov sodelovanja, usklajevanja in izmenjave informacij	✓			✓	
PU10 – Zagotavljanje, da se pri projektih 5G, podprtih z javnim financiranjem, upoštevajo tveganja za kibernetko varnost	✓		✓		

Vir: Nabor orodij EU za kibernetko varnost tehnologije 5G

Kratice

BDP: bruto domači proizvod

BEREC: Organ evropskih regulatorjev za elektronske komunikacije

EFSI: Evropski sklad za strateške naložbe

EIB: Evropska investicijska banka

ENISA: Agencija Evropske unije za varnost omrežij in informacij

ESRR: Evropski sklad za regionalni razvoj

RSPG: Skupina za politiko radiofrekvenčnega spektra

Glosar

Agencija Evropske unije za kibernetisko varnost: agencija EU, vzpostavljena za razvoj varnosti omrežij in informacij na visoki ravni ter njeno ohranjanje v vseh sektorjih zasebnega in javnega življenja.

Eksabajt: merska enota za zmogljivost shranjevanja digitalnih informacij, ki je enakovredna 1 milijardi gigabajtov.

Evropski sklad za strateške naložbe: mehanizem za podporo naložbam, ki sta ga vzpostavili Evropska investicijska banka (EIB) in Komisija v okviru naložbenega načrta za Evropo zaradi spodbujanja zasebnih naložb v projekte strateškega pomena za EU.

Global System for Mobile Communications Association: panožna organizacija, ki zastopa interese mobilnih operaterjev po vsem svetu, pa tudi proizvodnih in storitvenih podjetij in organizacij, ki imajo interes za mobilno infrastrukturo.

Internet stvari: fizični predmeti z vgrajenimi senzorji, programsko opremo in drugimi tehnologijami, ki jim omogočajo, da se brezžično povežejo in izmenjujejo podatke z drugimi napravami in sistemi.

Izsiljevalsko programje: zlonamerna programska oprema, ki žrtvam onemogoči dostop do računalniškega sistema ali povzroči, da datoteke niso berljive. Za ponoven dostop so žrtve prisiljene plačati odkupnino.

Latenca: čas, v katerem nabor podatkov v računalniškem omrežju pripotuje od ene točke do druge.

Nacionalni načrti za širokopasovne povezave: dokumenti držav članic, ki vsebujejo strateške cilje za doseganje ciljev EU na področju širokopasovnih povezav.

Operater mobilnega omrežja: telekomunikacijsko podjetje, ki zagotavlja brezžično glasovno in podatkovno komuniciranje za uporabnike mobilnih telefonov z naročnino.

Organ evropskih regulatorjev za elektronske komunikacije: organ, v katerem so predstavniki nacionalnih regulativnih organov držav članic in ki tem organom in Komisiji pomaga pri izvajanju regulativnega okvira EU, da bi vzpostavili enotni trg za elektronske komunikacije.

Radijsko dostopovno omrežje: pomemben del sodobne telekomunikacijske tehnologije, ki posamezne naprave z radijskimi povezavami povezuje z drugimi deli omrežja.

Radiofrekvenčni spekter: del elektromagnetnega spektra, ki ustreza radijskim frekvencam.

Skupina za politiko radiofrekvenčnega spektra: svetovalna skupina na visoki ravni, sestavljena iz predstavnikov držav članic, ki pomaga in svetuje institucijam EU pri razvoju enotnega trga za brezžične proizvode in storitve.

Skupina za sodelovanje na področju varnosti omrežij in informacij: organ, ustanovljen z direktivo o varnosti omrežij in informacijskih sistemov za zagotavljanje sodelovanja in izmenjave informacij med državami članicami. Sestavljajo ga predstavniki držav članic EU, Evropske komisije in Agencije EU za kibernetsko varnost.

Širokopolasovna povezava: zelo hiter hkratni prenos več oblik informacij (kot so podatki, zvok in video).

Odgovori Komisije

<https://www.eca.europa.eu/sl/Pages/DocItem.aspx?did=60614>

Časovni okvir

<https://www.eca.europa.eu/sl/Pages/DocItem.aspx?did=60614>

Revizijska ekipa

V posebnih poročilih Sodišča so predstavljeni rezultati njegovih revizij politik in programov EU ali tem v zvezi z upravljanjem na posameznih področjih proračuna. Sodišče izbira in načrtuje revizijske naloge tako, da je njihov učinek kar največji, in pri tem upošteva tveganje za smotrnost ali skladnost, višino ustreznih prihodkov ali porabe, prihodnji razvoj ter politični in javni interes.

To revizijo smotrnosti poslovanja je opravil revizijski senat II – Naložbe v kohezijo, rast in vključevanje, ki ga vodi članica Evropskega računskega sodišča Iliana Ivanova. Revizijo je vodila članica Evropskega računskega sodišča Annemie Turtelboom, pri njej pa so sodelovali vodja njenega kabineta Florence Fornaroli, ataše v njenem kabinetu Celil Ishik, vodilni upravni uslužbenec Niels-Erik Brokopp, vodja naloge Paolo Pesce ter revizorji Jussi Bright, Rafal Gorajski, Zuzana Gullová, Alexandre Tan, Aleksandar Latinov in Nils Westphal.



Annemie Turtelboom



Florence Fornaroli



Celil Ishik



Niels-Erik Brokopp



Paolo Pesce



Jussi Bright



Rafal Gorajski



Zuzana Gullová



Aleksandar Latinov



Nils Westphal

COPYRIGHT

© Evropska unija, 2022

Politika Evropskega računskega sodišča (Sodišča) glede ponovne uporabe se izvaja s sklepom [Decision of the European Court of Auditors No 6-2019](#) o politiki odprtih podatkov in ponovni uporabi dokumentov.

Če ni drugače navedeno (npr. v posameznih obvestilih o avtorskih pravicah), so vsebine Sodišča, ki so v lasti EU, pod licenco [Creative Commons Attribution 4.0 International \(CC BY 4.0\)](#). To pomeni, da je ponovna uporaba dovoljena, če se ustrezno navede vir in označijo spremembe. Oseba, ki dokumente ponovno uporabi, ne sme potvoriti njihovega prvotnega pomena ali sporočila. Sodišče ni odgovorno za morebitne posledice ponovne uporabe.

Če so na gradivu prikazane določljive fizične osebe, npr. na fotografijah uslužbencev Sodišča, ali če gradivo vsebuje dela tretjih oseb, je treba pridobiti dodatne pravice. Kadar je pridobljeno dovoljenje, se z njim razveljavi in nadomesti zgoraj omenjeno splošno dovoljenje, zato morajo biti v njem jasno navedene omejitve glede uporabe.

Za uporabo in prikazovanje vsebin, katerih lastnica ni EU, je morda treba pridobiti dovoljenje neposredno od imetnikov avtorskih pravic:

— Slike v Prilogi VI: © [nPerf](#), podjetje nPerf SAS

Programska oprema ali dokumenti, za katere veljajo pravice industrijske lastnine, kot so patenti, blagovne znamke, registrirani modeli, logotipi in imena, niso vključeni v politiko Sodišča glede ponovne uporabe in vam niso dani na voljo v okviru licence.

Na spletiščih institucij Evropske unije znotraj domene europa.eu so povezave do spletišč tretjih oseb. Ker Sodišče na ta spletišča ne more vplivati, vas poziva, da preberete njihove dokumente o politiki glede varstva osebnih podatkov in avtorskih pravic.

Uporaba logotipa Evropskega računskega sodišča

Logotip Sodišča se ne sme uporabiti brez njegove predhodne privolitve.

PDF	ISBN 978-92-847-7417-3	ISSN 1977-5784	doi:10.2865/867462	QJ-AB-21-029-SL-N
HTML	ISBN 978-92-847-7393-0	ISSN 1977-5784	doi:10.2865/417221	QJ-AB-21-029-SL-Q

Zaradi omrežij 5G naj bi se evropski BDP med letoma 2021 in 2025 povečal za do 1 bilijon EUR, s potencialom za nastanek ali preobrazbo do 20 milijonov delovnih mest v vseh gospodarskih sektorjih. Sodišče je ugotovilo, da je zaradi zamud ogrožena uresničitev ciljev EU glede uvajanja omrežij 5G in da so za obravnavo varnostnih vprašanj potrebna nadaljnja prizadevanja. Sodišče je v poročilu Komisiji dalo več priporočil, katerih namen je pospešiti pravočasno in usklajeno uvajanje varnih omrežij 5G v EU.

Posebno poročilo Sodišča v skladu z drugim pododstavkom člena 287(4) PDEU.



EVROPSKO
RAČUNSKO
SODIŠČE



Urad za publikacije
Evropske unije

EVROPSKO RAČUNSKO SODIŠČE
12, rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel. +352 4398-1

Vprašanja: eca.europa.eu/sl/Pages/ContactForm.aspx

Spletišče: eca.europa.eu

Twitter: @EUAuditors