HR 2022

03

Tematsko izvješće

Uvođenje 5G mreža u EU-u:

bilježe se kašnjenja u uvođenju mreža, a određena sigurnosna pitanja i dalje nisu riješena

EUROPSKI REVIZORSKI SUD

Sadržaj

Sažetak

I. „Peta generacija” telekomunikacijskih sustava, odnosno 5G, novi je svjetski bežični standard koji nudi puno veći podatkovni kapacitet i brzine prijenosa. 5G usluge neophodne su za širok raspon inovativnih aplikacija koje bi mogle preobraziti velik broj sektora naših gospodarstava i poboljšati svakodnevicu građana. Stoga 5G tehnologija ima stratešku važnost za cijelo jedinstveno tržište.

II. U svojem akcijskom planu za 5G iz 2016. Komisija je predstavila cilj kojim bi se do 2025. zajamčila kontinuirana pokrivenost 5G mrežama u gradskim područjima i duž glavnih prometnih pravaca. U ožujku 2021. Komisija je taj cilj proširila na pokrivenost 5G mrežama svih naseljenih područja do 2030.

III. 5G mreže imaju potencijal potaknuti brojne mogućnosti za rast, ali donose i određene rizike. U svojoj preporuci iz 2019. o kibersigurnosti 5G mreže Komisija je upozorila da bi zbog oslanjanja velikog broja ključnih usluga na 5G mreže posljedice širih poremećaja bile osobito ozbiljne. Osim toga, zbog prekogranične naravi povezanih prijetnji bilo kakva veća slabost ili kibersigurnosni incidenti u jednoj od država članica nepovoljno bi utjecali na cijeli EU. Jedan od ishoda Komisijine preporuke bio je paket instrumenata EU-a za kibersigurnost 5G mreža („paket instrumenata”) koji je donesen u siječnju 2020.

IV. Diljem EU-a ukupni trošak uvođenja 5G mreža mogao bi dosegnuti iznos od 400 milijardi eura. U razdoblju 2014. – 2020. EU je osigurao financijska sredstva za projekte 5G mreža u iznosu koji premašuje 4 milijarde eura.

V. Sud je ispitao je li Komisija državama članicama pružila djelotvornu potporu u njihovu ostvarenju ciljeva EU-a za usklađeno uvođenje 5G mreža i rješavanja sigurnosnih pitanja u vezi s 5G mrežama. Sud je proveo procjenu aspekata povezanih s uvođenjem 5G mreža, za koju je 2020. bila ključna godina, kao i procjenu aspekata povezanih sa sigurnošću 5G mreža. Ovim izvješćem Sud nastoji pružiti uvide i preporuke za pravodobno uvođenje sigurnih 5G mreža u svim državama članicama EU-a. Revizija koju je Sud obavio bila je usmjerena na Komisiju, no njome se ispitala i uloga nacionalnih uprava i drugih aktera.

VI. Revizijom je utvrđeno da se kasni s uvođenjem 5G mreža u državama članicama. Do kraja 2020. 23 države članice već su pokrenule komercijalne 5G usluge i ostvarile srednjoročni cilj prema kojemu najmanje jedan veliki grad ima pristup 5G uslugama. Međutim, pojedine države članice u svojim nacionalnim strategijama za 5G mreže ili

planovima za razvoj širokopojasnog pristupa internetu ne upućuju na ciljeve EU-a za 2025. i 2030. Osim toga, u nekoliko zemalja Europski zakonik elektroničkih komunikacija još nije prenesen u nacionalno pravo i kasni se s dodjelom frekvencijskog spektra 5G mreže. Ta kašnjenja u dodjeli odgovarajućeg spektra mogu se pripisati raznim razlozima: slaboj potražnji među operatorima pokretnih mreža, poteškoćama u prekograničnoj koordinaciji sa zemljama izvan EU-a koje s njim dijele istočne granice, učinku pandemije bolesti COVID-19 na raspored dražbi i neizvjesnostima u pogledu načina rješavanja sigurnosnih pitanja. Ostvarenje ciljeva EU-a potencijalno je ugroženo zbog mjere u kojoj države članice zaostaju u uvođenju 5G mreža. Komisija inicijativama i smjernicama obvezujućeg i neobvezujućeg prava te financiranjem istraživanja povezanog s 5G mrežama podupire države članice u njihovoj provedbi akcijskog plana za 5G iz 2016. Međutim, Komisija nije jasno utvrdila očekivanu razinu kvalitete 5G usluga.

VII. U paketu instrumenata EU-a za kibersigurnost 5G mreža navodi se niz strateških i tehničkih mjera te mjera potpore za suočavanje sa sigurnosnim prijetnjama 5G mrežama i utvrđuju relevantni akteri za svaku od tih mjera. Nekoliko mjera odnosi se na pitanje visokorizičnih dobavljača 5G opreme. Paket instrumenata odobrili su Komisija i Europsko vijeće. Kriterijima u paketu nudi se operativni okvir koristan za obavljanje procjene profila rizičnosti dobavljača na usklađen način u svim državama članicama. No obavljanje te procjene istodobno je i dalje u nadležnosti država članica. Paket instrumenata donesen je u ranoj fazi uvođenja 5G mreža, no niz operatora pokretnih mreža u tom je trenutku već bio odabrao svoje dobavljače. Otkako je paket donesen, ostvaren je napredak u povećanju sigurnosti 5G mreža i u većini država članica primjenjuju se ograničenja na visokorizične dobavljače ili je u tijeku proces primjene takvih ograničenja. U narednim godinama zakonodavstvom o sigurnosti 5G mreža koje države članice donesu na temelju paketa instrumenata mogao bi se postići usklađeniji pristup prema visokorizičnim dobavljačima 5G opreme. Međutim, budući da nijedna od predloženih mjera nije pravno obvezujuća, Komisija nema ovlasti za jamčenje njihova provođenja. Stoga i dalje postoji rizik da se samim paketom instrumenata ne može zajamčiti usklađen pristup država članica u rješavanju sigurnosnih mrežnih aspekata.

VIII. Komisija je počela raditi na rješavanju pitanja stranih subvencija za dobavljače 5G opreme koje mogu imati posljedice za sigurnost. Komisija ne raspolaže dovoljnim informacijama o postupanju država članica u pogledu potencijalnih troškova zamjene koji bi mogli nastati u slučajevima kada bi operatori pokretnih mreža trebali ukloniti opremu visokorizičnih dobavljača iz mreža EU-a bez prijelaznog razdoblja.

IX. Sud preporučuje Komisiji da:

- promiče ujednačeno i pravodobno uvođenje 5G mreža unutar EU-a;
- potiče primjenu usklađenog pristupa sigurnosti 5G mreža u državama članicama; i
- prati pristupe država članica sigurnosti 5G mreža te procijeni učinak razlika u njihovim pristupima na djelotvorno funkcioniranje jedinstvenog tržišta.

Uvod

Narav i važnost 5G mreža

01. „Peta generacija” telekomunikacijskih sustava, odnosno 5G, novi je svjetski bežični standard. U usporedbi s 3G i 4G mrežama 5G mreža nudi puno veći podatkovni kapacitet i brzine prijenosa. 5G mreža uključuje određene mrežne elemente koji se temelje na prethodnim generacijama mobilnih i bežičnih komunikacijskih tehnologija, ali ona ne proizlazi iz postupnog razvoja tih mreža. Pojedinačnim korisnicima i povezanim uređajima 5G mreža jamči univerzalnu širokopojasnu povezivost vrlo visokog kapaciteta i niske latencije.

02. S pomoću „interneta stvari” 5G mrežama povezat će se više uređaja no ikad dosad. Procijenjeno je da je do kraja 2018. u cijelom svijetu bilo u upotrebi 22 milijarde povezanih uređaja. Predviđa se da će se taj broj povećati na oko 50 milijardi do 2030.[1], čime će se stvoriti golema mreža međusobno povezanih uređaja u rasponu od pametnih telefona pa sve do kuhinjskih aparata. Očekuje se da će globalna potrošnja podatkovnog prometa skočiti s 12 eksabajta mobilnog podatkovnog prometa mjesečno 2017.[2] na više od 5 000 eksabajta do 2030[3].

03. 5G usluge neophodne su za širok raspon inovativnih aplikacija koje bi mogle preobraziti velik broj sektora gospodarstva EU-a i poboljšati svakodnevicu građana (vidjeti ***sliku 1.***). U jednoj studiji iz 2017. provedenoj za Komisiju navodi se da bi koristi uvođenja 5G mreža u četiri ključna strateška industrijska sektora (automobilski, zdravstveni, prometni i energetski) mogle doseći čak 113 milijardi eura godišnje[4]. U studiji se isto tako predviđa da bi se uvođenjem 5G mreža moglo potaknuti otvaranje 2,3 milijuna radnih mjesta u državama članicama. U jednoj drugoj studiji iz 2021. procjenjuje se da bi doprinos 5G mreže europskom bruto domaćem proizvodu (BDP) u

---

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., veljača 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”, veljača 2017.

razdoblju 2021. – 2025. mogao dosegnuti iznos do 1 bilijuna eura uz potencijal za otvaranje ili preobrazbu do 20 milijuna radnih mjesta u svim sektorima gospodarstva[5].

Slika 1. – 5G mrežom obuhvatit će se svi aspekti našeg života

Izvor: Europska komisija.

Sigurnosna pitanja

04. Iako 5G mreža ima potencijal potaknuti brojne mogućnosti za rast, ona donosi i određene rizike (vidjeti ***Prilog I.*** u kojemu se ističu glavne mogućnosti i rizici 5G mreže). Jedan takav rizik čine sigurnosne prijetnje. Telekomunikacijskim sustavima oduvijek su prijetili kibernapadi (vidjeti ***Prilog II.***)[6]. Sigurnosna pitanja u pogledu 5G mreže izazivaju posebnu zabrinutost jer za razliku od telekomunikacijskih sustava 3G i 4G mreža 5G mreža nudi veći prostor za napade zbog naravi svoje tehnologije i posebno svojeg oslanjanja na softver[7].

05. Budući da se očekuje da će 5G mreže postati okosnica širokog raspona usluga i aplikacija, dostupnost tih mreža postat će veliki izazov u pogledu sigurnosti na nacionalnoj razini i razini EU-a. Ako hakeri provale u neku 5G mrežu, mogu ugroziti njezine ključne funkcije kako bi poremetili usluge ili preuzeli kontrolu nad ključnom infrastrukturom (na primjer, električnom mrežom) koja u EU-u često nadilazi državne

---

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

[6] Pregled br. 02/2019: Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a (Informativni dokument); Zbirka revizija Kontaktnog odbora za 2020. – Kibersigurnost; i Služba Europskog parlamenta za istraživanja – Europsko znanstveno-medijsko čvorište.

[7] Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, „EU coordinated risk assessment of the cybersecurity of 5G networks”, 9.10.2019. Točka 3.4.

granice. U studijama se procjenjuje da gospodarski učinak kiberkriminala može dosegnuti iznos od 5 000 milijardi eura godišnje na svjetskoj razini, tj. iznos veći od 6 % svjetskog BDP-a tijekom 2020.[8]

06. Još jedan izazov za sigurnost 5G mreža donosi ključna uloga ograničenog broja dobavljača u uspostavi i radu 5G mreža. Izloženost mogućim poremećajima u opskrbi povećava se kada postoji ovisnost o samo jednom dobavljaču, osobito ako je s njime povezan visok stupanj rizika, jer primjerice na njega mogu utjecati pojedine zemlje izvan EU-a. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, koju čine predstavnici država članica i tijela EU-a, istaknula je 2019. rizik od „neprijateljskih državnih aktera" koji bi si mogli osigurati jednostavnu ulaznu točku u 5G mrežu na temelju povlaštenog pristupa, izvršavanjem pritiska na dobavljača ili pozivanjem na nacionalne pravne obveze[9] (vidjeti ***okvir 1.***). U tom je kontekstu EU počeo raditi na razvoju inicijativa u području sigurnosti 5G mreža.

Okvir 1.

Sigurnosna pitanja u kontekstu suradnje EU-a i Kine na 5G mrežama

- EU je s Kinom 2015. potpisao zajedničku izjavu o strateškoj suradnji na 5G mrežama kojom se obvezao na uzajamnost i otvorenost u pogledu pristupa financiranju istraživanja u području 5G mreža i pristupa tržištu 5G mreža[10].
- Kina je 2017. donijela zakon o nacionalnim obavještajnim aktivnostima kojim se sve kineske organizacije i građane obvezuje na suradnju u nacionalnim obavještajnim aktivnostima uz primjenu zaštitnih mjera u pogledu tajnosti[11]. SAD je 2018. na to odgovorio poduzimanjem mjera za ograničavanje poslovanja nekoliko kineskih poduzeća, uključujući Huawei, koji je jedan od ključnih dobavljača 5G opreme.

---

[8] Svjetski gospodarski forum, „Wild Wide Web – Consequences of Digital Fragmentation", 2021.

[9] Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, „EU coordinated risk assessment of the cybersecurity of 5G networks", 9.10.2019.

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

[11] Rezolucija Europskog parlamenta od 12. ožujka 2019.; Zakon o nacionalnim obavještajnim aktivnostima Narodne Republike Kine, članak 14. Vidjeti i njegov engleski prijevod na https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

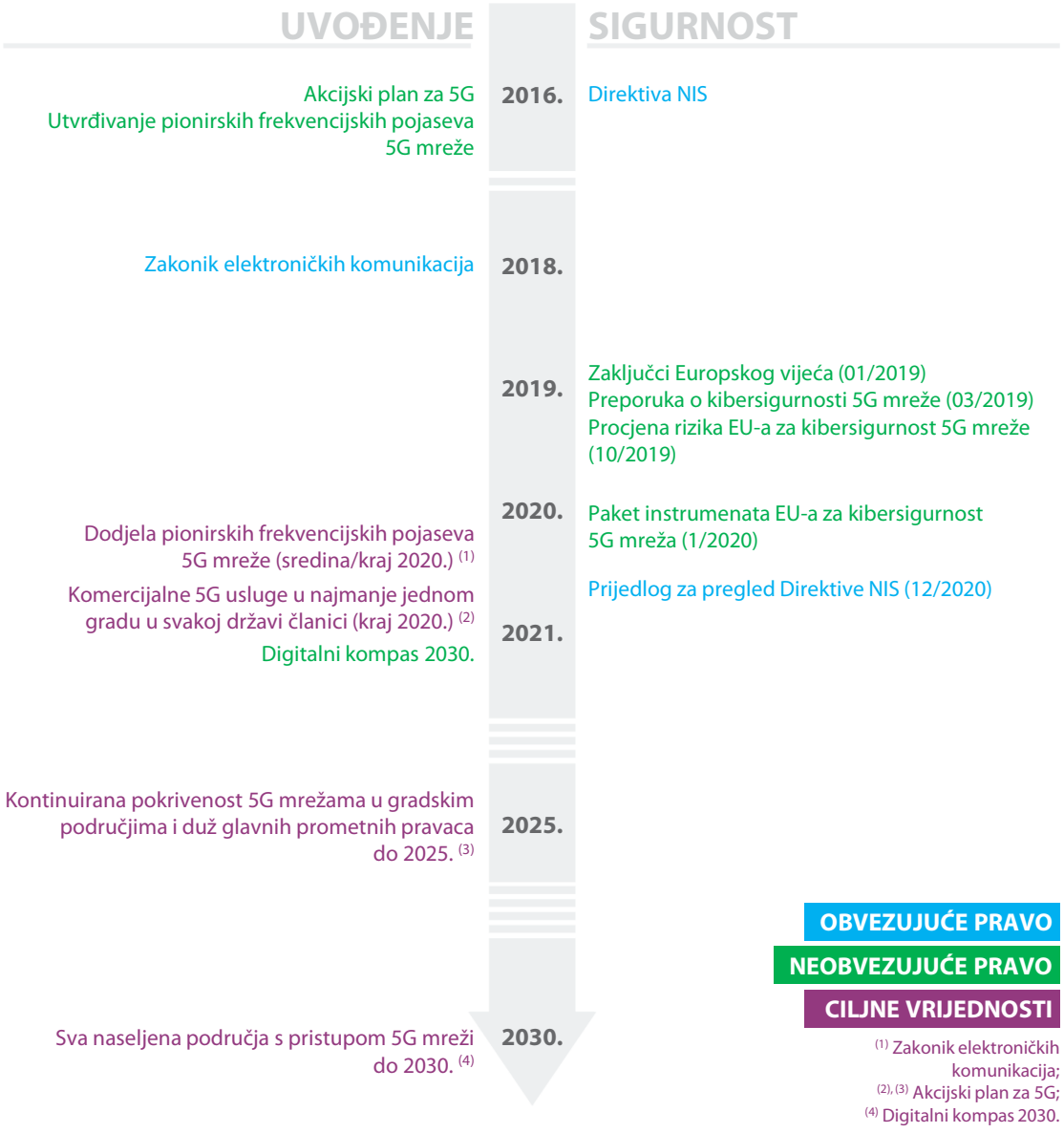
U ožujku 2019. Europski parlament izrazio je zabrinutost i zbog činjenice da bi s kineskim dobavljačima 5G opreme mogao biti povezan sigurnosni rizik za EU zbog zakona koji se primjenjuju u njihovoj zemlji podrijetla.

07. Povjerljivost i privatnost također su potencijalno ugrožene jer telekomunikacijski operatori često eksternaliziraju pohranjivanje svojih podataka u podatkovnim centrima. Postoji opasnost da se takvi podatci pohranjuju na opremi dobavljača 5G opreme koji se nalaze u zemljama izvan EU-a u kojima su razine pravne i podatkovne zaštite drukčije nego u EU-u.

Inicijative za 5G mreže poduzete na razini EU-a

08. Okvir politike koji se odnosi na 5G mreže i njihovu sigurnost čine „obvezujuće pravo" čija je primjena obvezna i može se zajamčiti (na primjer uredbe) i „neobvezujuće pravo" (na primjer komunikacije Komisije). U ***Prilogu III.*** predstavljeni su pravni okvir i okvir politike. Na ***slici 2.*** prikazani su glavni dokumenti politike uz ključne ciljne vrijednosti.

Slika 2. – Glavni dokumenti politike i ključne ciljne vrijednosti koji se odnose na uvođenje i sigurnost 5G mreža



Izvor: Sud.

Uloge i obveze

09. Iako su operatori pokretnih mreža odgovorni za sigurno uvođenje 5G mreža upotrebom opreme koju nabavljaju od dobavljača tehnologije, a države članice odgovorne za nacionalnu sigurnost, sigurnost 5G mreža pitanje je od strateške važnosti za cijelo jedinstveno tržište i tehnološku suverenost EU-a[12]. Stoga Komisija i agencije

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

EU-a podupiru i koordiniraju djelovanje država članica u pogledu tehničkih i sigurnosnih aspekata 5G mreža.

10 U *tablici 1* dodatno se obrazlažu glavne uloge i obveze u području 5G mreža.

Tablica 1. – Uloge i obveze

	Komisija i agencije EU-a	Tijela država članica	Operatori pokretnih mreža i dobavljači 5G opreme
Raspodjela i dodjela pionirskih frekvencijskih pojaseva 5G mreže		✓	
Definiranje politike EU-a o 5G mrežama	✓	✓	
Uvođenje 5G mreža			✓
Ulaganje i financiranje	✓	✓	✓
Nacionalna sigurnost		✓	
Sigurnost 5G mreža		✓	✓
Potpora i koordinacija djelovanja država članica	✓		

Izvor: Sud.

Trošak uvođenja 5G mreža i povezana financijska potpora EU-a

Ukupni trošak uvođenja 5G mreža u svim državama članicama mogao bi dosegnuti 400 milijardi eura

11. Prema procjenama iz 2021. ukupni trošak uvođenja 5G mreža u svim državama članicama EU-a do 2025. mogao bi dosegnuti iznos između 281 i 391 milijarde eura. Taj iznos ravnomjerno je raspodijeljen na izgradnju nove infrastrukture za 5G mreže i nadogradnju fiksne infrastrukture kako bi se postigle gigabitne brzine[13]. Većinu tih ulaganja moraju financirati operatori pokretnih mreža.

[13] Procjena koju je Komisija obavila na temelju podataka iz EIB-a, analize, priopćenja udruge GSMA i raznih poduzeća te izvješća udruženja ETNO – Europske telekomunikacije, „Connectivity & Beyond: How Telcos Can Accelerate a Digital Future for All”, ožujak 2021.

U razdoblju 2014. – 2020. EU je osigurao potporu za razvoj 5G mreža u iznosu većem od 4 milijarde eura

12. Tijekom razdoblja 2014. – 2020. EU je osigurao potporu za razvoj 5G mreža u iznosu većem od 4 milijarde eura izravno iz proračuna EU-a i financiranjem sredstvima Europske investicijske banke (EIB). Iz proračuna EU-a financirali su se projekti isključivo povezani s istraživanjem, dok je EIB financirao projekte i u području istraživanja i u području uvođenja.

13. EIB je bio najveći pružatelj financijskih sredstava EU-a za projekte povezane s 5G mrežama. Prema stanju zabilježenom u kolovozu 2021. EIB je izdao zajmove u ukupnom iznosu od 2,5 milijardi eura za devet projekata 5G mreža u pet država članica[14]. Osim toga, za razdoblje 2014. – 2020. stavljeno je na raspolaganje 1,9 milijardi eura iz proračuna EU-a. U ***tablici 2.*** sažeto su prikazani glavni izvori financijske potpore EU-a za 5G mreže.

Tablica 2. – Financiranje 5G mreža sredstvima EU-a (2014. – 2020.)

Financijska sredstva EU-a	Iznos
EIB	2,485 milijardi eura[1]
Europski fond za strateška ulaganja (EFSU)	1 milijarda eura[2]
Obzor 2020.	755 milijuna eura[3]
EFRR	Najmanje 147 milijuna eura[4]

(1) Popis projekata za koje se pruža potpora financijskim sredstvima iz EIB-a.
(2) Popis projekata za koje se pruža potpora financijskim sredstvima iz EFSU-a.
(3) Informativna stranica o programu Obzor 2020.
(4) Skup podataka o projektima sufinanciranima iz EFRR-a tijekom višegodišnjeg financijskog okvira za razdoblje 2014. – 2020.

Izvor: Sud.

14. U okviru EFSU-a (kojim upravlja EIB) pružena je potpora za dva projekta kojima je cilj gušće postavljanje ćelija i podupiranje standardizacije. Ukupni trošak ulaganja za te projekte iznosio je 3,9 milijardi eura, uključujući financijska sredstva u iznosu od 1 milijarde eura iz EFSU-a (vidjeti ***Prilog IV.***).

[14] Popis projekata za koje se pruža potpora financijskim sredstvima EIB-a.

15. Komisija je od 2014. izravno sufinancirala i više od stotinu projekata 5G mreža, i to uglavnom financijskim sredstvima iz programa Obzor 2020., i u manjoj mjeri sredstvima iz EFRR-a. U ***Prilogu V.*** prikazani su primjeri takvih projekata.

Mehanizmom za oporavak i otpornost osigurat će se dodatno financiranje sredstvima EU-a za uvođenje 5G mreža u narednim godinama

16. Mehanizmom za oporavak i otpornost osigurat će se dopunski izvor financiranja za uvođenje 5G mreža u narednim godinama. Prema stanju iz rujna 2021. 16 država članica planiralo je financirati uvođenje 5G mreža u okviru Mehanizma za oporavak i otpornost, a njih 10 odlučilo je da to neće učiniti. Zadnja država članica još nije dostavila relevantne informacije.

Opseg revizije i revizijski pristup

17. Ovom revizijom Sud je procijenio podupire li Komisija djelotvorno države članice u:

- postizanju ciljeva EU-a za 2025. i 2030. koji se odnose na uvođenje 5G mreža; i
- usklađenom rješavanju sigurnosnih pitanja u vezi s 5G mrežama.

Sud je u oba navedena područja također ispitao mjere i aktivnosti država članica.

18. U ovom izvješću pojam „sigurnost 5G mreža" odnosi se na kibersigurnost i sigurnost hardvera/softvera. Sud je ispitao i sigurnost i uvođenje 5G mreža za koje je 2020. bila ključna godina (vidjeti ***sliku 2.***). Svojim izvješćem Sud nastoji pružiti uvide i preporuke za pravodobno uvođenje sigurnih 5G mreža u EU-u.

19. Revizijom koju je Sud obavio obuhvaćeno je razdoblje od 2016. do svibnja 2021. Sud je u najvećoj mogućoj mjeri uključio dodatne ažurirane informacije. Revizijske aktivnosti Suda obuhvaćale su sljedeće:

- pregled zakonodavstva EU-a, inicijativa Komisije i druge relevantne dokumentacije;
- razgovore s predstavnicima Komisije, EIB-a, Tijela europskih regulatora za elektroničke komunikacije (BEREC), Agencije Europske unije za kibersigurnost (ENISA), telekomunikacijskih udruženja, operatora pokretnih mreža, dobavljača 5G opreme, međunarodnih organizacija, stručnjaka u predmetnom području radi stjecanja uvida, kao i s tijelima u Finskoj, Njemačkoj, Poljskoj i Španjolskoj. Odabir država članica temeljio se na kriterijima kao što su iznos financijskih sredstava EU-a namijenjen za projekte 5G mreža, razina napretka u njihovu uvođenju i uzimanje u obzir ravnomjerne zemljopisne zastupljenosti;
- ispitivanje nacionalnih regulatornih tijela za telekomunikacije iz svih 27 država članica EU-a kako bi se dobio širi uvid u izazove 5G tehnologije u državama članicama; i
- pregled 10 sufinanciranih projekata EU-a (EFSU, EFRR i Obzor 2020.) koji se odnose na 5G tehnologiju odabranih u ogledne svrhe.

20. Sud se također oslonio na svoj nedavni pregled odgovora EU-a na kinesku strategiju ulaganja pod državnom kontrolom[15], kao i na prethodna izvješća, kao što su izvješće o širokopojasnom pristupu internetu[16], inicijativi za digitalizaciju europske industrije[17] i kibersigurnosnoj politici EU-a[18].

[15] Pregled br. 03/2020 „Odgovor EU-a na kinesku strategiju ulaganja pod državnom kontrolom".

[16] Tematsko izvješće br. 12/2018 „Širokopojasni pristup internetu u državama članicama EU-a: postignut je određen napredak, ali neće se dosegnuti sve ciljne vrijednosti iz strategije Europa 2020."

[17] Tematsko izvješće br. 19/2020 „Digitalizacija europske industrije: ambiciozna inicijativa čiji uspjeh ovisi o kontinuiranoj predanosti EU-a, vlada i poduzeća".

[18] Pregled br. 02/2019 „Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a (informativni dokument)".

Opažanja

Kašnjenjima u uvođenju 5G mreža ugrožavaju se izgledi za ostvarenje ciljeva EU-a za 2025. i 2030.

21. Kad je riječ o pravodobnom uvođenju 5G mreža, Sud je ispitao sljedeće:

- jesu li države članice ostvarile zadovoljavajući napredak u pogledu uvođenja 5G mreža;
- je li Komisija pružila odgovarajuću potporu državama članicama; i
- jesu li države članice uklonile ključne prepreke brzom uvođenju 5G mreža.

Države članice zaostaju u uvođenju 5G mreža

Komisija je utvrdila rokove za uvođenje 5G mreža u svojem akcijskom planu za 5G iz 2016.

22. U svojem akcijskom planu za 5G iz 2016. Komisija je predložila rokove za uvođenje 5G mreža u EU-u: države članice trebale su pokrenuti prve 5G mreže do kraja 2018., potpuno komercijalne 5G usluge u najmanje jednom velikom gradu do kraja 2020. i zajamčiti kontinuiranu pokrivenost 5G mrežama u gradskim područjima i duž glavnih prometnih pravaca do 2025.

23. U ožujku 2021. Komisija je dodala još jedan rok za pokrivenost 5G mrežama svih naseljenih područja do 2030.[19]

U 23 države članice komercijalne 5G usluge pokrenute su prije kraja 2020.

24. Do kraja 2020. 23 države članice ostvarile su cilj prema kojemu najmanje jedan veliki grad ima pristup 5G uslugama. Samo Cipar, Litva, Malta i Portugal nisu uspjeli ostvariti taj cilj. Prema stanju na kraju listopada 2021. samo Litva i Portugal još nisu nudili 5G usluge ni u jednom od svojih gradova.

---

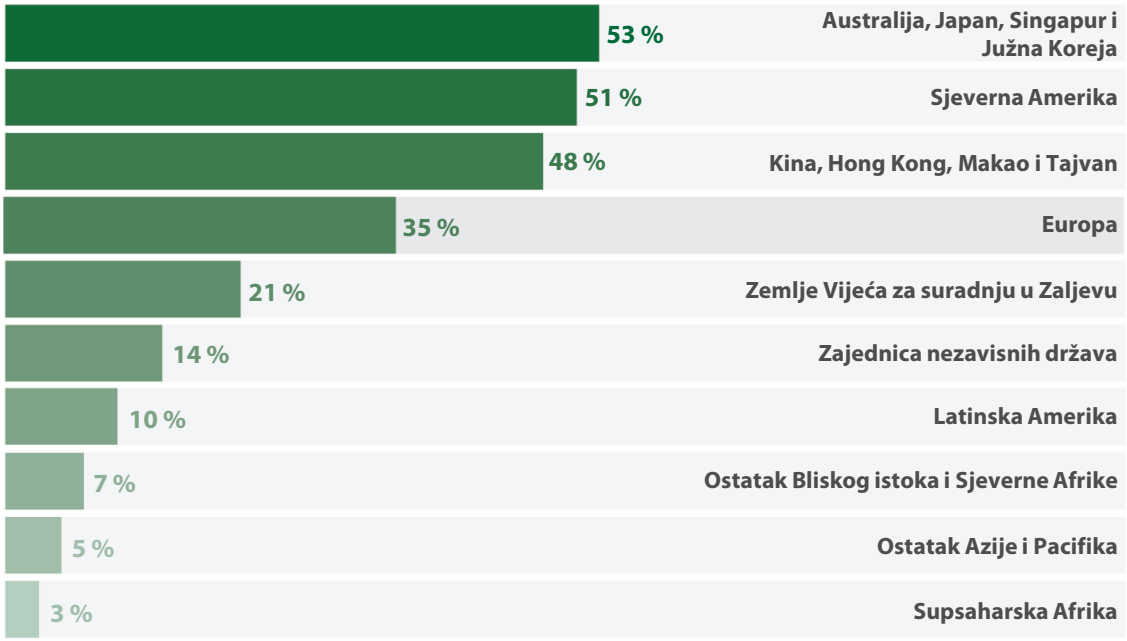
[19] Europska komisija, Digitalni kompas 2030.: europski pristup za digitalno desetljeće, COM(2021) 118 final.

Postoji opasnost da većina država članica neće ispuniti rokove utvrđene za 2025. i 2030.

25. Prema jednoj nedavnoj studiji Komisije izgledno je da će samo 11 država članica ostvariti kontinuiranu pokrivenost 5G mrežama u svim svojim gradskim područjima i duž glavnih kopnenih prometnih pravaca do 2025.[20] Komisija smatra da je vjerojatnost za ostvarenje tog cilja za preostalih 16 država članica srednja (Austrija, Češka, Estonija, Njemačka, Irska, Poljska, Litva i Slovenija) ili niska (Belgija, Bugarska, Hrvatska, Cipar i Grčka).

26. Jedna organizacija iz predmetnog sektora, Udruga za globalni sustav pokretnih telekomunikacija (engl. *Global System for Mobile Communications Association* (GSMA)), istaknula je 2021. da uvođenje 5G mreža u EU-u napreduje drukčijim tempom u odnosu na druge dijelove svijeta. Na primjer, procijenila je da će se do 2025. 51 % svih mobilnih veza u Sjevernoj Americi temeljiti na 5G mrežama, ali bi taj postotak u Europi (što uključuje i zemlje izvan EU-a), kako se očekuje, trebao iznositi tek 35 % (vidjeti ***sliku 3.***).

Slika 3. – 5G veze izražene kao udio u ukupnim mobilnim vezama do 2025.



Izvor: GSMA.„The Mobile Economy 2021.”.

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

27. Postoji velika opasnost da trenutačnim tempom uvođenja većina država članica neće ispuniti rok utvrđen za 2025., a time ni rok za 2030. koji se odnosi na pokrivenost svih naseljenih područja 5G mrežama. U tom kontekstu Sud je ispitao je li Komisija državama članicama pružila djelotvornu potporu kako bi ostvarile ciljeve EU-a za uvođenje i pokretanje 5G mreža do 2025. i 2030.

U potpori koju Komisija pruža državama članicama postoje određeni nedostatci

Komisija nije definirala očekivanu kvalitetu usluge 5G mreža

28. Komisija dosad nije definirala očekivanu kvalitetu usluge 5G mreža, npr. u pogledu najmanje brzine i najveće latencije. Osim toga, u akcijskom planu iz 2016. od država članica zatraženo je da do kraja 2020. pokrenu „potpuno komercijalne” 5G usluge u Europi, no bez definiranja tih koncepata koji su povezani s kvalitetom.

29. Zbog nedovoljne jasnoće u pogledu očekivane kvalitete usluge postoji opasnost da države članice te uvjete tumače na različite načine. Sud je istaknuo primjere različitih pristupa uvođenju 5G mreža u državama članicama (vidjeti ***okvir 2.***).

Okvir 2.

Primjeri različitih pristupa uvođenju 5G mreža

Brzina i latencija dva su ključna aspekta funkcionalnosti usluga za čije se pružanje koriste 5G mreže. Na primjer, telekirurgija ili industrijska automatizacija koje se temelje na 5G mrežama zahtijevaju vrlo veliku brzinu i nisku latenciju. Međutim, dosad su samo dvije države članice (Njemačka i Grčka) definirale zahtjeve u pogledu najmanje brzine i najveće latencije[21].

Potrebu da „najmanje jedan veliki grad ima pristup 5G uslugama do kraja 2020.” države članice različito tumače. To dovodi do situacije u kojoj grad klasificiran kao grad koji „ima pristup 5G uslugama” može podrazumijevati raspon gradova u kojima samo nekoliko ulica ima pristup 5G mrežama, kao što je Luxembourg, do gradova čije gotovo cijelo gradsko područje ima pristup 5G mreži, kao što je Helsinki. U ***Prilogu VI.*** navode se primjeri pokrivenosti za odabrane gradove.

[21] Izvješće 5G opservatorija „5G Observatory Quarterly Report 12”, do lipnja 2021.

30. Potraje li, ta bi situacija mogla dovesti do nejednakosti u pristupu 5G uslugama u EU-u i njihovoj kvaliteti („digitalni jaz”): građani u jednom dijelu EU-a imali bi bolji pristup 5G mrežama i bolju kvalitetu 5G mreža nego građani u drugim dijelovima EU-a. Digitalni jaz mogao bi utjecati i na potencijal za gospodarski razvoj jer 5G tehnologija može revolucionarizirati sektore kao što su zdravstvena skrb, obrazovanje i radna snaga samo ako je popraćena dovoljno uspješnom funkcionalnošću 5G mreža.

31. Potrebno je razjasniti i očekivanu uspješnost 5G mreža s obzirom na inicijativu Komisije da se uvede veća transparentnost u pogledu kvalitete usluge koju pružaju operatori pokretnih mreža za roaming, o kojoj je Komisija nedavno iznijela zakonodavni prijedlog[22].

Tromjesečno izvješćivanje Komisije o uvođenju 5G mreža nije uvijek pouzdano

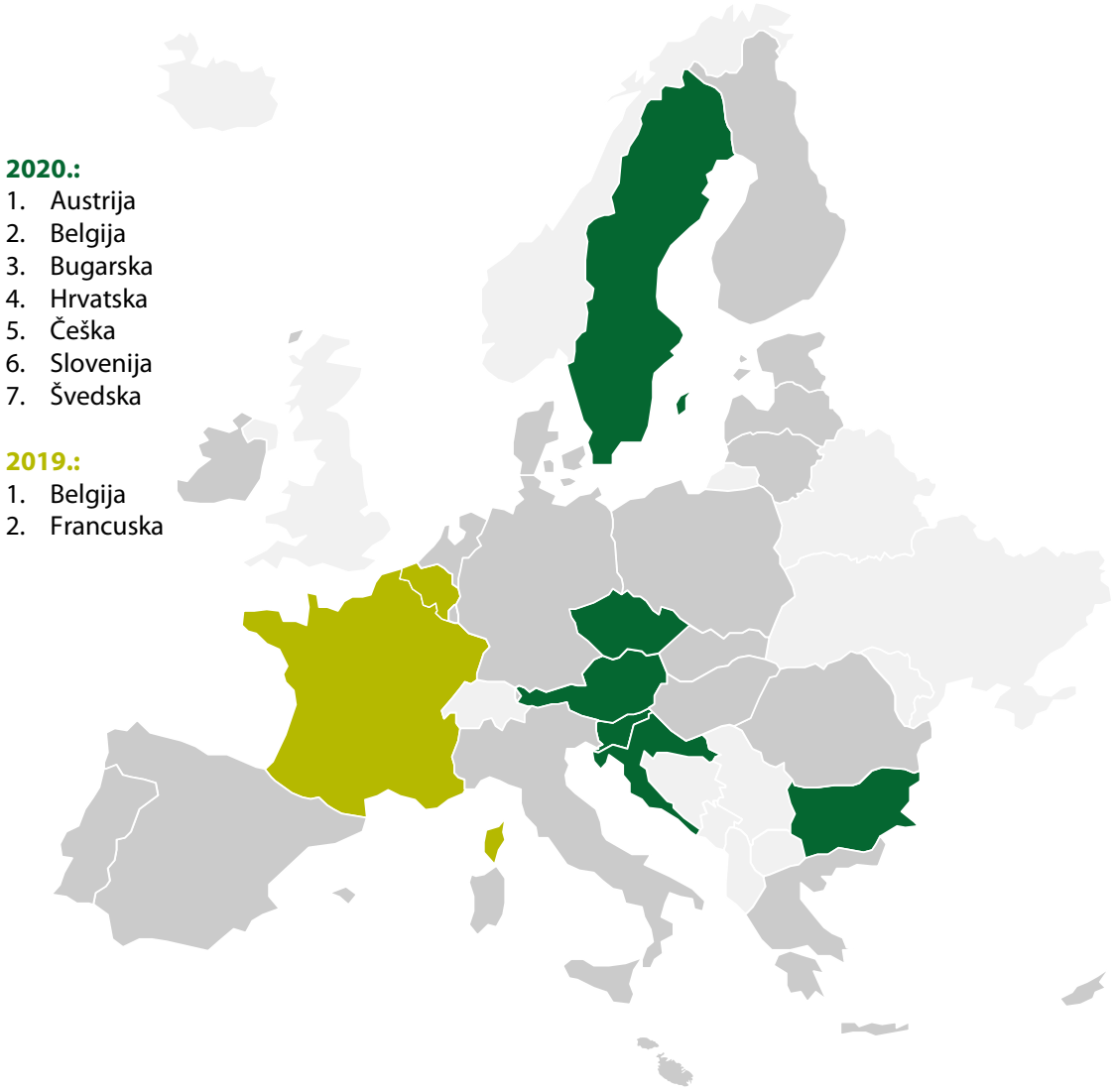
32. Komisija prati razinu uvedenosti 5G mreža u državama članicama s pomoću 5G opservatorija. Taj opservatorij pruža informacije o uvođenjima 5G mreža i o strategijama država članica za 5G mreže na tromjesečnoj osnovi. Međutim, Sud je utvrdio da za dvije od četiri preispitane države članice informacije sadržane u tim izvješćima nisu uvijek bile pouzdane. Na primjer, u tromjesečnom izvješću br. 10, u kojemu su iznesene informacije iz razdoblja do kraja prosinca 2020., naveden je mnogo manji broj općina s 5G mrežama u Finskoj od stvarnoga broja (40 umjesto 70) i nisu pružene informacije o činjenici da su u Poljskoj odgođene dražbe frekvencijskog spektra 5G mreže (vidjeti odlomak ***42***.).

Komisija je tek nedavno iskoristila proces europskog semestra za praćenje napretka država članica u uvođenju 5G mreža

33. Sud je utvrdio da je Komisija u posljednje dvije godine u većoj mjeri iskoristila proces europskog semestra za poticanje napretka država članica u uvođenju 5G mreža. Preporuke po državama članicama koje se izravno odnose na 5G mreže povećale su se s preporuka upućenih dvjema državama članicama 2019. na sedam država članica 2020. (vidjeti ***sliku 4.***).

[22] Europska komisija, Prijedlog uredbe o roamingu u javnim pokretnim komunikacijskim mrežama u Uniji (preinaka), COM(2021) 85 final od 24.2.2021.

Slika 4. – Preporuke po državama članicama o 5G mrežama



Izvor: Sud, na temelju preporuka po državama članicama.

Države članice i dalje moraju ukloniti ključne prepreke brzom uvođenju 5G mreža

34. Da bi se ostvarili ciljevi EU-a za uvođenje 5G mreža do 2025. i 2030., države članice moraju ispuniti tri ključna osnovna preduvjeta: strateški preduvjet jamčenjem da se ti ciljevi jasno odražavaju u njihovim nacionalnim strategijama za 5G mreže ili nacionalnim planovima za razvoj širokopojasnog pristupa internetu[23], zakonodavni preduvjet prenošenjem Europskog zakonika elektroničkih komunikacija iz 2018.[24] u

[23] Studija Komisije „Study on National Broadband Plans in the EU-27”.

[24] Direktiva (EU) 2018/1972 o Europskom zakoniku elektroničkih komunikacija.

nacionalno zakonodavstvo i preduvjet usmjeren na poslovanje, i to dodjelom odgovarajućeg spektra[25]. U ***tablici 3.*** pruža se pregled napretka država članica u ispunjavanju tih triju preduvjeta.

[25] Komunikacija Europske komisije, Sigurno uvođenje 5G mreža u EU-u – Provedba paketa instrumenata EU-a, COM(2020) 50 final.

Tablica 3. – Stanje u pogledu ispunjenosti osnovnih preduvjeta za ostvarivanje ciljeva za 2025.

Država članica	Nacionalni plan za razvoj širokopojasnog pristupa internetu u skladu s ciljevima za 2025.	Prenošenje Europskog zakonika elektroničkih komunikacija	Pionirski frekvencijski pojasevi 5G mreže (kolovoz 2021.)			Vjerojatnost ostvarenja cilja
			700 MHz	3,6 GHz	26 GHz	
Belgija				privremena upotreba		mala
Bugarska		✓		✓		mala
Češka	✓	✓	✓	✓		srednja
Danska		✓	✓	✓	✓	velika
Njemačka	✓	✓	✓	✓	✓	srednja
Estonija						srednja
Irska				✓		srednja
Grčka	✓	✓	✓	✓	✓	mala
Španjolska	✓		✓	✓		velika
Francuska	✓	✓	✓	✓		velika
Hrvatska			✓	✓	✓	mala
Italija			✓	✓	✓	velika
Cipar	✓		✓	✓		mala
Litva	✓					srednja
Latvija				✓		velika
Luksemburg			✓	✓		velika
Mađarska	✓	✓	✓	✓		velika
Malta		✓				srednja
Nizozemska	✓		✓			srednja
Austrija	✓	✓	✓	✓		srednja
Poljska	✓					srednja
Portugal				privremena upotreba		srednja do visoka
Rumunjska						velika
Slovenija	✓		✓	✓	✓	srednja
Slovačka			✓			velika
Finska	✓	✓	✓	✓	✓	velika
Švedska	✓		✓	✓		velika

Izvor: studija Komisije „Study on National Broadband Plans in the EU-27”, 5G opservatorij i RSPG.

Malo je država članica u svoje nacionalne strategije za 5G mreže uključilo ciljeve uvođenja 5G mreža do 2025. i 2030.

35. Države članice utvrđuju svoju politiku o 5G mrežama u vidu posebnih nacionalnih strategija za 5G mreže ili ažuriranjem svojih postojećih nacionalnih planova za razvoj širokopojasnog pristupa internetu. U studiji Komisije iz 2021. o nacionalnim planovima za razvoj širokopojasnog pristupa internetu[26] ističe se da je samo 14 država članica u svoje nacionalne strategije za 5G mreže ili ažurirane planove za razvoj širokopojasnog pristupa internetu uključilo cilj EU-a da se uvede „kontinuirana pokrivenost 5G mrežama u svim gradskim područjima i duž glavnih kopnenih prometnih pravaca do 2025." (vidjeti ***tablicu 3.***). Takvo uključivanje ključno je za potporu uspješnoj provedbi predmetne politike.

Većina država članica nije prenijela Direktivu o Europskom zakoniku elektroničkih komunikacija u svoje nacionalno zakonodavstvo do kraja 2020.

36. Direktivu o Europskom zakoniku elektroničkih komunikacija kojom se utvrđuju zadaće nacionalnih regulatornih i drugih nadležnih tijela i određuju rokovi za dodjelu pionirskih frekvencijskih pojaseva 5G mreže države članice trebale su prenijeti u svoje zakonodavstvo do 21. prosinca 2020. Do kraja veljače 2021. samo su tri države članice (Finska, Grčka i Mađarska) objavile da su donijele sve potrebne mjere za prenošenje Direktive. Stoga je Komisija protiv preostale 24 države članice pokrenula postupke zbog povrede prava[27].

37. Na kraju studenoga 2021. i dalje su se vodila 23 postupka zbog povrede prava. Iako očekuje da će uskoro zaključiti postupke zbog povrede prava u slučaju šest država članica (Austrija, Bugarska, Češka, Francuska, Njemačka i Malta), Komisija će postupke protiv ostalih 17 država članica možda morati uputiti Sudu EU-a[28] (vidjeti ***tablicu 3.***).

Kasni se s dodjelom pionirskih frekvencijskih pojaseva 5G mreže

38. Komisija i države članice utvrdile su 2016. tri pionirska frekvencijska pojasa koja će se upotrebljavati za 5G usluge:

- frekvencijskim spektrom od 700 Mhz olakšava se prodiranje bežičnog signala kroz zgrade i operatorima se omogućuje šira pokrivenost (stotine kvadratnih

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

[27] Priopćenje za tisak koje je objavila Europska komisija IP/21/206 od 4.2.2021.

[28] Priopćenje za tisak koje je objavila Europska komisija IP/21/4612 od 23.9.2021.

kilometara). Međutim, brzina i latencija 5G mreže tek su za nijansu bolje od 4G mreže (sa 150 na 250 megabita po sekundi);

- srednjepojasnim frekvencijskim spektrom od 3,6 GHz mogu se prenositi znatne količine podataka (do 900 megabita po sekundi) na znatne udaljenosti (u krugu od nekoliko kilometara); i
- visokopojasnim frekvencijskim spektrom od 26 GHz mogu se proizvesti velike brzine od 1 do 3 gigabita po sekundi na kratkim udaljenostima (tj. kraćima od 2 km), no osjetljiviji je na smetnje.

39. Očekivalo se da države članice niskopojasni spektar stave u primjenu do 30. lipnja 2020.[29], a potom i srednjepojasni i visokopojasni spektar do 31. prosinca 2020.[30] Međutim, do kraja 2020. države članice dodijelile su manje od 40 % ukupnih dostupnih pionirskih frekvencijskih pojaseva (vidjeti ***tablicu 4.***):

- pojas 700 MHz dodijeljen je u 13 država članica;
- frekvencijski pojas od 3,6 GHz dodijeljen je u 17 država članica (uključujući dvije države članice koje su dopustile privremenu upotrebu); i
- frekvencijski pojas od 26 GHz dodijeljen je u četiri države članice.

Do kraja listopada 2021. stopa dodjele povećala se na 53 %[31].

[29] Odluka (EU) 2017/899 o uporabi frekvencijskog pojasa 470 – 790 MHz u Uniji.

[30] Direktiva (EU) 2018/1972 o Europskom zakoniku elektroničkih komunikacija.

[31] 5G opservatorij i RSPG.

Tablica 4. – Stanje u pogledu dodjele pionirskih frekvencijskih pojaseva 5G mreže zabilježeno u prosincu 2020.

Država članica	700 MHZ	3,6 GHZ	26 GHZ
Belgija		privremena upotreba	
Bugarska			
Češka	✓	✓	
Danska	✓	✓	✓
Njemačka	✓	✓	✓
Estonija		–	
Irska		✓	
Grčka	✓	✓	✓
Španjolska		✓	
Francuska	✓	✓	
Hrvatska			
Italija		✓	✓
Cipar	✓	✓	
Latvija		✓	
Litva			
Luksemburg	✓	✓	
Mađarska	✓	✓	
Malta			
Nizozemska	✓		
Austrija	✓	✓	
Poljska			
Portugal		privremena upotreba	
Rumunjska			
Slovenija			
Slovačka	✓	✓	
Finska	✓	✓	✓
Švedska	✓	✓	

Izvor: 5G opservatorij i RSPG.

Kašnjenja u dodjeli pionirskih frekvencijskih pojaseva mogu se pripisati nizu razloga

40. Sud je utvrdio da su kašnjenja u dodjeli frekvencijskog pojasa od 26 GHz uglavnom izazvana slabom potražnjom među operatorima pokretnih mreža. U Španjolskoj je, primjerice, za potrebe 5G tehnologije od ukupno 26 GHz dostupno 1,5 GHz. Međutim, na temelju informacija prikupljenih u okviru javnog savjetovanja koje je dovršeno u srpnju 2019., 1,5 GHz još nije dodijeljeno operatorima jer za njime ne postoji potražnja. Novo javno savjetovanje planira se do kraja 2021. u cilju održavanja dražbe za taj frekvencijski pojas u drugom tromjesečju 2022. Osim toga, operatori pokretnih mreža u Finskoj istaknuli su da još ne postoji ni snažan interes ni poslovna isplativost za dodjelu frekvencijskog pojas od 26 GHz.

41. Pitanja prekogranične koordinacije sa zemljama izvan EU-a koje s njim dijele istočne granice (Bjelarus, Rusija i Ukrajina) također doprinose kašnjenjima u dodjeli frekvencijskog spektra 5G mreže. Na temelju postojećih međunarodnih sporazuma te zemlje izvan EU-a upotrebljavaju frekvencijski pojas od 700 MHz za televizijski prijenos i pojas od 3,6 GHz za usluge vojnih satelita. Navedeno se pitanje uglavnom odnosi na baltičke zemlje (Estonija, Latvija i Litva) i Poljsku. Komisija smatra da je ostvaren određeni napredak u slučaju Ukrajine i Bjelarusa, koji bi do kraja 2022. trebali pustiti pojas od 700 Mhz u promet. U bilateralnim pregovorima s Rusijom još nije ostvaren napredak. U tom kontekstu Estonija i Poljska zatražile su odstupanje od rokova za dodjelu pojasa 700 MHz do sredine 2022.

42. Osim toga, u Poljskoj i Španjolskoj dražbe frekvencijskog spektra 5G mreže odgođene su tijekom pandemije bolesti COVID-19 (vidjeti ***okvir 3.***).

Okvir 3.

Primjeri kašnjenja u dodjeli frekvencijskog spektra 5G mreže prouzročeni pandemijom bolesti COVID-19

- Poljska je u ožujku 2020. najavila dražbu za frekvencijski pojas od 3,6 GHz koji se trebao dodijeliti do 30. lipnja 2020. Uslijed izbijanja pandemije poljska nadležna tijela odlučila su obustaviti sve upravne postupke tijekom trajanja pandemije. U rujnu 2021. proces dražbi tog pojasa još nije bio dovršen.

- U Španjolskoj je dražba za pojas 700 MHz prvotno planirana za ožujak 2020. Međutim, španjolska tijela navode da se zbog pandemije bolesti COVID-19 kasnilo s puštanjem u promet tog pojasa koji se upotrebljava za digitalnu televiziju. Potom je dražba odgođena do svibnja 2020., a zatim do prvog tromjesečja 2021. Nakon izmjene španjolskog zakonodavstva u travnju 2021. radi usklađivanja trajanja licencija s Europskim zakonikom elektroničkih komunikacija, dražba je odgođena za ljeto 2021., a frekvencijski pojas od 700 MHz konačno je dodijeljen u srpnju 2021.

43. Još jedan razlog zbog kojeg su zabilježena kašnjenja u dodjeli pionirskih frekvencijskih pojaseva 5G mreže različiti su pristupi država članica sigurnosti 5G mreža i njihova kašnjenja u donošenju zakona o sigurnosti 5G mreža, čime se stvara poslovna neizvjesnost (vidjeti odlomke ***74***. i ***75***.):

- U Španjolskoj je u pravila o dražbama pionirskih frekvencijskih pojaseva uključena opća klauzula u kojoj se navodi da su koncesionari javnih usluga dužni postupati u

skladu sa svim obvezama u pogledu sigurnosti 5G mreža koje se u bilo kojem budućem trenutku utvrde europskim ili španjolskim propisima. Španjolski operator pokretne mreže s kojim je Sud obavio razgovor smatrao je da je na temelju te klauzule obvezan donositi odluke o strategijama i kupnji u uvjetima neizvjesnosti. Također je istaknuo da relevantna nacionalna tijela nisu bila voljna razjasniti određene ključne uvjete, kao što je mogućnost naknade ako se od njih na temelju budućeg zakonodavstva, koje se planira donijeti do kraja 2022., bude očekivalo da zamijene svoju opremu.

- U Poljskoj je jedan od iznesenih razloga za odgodu dodjele frekvencijskog spektra 5G mreže bila potreba da se pričeka donošenje zakona kojim će se pojasniti sigurnosni zahtjevi za 5G mreže.

Potrebni su dodatni napori kako bi se riješila sigurnosna pitanja u okviru uvođenja 5G mreža

44. Kad je riječ o sigurnosnim aspektima 5G mreža, Sud je ispitao sljedeće:

- je li Komisija poduzela potrebne korake za promicanje pouzdane izrade sigurnosnog okvira i pružila odgovarajuću potporu državama članicama; i

- uvode li države članice sigurne 5G mreže na usklađen način, usvajaju li mjere ublažavanja uključene u paket instrumenata EU-a za kibersigurnost 5G mreža (paket instrumenata) i ažuriraju li svoje zakonodavstvo.

Komisija je brzo reagirala kad je sigurnost 5G mreža postala veoma važno pitanje na razini EU-a

45. Akcijskim planom za 5G iz 2016. ne uzimaju se u obzir sigurnosna pitanja. Sigurnost 5G mreža i pretjerana ovisnost o dobavljačima iz trećih zemalja, a posebno iz Kine, utvrđene su u ožujku 2019. kao jedan od ključnih problema. Europski parlament u svojoj je rezoluciji od 12. ožujka 2019.[32] izrazio zabrinutost zbog dobavljača 5G opreme iz zemalja izvan EU-a s kojima bi zbog zakona svojih zemalja podrijetla mogao biti povezan sigurnosni rizik za EU. Istog je dana Komisija u svojem strateškom pregledu o odnosu EU-a i Kine istaknula da je EU-u potreban zajednički pristup sigurnosti 5G mreža kako bi se zaštitio od potencijalno ozbiljnih posljedica za sigurnost ključne

[32] Rezolucija Europskog parlamenta od 12. ožujka 2019. (2019/2575(RSP)).

digitalne infrastrukture[33]. Europsko vijeće u svojim je zaključcima od 21. i 22. ožujka 2019. zatražilo od Komisije da iznese preporuku o usklađenom pristupu sigurnosti 5G mreža[34].

46. Nekoliko dana kasnije Komisija je iznijela takvu preporuku u kojoj je sadržan niz mjera na nacionalnoj razini (na primjer procjena rizika u vezi s 5G mrežama) i razini EU-a (na primjer usklađena procjena rizika) kojima se nastoji osigurati visoka razina kibersigurnosti 5G mreža diljem EU-a[35].

47. Gotovo sve države članice dovršile su svoje nacionalne procjene rizika do roka u srpnju 2019.[36] U listopadu 2019. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava objavila je izvješće o koordiniranoj procjeni rizika kibersigurnosti 5G mreža na razini EU-a i paket instrumenata EU-a za kibersigurnost 5G mreža[37] u siječnju 2020. (vidjeti ***Prilog VII.***). Paket instrumenata ubrzo su odobrili Komisija i Europsko vijeće[38].

U paketu instrumenata EU-a za kibersigurnost 5G mreža iz 2020. prvi su put utvrđene mjere za suočavanje sa sigurnosnim prijetnjama na razini EU-a, no one nisu bile obvezujuće naravi

Pristupanjem pitanju sigurnosti 5G mreža koje je u nacionalnoj nadležnosti ograničava se područje djelovanja Komisije

48. Ugovorima EU-a[39] utvrđuje se područje primjene mjera za pružanje odgovora na izazove, kao što su izazovi koji se odnose na uvođenje sigurnih 5G mreža na razini EU-a. To je područje primjene opsežno i ostavlja prostora za tumačenje Komisiji i državama članicama (vidjeti ***okvir 4.***).

---

[33] JOIN(2019) 5 final od 12.3.2019.EU i Kina – strateški pregled.

[34] Zaključci Europskog vijeća od 21. i 22. ožujka 2019.

[35] Preporuka Komisije (EU) 2019/534 od 26. ožujka 2019. „Kibersigurnost 5G mreža”.

[36] Priopćenje za tisak od 19. srpnja 2019.

[37] Kibersigurnost 5G mreža – paket instrumenata EU-a za smanjivanje rizika. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, 01/2020.

[38] Komunikacija Europske komisije, Sigurno uvođenje 5G mreža u EU-u – Provedba paketa instrumenata EU-a, COM(2020) 50 final; i Zaključci Europskog vijeća od 1. i 2. listopada 2020. (EUCO 13/20).

[39] Ugovor o funkcioniranju Europske unije.

Okvir 4.

Nadležnosti EU-a u području 5G mreža: podijeljena nadležnost ili pitanje nacionalne sigurnosti?

U pravilu 5G mreže pripadaju području primjene nadležnosti jedinstvenog tržišta EU-a (podijeljena nadležnost) i kao usluga (koju pružaju operatori pokretnih mreža) i kao roba (sama 5G oprema koju kupuju operatori pokretnih mreža za uspostavu vlastitih 5G mreža). U okviru podijeljene nadležnosti EU (Komisija i druge institucije EU-a) može donijeti pravno obvezujuće mjere (zakonodavstvo) kako bi se zajamčila uspostava njegova jedinstvenog tržišta i promicalo njegovo pravilno funkcioniranje. Sigurnost 5G mreža mogla bi se također razmotriti u širem smislu u vezi s područjem slobode, sigurnosti i pravde EU-a. Sigurnost se u tom smislu može shvatiti kao opći pojam koji se odnosi na sprječavanje kaznenih djela i borbu protiv njih što je čini još jednim od pitanja pod podijeljenom nadležnošću u pogledu kojega EU može donositi pravno obvezujuće mjere.

Suprotno tome, uže tumačenje sigurnosti bilo bi njezino ograničavanje na prijetnje nacionalnoj sigurnosti država članica. Promatranjem sigurnosnog pitanja isključivo kroz prizmu nacionalne nadležnosti djelovanje EU-a svodi se samo na mjere kojima se državama članicama pomaže u njihovim nastojanjima da zajamče sigurnost svojih 5G mreža.

49. Pitanje sigurnosti 5G mreža proteže se kroz nacionalne nadležnosti i nadležnosti EU-a te se njime dotiče i pitanje nacionalne sigurnosti. Komisija je pitanju sigurnosti 5G mreža pristupila u smislu prijetnji nacionalnoj sigurnosti te se stoga odlučila za mjere neobvezujućeg prava. Time se podrazumijeva da EU ne može donositi pravno obvezujuće mjere kojima bi se države članice obvezalo da primjenjuju jedinstvene mjere za ublažavanje rizika ili da provode primjenjive zahtjeve. Umjesto toga Komisija može izdavati neobvezujuće preporuke i komunikacije, pomoći u dijeljenju najboljih praksi i koordinirati nacionalne mjere država članica. Ipak, moguć je drukčiji pristup. Takav je primjer Direktiva NIS[40] koja je zakon EU-a koji se bavi sigurnošću mrežnih i informacijskih sustava u Uniji. Taj je zakon predložila Komisija i on je donesen u okviru

[40] Direktiva (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije.

pravne osnove „jedinstvenog tržišta”, iako kibersigurnost u velikoj mjeri pripada području nacionalne nadležnosti[41].

Paket instrumenata EU-a za kibersigurnost 5G mreža donesen je u ranoj fazi uvođenja, ali neki operatori pokretnih mreža već su bili odabrali svoje dobavljače

50. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava donijela je 2020. paket instrumenata EU-a za kibersigurnost 5G mreža u kojemu se navodi niz strateških i tehničkih mjera te mjera potpore za suočavanje sa sigurnosnim prijetnjama 5G mrežama i utvrđuju relevantni akteri za svaku od tih mjera. Taj paket, koji su odobrili Komisija i Europsko vijeće, donesen je samo devet mjeseci nakon što su Europski parlament i Vijeće prvi put izrazili svoju zabrinutost za sigurnost 5G mreža. U novije vrijeme paket instrumenata EU-a za kibersigurnost 5G mreža spominje se u novoj europskoj strategiji za poticanje pametnih, čistih i sigurnih veza u digitalnim sustavima diljem svijeta kao alat za usmjeravanje ulaganja u digitalnu infrastrukturu[42]. Pristup neobvezujućeg prava koji je uvela Komisija doprinio je brzom pokretanju mjera za suočavanje sa sigurnosnim prijetnjama i na razini EU-a i lakšoj suradnji država članica u tom prekograničnom pitanju. Za usporedbu, od prijedloga Komisije[43] do donošenja Direktive NIS bilo je potrebno više od tri godine[44], a za Direktivu o Europskom zakoniku elektroničkih komunikacija više od dvije godine[45]. Za prenošenje direktiva u nacionalne pravne sustave država članica bilo je potrebno još više vremena (vidjeti također odlomke ***36***. i ***37***.).

51. Paket instrumenata EU-a za kibersigurnost 5G mreža donesen je četiri godine nakon što je politika o 5G mrežama predstavljena u akcijskom planu za 5G i iste godine kad su trebale biti ostvarene srednjoročne ključne etape uvođenja utvrđene u tom akcijskom planu. U tom kontekstu predstavnici ministarstava država članica, nacionalna regulatorna tijela i operatori pokretnih mreža koji su ispitani za potrebe ove revizije smatrali su da su mjere za sigurnosne aspekte 5G mreža započele prekasno.

---

[41] Pregled br. 02/2019 „Izazovi u pogledu djelotvornosti kibersigurnosne politike EU-a (informativni dokument)”, odlomak 36.

[42] Zajednička komunikacija Europskog parlamenta, Vijeća, Europskog gospodarskog i socijalnog odbora, Odbora regija i Europske investicijske banke – Global Gateway. JOIN(2021) 30 final, 1.12.2021.

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

[44] Direktiva (EU) 2016/1148.

[45] COM(2016) 0590 final/2 od 12.10.2016 i Direktiva (EU) 2018/1972 o Europskom zakoniku elektroničkih komunikacija.

52. Paket instrumenata objavljen je u razdoblju kada su uvođenje 5G mreža i planovi za njih u većini država članica još bili u ranoj fazi. Većina ugovora između dobavljača i operatera za 5G opremu sklopljena je 2020. i 2021. Međutim, prema navodima Udruženja europskih operatora telekomunikacijskih mreža (ETNO), u trenutku kada je paket instrumenata EU-a za kibersigurnost 5G mreža postao dostupan niz operatora pokretnih mreža već je bio odabrao svoje dobavljače.

Paketom instrumenata EU-a za kibersigurnost 5G mreža pružen je okvir za procjenu profila rizičnosti dobavljača, ali i dalje su prisutni nedostatci

Neke države članice i nacionalna tijela smatraju da jedan dio kriterija koji se upotrebljavaju za svrstavanje dobavljača u skupinu visokorizičnih dobavljača nije dovoljno jasan

53. Jedna od ključnih značajki paketa instrumenata EU-a za kibersigurnost 5G mreža odnosi se na to da države članice trebaju procijeniti dobavljače i da za bitnu imovinu utvrđenu kao ključnu trebaju primijeniti ograničenja na dobavljače svrstane u skupinu visokorizičnih dobavljača. Države članice trebale bi obavljati tu procjenu na temelju neiscrpnog popisa kriterija preuzetih iz koordinirane procjene rizika na razini EU-a. Takvi su kriteriji na primjer:

- vjerojatnost da na određenog dobavljača utječe pojedina zemlja izvan EU-a, na primjer postojanjem snažne poveznice između dobavljača i vlade zemlje izvan EU-a ili u vidu zakonodavstva zemlje izvan EU-a, posebno ako nije uspostavljen zakonodavni ili demokratski sustav provjere i ravnoteže ili ne postoje sporazumi o sigurnosti ili zaštiti podataka između EU-a i predmetne zemlje izvan EU-a;
- sposobnost dobavljača da osigura opskrbu; i
- ukupna kvaliteta proizvoda dobavljača i kibersigurnosnih praksi.

54. Paket instrumenata izrađen je kako bi se izbjegla rascjepkanost i promicala usklađenost na unutarnjem tržištu. Kriterijima u paketu nudi se operativni okvir koristan za obavljanje procjene profila rizičnosti dobavljača na usklađen način u svim državama članicama. Tim se okvirom Komisiji ujedno omogućilo da zajedno s državama članicama brzo odgovara na nova sigurnosna pitanja u vezi s 5G mrežama. Istodobno, nacionalna tijela i dalje su odgovorna za primjenu tih kriterija pri procjeni rizika povezanih s konkretnim dobavljačima. Do listopada 2021., uzimajući u obzir taj okvir, 13 država članica donijelo je ili izmijenilo zakonodavstvo o sigurnosti 5G mreža (vidjeti odlomak ***75***. i ***sliku 6.***).

55. Međutim, predstavnici ministarstava dvije od četiri države članice s kojima je Sud za potrebe ove revizije obavio razgovor smatrali su da su se neki od tih kriterija za razvrstavanje dobavljača 5G opreme mogli tumačiti na različite načine i da bi ih bilo potrebno dodatno pojasniti. Ujedno su pozvali Komisiju da pruži dodatnu potporu i smjernice u vezi s razvrstavanjem visokorizičnih dobavljača. Predstavnici država članica s kojima je obavljen razgovor također su istaknuli da je ta situacija stvorila opasnost da države članice primijene različite pristupe prema visokorizičnim dobavljačima (vidjeti također odlomke ***74***. i ***75***. te ***okvir 5.***). Jedanaest nacionalnih regulatornih tijela koja su sudjelovala u anketi koju je proveo Sud, koja su u različitoj mjeri uključena u pitanje sigurnosti 5G mreža, izrazila su sličnu zabrinutost.

Zemlja podrijetla dobavljača 5G opreme utječe na procjenu sigurnosnih rizika

56. Dobavljači 5G opreme razlikuju se u pogledu svojih korporativnih značajki i dolaze iz zemalja koje imaju različite veze s EU-om. Na ***slici 5.*** predstavljene su određene zajedničke značajke i razlike među glavnim dobavljačima 5G opreme i njihovim zemljama podrijetla, posebno u područjima na koja se u paketu instrumenata upućuje kao na područja za koja je izgledno da će utjecati na procjenu profila rizičnosti dobavljača (vidjeti odlomak ***53***.).

Slika 5. – Zajedničke značajke i razlike među dobavljačima 5G opreme i njihovim zemljama podrijetla

Izvor: Sud, na temelju zemalja članica WTO-a; zemalja članica OECD-a; OECD-ova indeksa regulatorne restriktivnosti za izravna strana ulaganja; , skupa podataka Svjetske banke o pokazateljima kvalitete upravljanja u svijetu, 2019.; skupa podataka Svjetskog gospodarskog foruma o globalnoj konkurentnosti, rang-lista 2018.; odluka o primjerenosti; publikacije portala Statista „Who is leading the 5G patent race?”; podataka društva Ericsson; podataka društva Nokia; podataka društva Qualcomm; podataka društva Sharp; podataka društva LG; podataka društva Samsung; podataka društva Huawei i podataka društva ZTE. Tečajna lista na datum 31.12.2020.

57 Jedan čimbenik rizika mjera je u kojoj zemlja podrijetla dobavljača postupa u skladu s temeljnim političkim i gospodarskim vrijednostima EU-a. Povezani čimbenici svojstveni za svaku zemlju kao što su vladavina prava, neovisnost pravosuđa, otvorenost prema stranim ulaganjima i postojanje sporazuma o zaštiti podataka mogu se primijeniti kao mjera pravne zaštite određenog poduzeća od vladinog utjecaja kao i zaštita koju to poduzeće može prenijeti na svoje klijente.

58 Iako su dobavljači sa sjedištem u državama članicama EU-a obvezni pridržavati se standarda i pravnih zahtjeva EU-a, to nije primjenjivo na šest glavnih dobavljača sa sjedištem u zemljama izvan EU-a koji posluju u skladu s okvirom zakonodavstava trećih zemalja (vidjeti ***sliku 5.***). Takva se zakonodavstva mogu znatno razlikovati od standarda na razini EU-a, na primjer u pogledu zaštite podataka za građane, djelotvornosti takve zaštite ili općenito načina jamčenja neovisnosti pravosuđa s pomoću zakonodavnih i/ili demokratskih provjera i ravnoteže. Kad je riječ o neovisnosti pravosuđa, SAD i Japan imaju bolje rezultate od ostalih zemalja podrijetla dobavljača 5G opreme koje su izvan EU-a, dok u pogledu ocjene vladavine prava Južna Koreja ima najbolje rezultate među zemljama izvan EU-a.

59 5G mreže pretežito pokreće softver. Činjenica da neki dobavljači posluju u skladu s okvirom zakonodavstva izvan EU-a mogla bi biti posebno zabrinjavajuća u slučajevima u kojima su kontrolni centri softvera također izvan EU-a, zbog čega bi korisnici unutar EU-a potencijalno bili obvezni poštovati zakonodavstvo doneseno izvan EU-a.

60 Komisija se počela baviti tim pitanjima uzimajući u obzir da bi svako poduzeće koje pruža usluge građanima EU-a trebalo poštovati pravila i vrijednosti EU-a[46]. Komisija je započela dijaloge s nekoliko zemalja kako bi zajamčila snažnu zaštitu privatnosti osobnih podataka[47]. Na ***slici 5.*** vidljivo je i to da je Komisija već priznala primjerenost sustava zaštite podataka u Japanu (i, prethodno, sustava zaštite podataka u SAD-u). Međutim, valja napomenuti da odluke o primjerenosti mogu biti osporene i da se na njih primjenjuje strogi sudski nadzor. Na primjer, Sud Europske unije ukinuo je 2015. dotad mjerodavni pravni instrument za razmjenu podataka sa SAD-om, tj. sustav „sigurne luke”[48], a kasnije tijekom 2020. presudio je da se sustavom zaštite privatnosti,

---

[46] Komunikacija Europske komisije, Izgradnja digitalne budućnosti Europe, COM(2020) 67 final.

[47] EU i Kina – strateški pregled.

[48] Presuda u predmetu C-362/14 i https://curia.europa.eu/jcms/upload/docs/application/pdf/2015. – 10./cp150 117hr.pdf

kojim je zamijenjen sustav „sigurne luke”, ne pruža primjerena zaštita građanima EU-a[49]. Stoga trenutačno ne postoji odluka o primjerenosti za SAD. Općenitije govoreći, i ne gledajući samo na postojanje sustava zaštite podataka, važno je uzeti u obzir širi pravni i institucionalni okvir, uključujući, primjerice, poštovanje vladavine prava i način na koji je zajamčena neovisnost pravosuđa.

61 Na ***slici 5.*** prikazano je i da među dobavljačima 5G opreme postoje znatne razlike u pogledu njihovih udjela u patentima 5G tehnologije, prihodima i broju zaposlenih. To utječe na resurse koji su im na raspolaganju, što pak može utjecati na njihovu otpornost i sposobnost da zajamče neprekidnu opskrbu. Na primjer, Samsung i Huawei dobavljači su s najvećim udjelom patenata 5G tehnologije i ostvaruju najveće prihode kao korporacije te imaju ukupno najveći broj zaposlenih.

62 Vjerojatnost da na određenog dobavljača utječe vlada pojedine zemlje izvan EU-a još je jedan važan čimbenik definiran u paketu instrumenata kao čimbenik na temelju kojega se utvrđuje profil rizičnosti pojedinog dobavljača. U tom kontekstu vlasništvo ima važnu ulogu jer vlasnici s velikim brojem udjela imaju mogućnost izvršavati pritisak ili utjecati na upravljačke odluke. Osim toga, poduzeća u privatnom ili državnom vlasništvu smatraju se manje otvorenima za javni nadzor u pogledu revizija i odgovornosti u usporedbi s javnim poduzećima koja podliježu strogim zahtjevima za objavljivanje informacija tijekom godine u korist ulagačima i regulatornim tijelima. Većina dobavljača 5G opreme javno je uvrštena na burzu u svojoj zemlji podrijetla ili u inozemstvu, dok je kineske dobavljače teže razvrstati i općenito se smatraju blisko povezanima s kineskom vladom[50].

Države članice ocijenile su potporu Komisije i agencije ENISA u provedbi paketa instrumenata EU-a za kibersigurnost 5G mreža korisnom

63. Komisija je pružila potporu državama članicama razmjenom primjera najboljih praksi u pogledu određenih ključnih mjera paketa instrumenata EU-a za kibersigurnost 5G mreža, uključujući u pogledu visokorizičnih dobavljača. Tu potporu, koja se često pružala u kontekstu Skupine za suradnju u području sigurnosti mrežnih i informacijskih

[49] Presuda u predmetu C-311/18 i https://curia.europa.eu/jcms/upload/docs/application/pdf/2020. – 07./cp200 091hr.pdf

[50] https://www.europarl.europa.eu/doceo/document/E-9. – 202.0. – 004. 305_EN.html i https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637 912/EPRS_ATA(2019)63 7 912_EN.pdf

sustava, dopunjavale su konkretne aktivnosti Agencije Europske unije za kibersigurnost (ENISA), kao što su organiziranje internetskih seminara ili izdavanje smjernica o:

- provedbi paketa instrumenata s naglaskom na tehničkim mjerama; i
- najboljim praksama u pogledu mrežne sigurnosti, posebno o:
  - 5G prijetnjama[51];
  - pripremi nacionalnih procjena rizika za 5G mreže; i
  - sigurnosnim mjerama u skladu s Europskim zakonikom elektroničkih komunikacija[52], uključujući posebne smjernice o sigurnosti 5G mreža[53].

64. Komisija je zadužila ENISA-u i za izradu programa kibersigurnosne certifikacije za 5G mreže na razini EU-a koji bi trebao pomoći u prevladavanju rizika povezanih s tehničkim slabostima mreža i dodatno unaprijediti kibersigurnost[54]. Iako bi se tom certifikacijom mogla poboljšati sigurnost, njome se ipak ne može spriječiti unos prijetnji u sustave koje mogu izazvati ažuriranja softvera.

65. Svi predstavnici tijela država članica koje je Sud ispitao za potrebe ove revizije naglasili su korisnost potpore Komisije i ENISA-e u provedbi paketa instrumenata EU-a za kibersigurnost 5G mreža. Osim toga, većina nacionalnih regulatornih tijela za telekomunikacije (15 od 21) navela je da Komisija i/ili ENISA podržavaju nacionalna tijela u razmjeni najboljih praksi u pogledu provedbe ključnih strateških mjera.

Paket instrumenata EU-a za kibersigurnost 5G mreža donesen je prekasno da bi se uzeo u obzir u projektima koji su se sufinancirali sredstvima EU-a tijekom razdoblja 2014. – 2020.

66. Jedan je od ciljeva paketa instrumenata EU-a za kibersigurnost 5G mreža zajamčiti da se u projektima 5G mreža sufinanciranima sredstvima EU-a uzmu u obzir kibersigurnosni rizici. Međutim, paket instrumenata usvojen je tek u siječnju 2020. Svi projekti koje je Sud pregledao za potrebe ove revizije odabrani su prije donošenja paketa instrumenata EU-a za kibersigurnost 5G mreža i stoga se ne može očekivati da se u njima slijedio preporučeni pristup kibersigurnosti, uključujući prema

---

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

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

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

[54] Priopćenje za tisak od 3. veljače 2021.

visokorizičnim dobavljačima. Na primjer, Sud je u svojem uzorku utvrdio jedan projekt programa Obzor 2020. i dva projekta EFRR-a u Španjolskoj u kojima se upotrebljava kineska 5G oprema koja je kasnije zabranjena u Švedskoj (vidjeti odlomak ***15***.).

67. Tijekom razdoblja 2021. – 2027. Komisija namjerava promicati usklađen pristup sigurnosti 5G mreža za projekte koji se sufinanciraju sredstvima EU-a na način da zajamči da je usklađenost s paketom instrumenata uvjet za financiranje sredstvima EU-a. Međutim, to će se razlikovati ovisno o načinu provedbe:

- u programima kojima izravno upravlja Komisija (na primjer programu Obzor Europa za razdoblje 2021. – 2027.) omogućit će se isključivanje dobavljača koji podliježu utjecaju vlade pojedine zemlje izvan EU-a. Time će se vjerojatno zajamčiti da se u projektima koji se financiraju sredstvima EU-a uzmu u obzir kibersigurnosni rizici i da se spriječe situacije u kojima se pojedini dobavljač u jednoj državi članici sufinancira sredstvima EU-a, dok je u drugoj državi članici zbog procjene da je visokorizičan iz takvog sufinanciranja isključen;

- za programe koji se provode pod podijeljenim upravljanjem u zakonodavstvu nema zahtjeva o kibersigurnosnim rizicima. Komisija stoga planira promicati da se u sporazume država članica o partnerstvu uključuje upućivanje na paket instrumenata kao način na koji bi se omogućilo da se pri financiranju projekata povezanih s 5 G mrežama sredstvima iz EFRR-a uzmu u obzir kibersigurnosni rizici; i

- za InvestEU (program koji zamjenjuje EFSU)[55] i Mehanizam za oporavak i otpornost Komisija planira poticati odgovorna tijela da u sporazumima o financiranju upućuju na paket instrumenata EU-a.

Države članice još nemaju usklađen pristup rješavanju pitanja sigurnosnih aspekata pri uvođenju 5G mreža

Informacije o tome kako države članice pristupaju rješavanju sigurnosnih pitanja nisu dovoljne

68. Komisija prati napredak provedbe paketa instrumenata EU-a za kibersigurnost 5G mreža i izvješćuje o njemu na temelju Skupine za suradnju u području sigurnosti mrežnih i informacijskih sustava, kao i na temelju bilateralnih razgovora s državama članicama i neizravno preko medija. Prvi rezultati tog praćenja objavljeni su u

[55] Uredba (EU) 2021/523 o uspostavi programa InvestEU.

srpnju 2020.[56] U prosincu 2020. Komisija je također objavila izvješće o učinku svoje Preporuke o kibersigurnosti 5G mreža[57]. Prema stanju u rujnu 2021. ne planira se daljnje izvješćivanje.

69. Međutim, prethodno navedena izvješća nemaju zajednički skup ključnih pokazatelja uspješnosti i ne čine usporediv skup detaljnih informacija o načinu na koji države članice pristupaju sigurnosnim pitanjima u vezi s 5G mrežama.

70. Osim toga, malo je javno dostupnih informacija o načinu na koji države članice pristupaju visokorizičnim dobavljačima, tj. njihovom utvrđivanju i činjenici isključuje li ih se iz pružanja 5G opreme, a čak su i te informacije proturječne i nepotpune. Na primjer:

- U svojem izvješću iz srpnja 2020. o napretku država članica u provedbi paketa instrumenata (vidjeti odlomak ***68***.) Komisija ističe da je otprilike polovica država članica (14 od 27) procijenila profil rizičnosti dobavljača i primijenila ograničenja na dobavljače koje smatra visokorizičnima.

- U izvješću iz prosinca 2020.[58] BEREC je naveo da je takva ograničenja uvelo samo devet država članica i da ih sedam od preostalih 18 država članica nema namjeru uvesti.

71. Čak i nakon što su države članice donijele zakonodavstva usmjerena na sigurnost 5G mreža (vidjeti i odlomak ***75***.), u njima se ne pojašnjava pristup država članica prema visokorizičnim dobavljačima. Bilo kakve konkretne odluke vjerojatno će se donijeti isključivo provedbenim aktima ili upravnim ili trgovačkim odlukama koje nisu javne.

72 Prema navodima dionika i donositelja odluka s kojima je Sud obavio razgovor (na primjer Europski parlament), informacije koje nisu javne (na primjer koje su iznesene u izvješćima Komisije ili Skupine za suradnju u području sigurnosti mrežnih i informacijskih sustava) i koje se odnose na pristup država članica prema visokorizičnim

---

[56] „Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity", srpanj 2020.

[57] „Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks", SWD(2020) 357 final od 16.12.2020.

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

dobavljačima također su oskudne te se ti subjekti moraju oslanjati na medijske i neslužbene izvore.

73 Unatoč prekograničnoj naravi sigurnosnih pitanja u vezi s 5G mrežama, sveukupno je malo dostupnih javnih informacija o načinu na koji države članice pristupaju sigurnosnim pitanjima, a posebno pitanju visokorizičnih dobavljača. Time se otežava razmjena saznanja među državama članicama i mogućnost primjene usklađenih mjera. Ujedno se ograničava i mogućnost Komisije da predlaže poboljšanja sigurnosti 5G mreža.

Postoje naznake da neke države članice primjenjuju različite pristupe prema dobavljačima 5G opreme

74. Nacionalna tijela imaju velike diskrecijske ovlasti u provedbi ključnih mjera u području sigurnosti 5G mreža (vidjeti odlomke ***48***. i ***49***.). U paketu instrumenata uzimaju se u obzir nacionalne ovlasti i relevantni čimbenici svojstveni za svaku zemlju (procjena prijetnji koju obavljaju nacionalne sigurnosne službe, vremenski okvir za uvođenje 5G mreža, prisutnost dobavljača, kibersigurnosne sposobnosti). Države članice dosad su primjenjivale različite pristupe u pogledu upotrebe opreme određenih dobavljača ili u pogledu opsega ograničenja koja primjenjuju na visokorizične dobavljače (vidjeti primjere četiriju država članica u ***okviru 5.***).

Okvir 5.

Primjeri različitih pristupa država članica prema kineskim dobavljačima 5G opreme

Okvir je uveden i ograničenja se primjenjuju[(1)]

U listopadu 2020. švedsko nacionalno regulatorno tijelo za telekomunikacije (PTS) uvelo je sljedeće uvjete za sudjelovanje na dražbi frekvencijskog spektra 5G mreže:

— postavljanje nove opreme i obavljanje središnjih funkcija za radijsku upotrebu u frekvencijskim pojasevima nisu dopuštene ako se temelje na upotrebi proizvoda kineskih dobavljača; i

— svaka postojeća infrastruktura takvog dobavljača mora se postupno ukinuti najkasnije do 1. siječnja 2025.

Okvir je uveden, ali se još ne primjenjuje[2], [3], [4]

U Njemačkoj se drugom inačicom zakona o sigurnosti IT-ja iz svibnja 2021. predviđa obvezna certifikacija ključnih sastavnica prije odobrenja njihove upotrebe. Njemački operatori pokretnih mreža s kojima je Sud obavio razgovor radije se zalažu za jedinstven europski postupak certifikacije pod pokroviteljstvom agencije ENISA, koji će služiti kao jedinstvena europska kontaktna točka, nego za potencijalno mnoštvo nacionalnih certifikacija. Tim se zakonom Saveznom ministarstvu unutarnjih poslova također omogućuje da zabrani upotrebu ključnih sastavnica ako bi one sa sobom mogle donositi prijetnju nacionalnoj sigurnosti.

U Austriji se ažuriranim zakonom o telekomunikacijama donesenim krajem listopada 2021. nadležnom ministru omogućuje da dobavljače svrsta u skupinu visokorizičnih dobavljača i da na njih primijeni ograničenja ili da ih isključi iz tržišta. Javno dostupne informacije iz listopada 2021. upućuju na to da je u toj zemlji u tijeku proširenje 5G mreže za koje se upotrebljava oprema kineskog dobavljača Huwei.

Okvir još nije uveden[5], [6]

Prema stanju u rujnu 2021. Mađarska nije uvela ograničenja ni za jednog dobavljača 5G opreme i vjerojatno ni neće u bliskoj budućnosti. Mađarska je također službeno odbila pridružiti se međunarodnom Programu za čistu 5G mrežu (engl. *5G Clean Network Program*) koji promiče SAD i čiji je cilj uvođenje ograničenja prisutnosti za kineske dobavljače u osnovnim 5G mrežama.

(1) Odluka 18. – 849.6 od 20.10.2020. o uvjetima dražbe frekvencijskih pojaseva 3,5 GHz i 2,3 GHz.

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

(3) Austrijski zakon o telekomunikacijama.

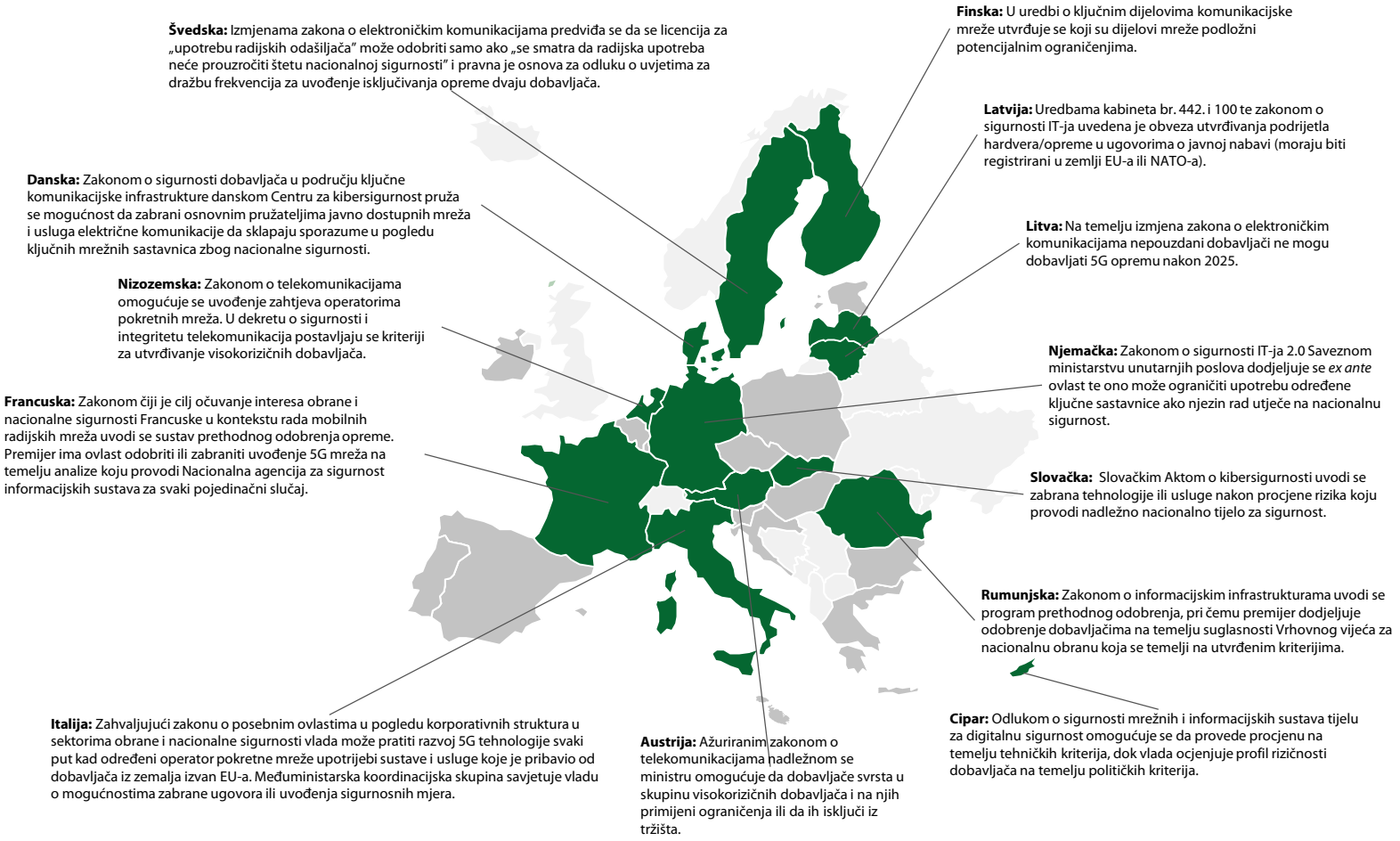
(4) https://www.euractiv.com/section/5g/news/austria-to-also-rely-on-huawei-in-5g-rollout/

(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. Otkako je paket instrumenata donesen, ostvaren je napredak u jačanju sigurnosti 5G mreža i u većini država članica primjenjuju se ograničenja na visokorizične dobavljače ili je u tijeku proces primjene takvih ograničenja. Do kraja 2021. 13 država članica donijelo je ili izmijenilo nacionalne zakone o sigurnosti 5G mreža. Tim regulatornim mjerama uzimaju se u obzir kriteriji utvrđeni u paketu instrumenata, ali se primjenjuju različiti pristupi (vidjeti ***sliku 6.***). Ostale države članice u procesu su predlaganja takvog zakonodavstva. U narednim godinama time bi se mogao postići usklađeniji pristup prema visokorizičnim dobavljačima 5G opreme, barem među onim državama članicama koje takvo zakonodavstvo provode.

Slika 6. – Države članice koje su donijele zakone kojima se omogućuje isključivanje opreme visokorizičnih dobavljača iz njihovih mreža, listopad 2021.

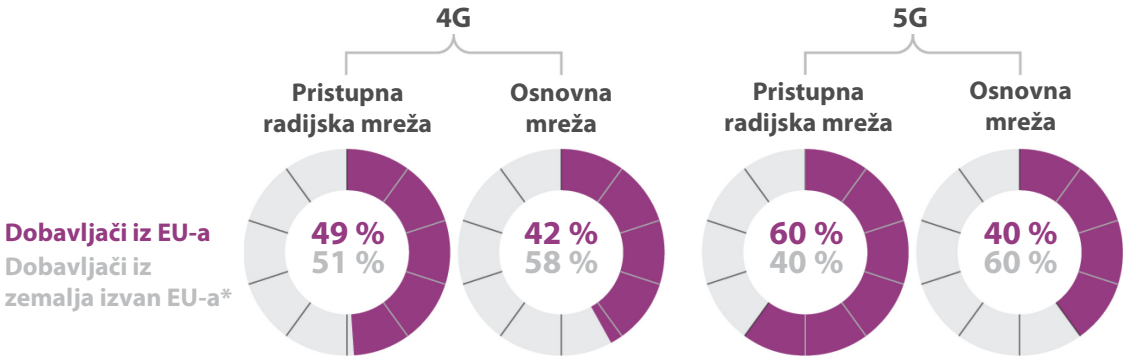


76. Komisija dosad nije procijenila kakav bi bio učinak takvih različitih pristupa u slučajevima u kojima jedna država članica uspostavi svoje 5G mreže koristeći se opremom dobavljača koji se u drugoj državi članici smatra visokorizičnim. To bi moglo utjecati na prekograničnu sigurnost ili natjecanje među operatorima pokretnih mreža koji posluju na jedinstvenom tržištu EU-a.

Komisija je nedavno počela rješavati pitanje stranih subvencija koje narušavaju unutarnje tržište

77. Prema stanju zabilježenom u prosincu 2020. više od polovice 4G i 5G opreme u EU-u potjecalo je od dobavljača iz zemalja izvan EU-a (vidjeti ***sliku 7.***).

Slika 7. – Udio operatora pokretnih mreža koji upotrebljavaju opremu dobavljača iz EU-a / zemalja izvan EU-a*



Izvor: Sud, na temelju podataka tijela BEREC. „Internal Report concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience)". BoR (20) 227.

78. Konkretno, prema stanju zabilježenom krana kraju 2019., 286 milijuna potrošača iz skupine EU-27 (64 % ukupnog broja stanovnika) koristilo se telekomunikacijskim mrežama s pomoću 4G opreme kineskih dobavljača[59]. U listopadu 2020. skupina zastupnika u Europskom parlamentu izrazila je zabrinutost pred ministrima telekomunikacija i trgovine država članica te Komisijom da je jedan od razloga za tako velik tržišni udio kineskih dobavljača taj što iskorištavaju nepravednu gospodarsku prednost, tj. primaju javne subvencije koje u skladu s pravilima o državnim potporama

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

EU-a nisu dostupne dobavljačima sa sjedištem u EU-u[60]. Sud je u jednom nedavnom pregledu istaknuo slične rizike u tom pogledu[61]. Takve subvencije mogu narušiti unutarnje tržište i na taj način stvoriti neravnopravne uvjete među dobavljačima 5G opreme s mogućim posljedicama za sigurnost. Kako bi se uhvatila u koštac s tim problemom, Komisija je u svibnju 2021. iznijela Prijedlog nove uredbe[62] kojim se utvrđuju postupci za istragu takvih subvencija i rješavanje pitanja povezanih poremećaja na tržištima.

Komisija ne raspolaže dovoljnim informacijama u pogledu mogućih troškova zamjene opreme kineskih dobavljača

79. Prema jednom izvješću iz lipnja 2020.[63] nametanje ograničenja za pojedinog ključnog dobavljača infrastrukture za 5G tehnologiju u EU-u povećalo bi ukupne troškove ulaganja za gotovo 2,4 milijarde eura godišnje tijekom sljedećeg desetljeća (tj. na 24 milijarde eura). Prema jednoj drugoj studiji[64] europski su operatori već suočeni s ažuriranjem 4G mreža koje su postavljene u razdoblju 2012. – 2016. jer je uobičajena poslovna praksa obnavljanje i modernizacija mrežne opreme čija starost premašuje tri do četiri godine. U toj se studiji procjenjuje da će ukupni trošak uklanjanja i zamjene nadogradive opreme kupljene od kineskih dobavljača u razdoblju od 2016. iznositi oko 3 milijarde eura.

80. Visok udio opreme kineskih dobavljača, u kombinaciji s njihovim mogućim svrstavanjem u skupinu visokorizičnih dobavljača u određenim državama članicama, mogao bi uzrokovati troškove zamjene u milijardama eura u slučaju da operatori pokretnih mreža trebaju ukloniti i zamijeniti opremu kineskih dobavljača u europskim mrežama bez prijelaznog razdoblja (vidjeti odlomke ***77***. – ***79***.). U načelu se državna potpora ne može odobriti za naknadu troškova operatorima za ispunjavanje pravnih

---

[60] Pismo zastupnika u Parlamentu upućeno europskim ministrima telekomunikacija i trgovine i europskim povjerenicima Thierryju Bretonu, Margrethe Vestager i Valdisu Dombrovskisu, 14.10.2020.

[61] Pregled Suda br. 03/2020: Odgovor EU-a na kinesku strategiju ulaganja pod državnom kontrolom.

[62] Prijedlog uredbe o stranim subvencijama kojima se narušava unutarnje tržište, COM(2021) 223 final od 5.5.2021.

[63] Oxford Economics, „Restricting competition in 5G network equipment throughout Europe”, lipanj 2020. (pod pokroviteljstvom društva Huawei).

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

obveza osim ako države članice mogu dokazati Komisiji da su potrebni zahtjevi ispunjeni (kao što je poticajni učinak). Sud je na temelju provedene analize utvrdio jedan slučaj u kojem bi se na temelju nacionalnih zakona mogla odobriti upotreba nacionalnih javnih financijskih sredstava kao potpora za namirenje troškova zamjene (vidjeti finski Zakon o elektroničkim komunikacijskim uslugama[65]). Države članice dužne su obavijestiti Komisiju o svim slučajevima pružanja državne potpore za naknadu takvih troškova operatorima pokretnih mreža. Prema navodima Komisije dosad nijedna država članica ni dionik nisu stupili s njom u kontakt u svrhu rasprave o mogućnosti upotrebe državne potpore. Prema navodima dionika u predmetnom sektoru s kojima je Sud obavio razgovor tijekom revizije, neizvjesnost državama članica u pogledu postupanja s takvim troškovima i moguće razlike među državama članicama narušavaju sigurnost poslovanja i ugrožavaju pravodobno uvođenje 5G mreža.

[65] Zakon o elektroničkim komunikacijskim uslugama 1207/2020 od 30.12.2020., članak 301.

Zaključci i preporuke

81. Revizijom koju je obavio Sud je općenito utvrdio da, unatoč potpori Komisije, države članice znatno kasne s uvođenjem 5G mreža i da je potrebno uložiti dodatne napore za rješavanje sigurnosnih pitanja u okviru uvođenja 5G mreža.

82. U svojem akcijskom planu za 5G iz 2016. Komisija je pozvala na pokrivenost 5G mrežama u svim gradskim područjima i duž glavnih prometnih pravaca do 2025. te, u ožujku 2021., na potpunu pokrivenost do 2030. Prema stanju na kraju 2020. 23 države članice pokrenule su komercijalne 5G usluge i ostvarile srednjoročni cilj prema kojemu najmanje jedan veliki grad ima pristup takvim uslugama. Međutim, Sud je revizijom utvrdio da pojedine države članice u svojim nacionalnim strategijama za 5G mreže ili planovima za razvoj širokopojasnog pristupa internetu ne upućuju na ciljeve Komisije. Osim toga, u nekoliko zemalja Europski zakonik elektroničkih komunikacija još nije prenesen u nacionalno pravo i kasni se s dodjelom frekvencijskog spektra 5G mreže. Ta kašnjenja u dodjeli odgovarajućeg spektra mogu se pripisati raznim razlozima: slaboj potražnji među operatorima pokretnih mreža, poteškoćama u prekograničnoj koordinaciji sa zemljama izvan EU-a koje s njim dijele istočne granice, učinku pandemije bolesti COVID-19 na raspored dražbi i neizvjesnostima u pogledu načina rješavanja sigurnosnih pitanja. Komisija smatra da će vjerojatno samo 11 država članica ostvariti cilj utvrđen za 2025. (vidjeti odlomke ***22***. – ***43***.).

83. Komisija inicijativama, smjernicama i financiranjem istraživanja povezanog s 5G mrežama podupire države članice u njihovoj provedbi akcijskog plana za 5G iz 2016. Međutim, Komisija nije utvrdila očekivanu razinu kvalitete usluge 5G mreža, kao što je stupanj funkcionalnosti koji bi ona trebala dosegnuti u pogledu najmanje brzine i najveće latencije. To je dovelo do različitog shvaćanja pojma „kvalitete 5G mreže” među državama članicama. Sud je primijetio različite pristupe država članica u uvođenju 5G usluga, kao što je činjenica da su samo dvije države članice definirale najmanju brzinu i najveću latenciju. U konačnici se tim različitim pristupima stvara rizik od nejednakosti u pristupu 5G uslugama u EU-u i njihovoj kvaliteti, čime se „digitalni jaz” među državama članicama i regijama povećava umjesto da se smanjuje (vidjeti odlomke ***22***. – ***31***.).

1. preporuka – Potrebno je promicati ujednačeno i pravodobno uvođenje 5G mreža u EU-u

Komisija bi trebala:

(a) zajedno s državama članicama utvrditi zajedničku definiciju očekivane kvalitete usluge 5G mreža, kao što su zahtjevi u vezi s funkcionalnošću u pogledu najmanje brzine i najveće latencije koje bi trebala ispunjavati;

(b) potaknuti države članice da u sljedeća ažuriranja svojih strategija za 5G mrežu / digitalnih strategija ili planova za razvoj širokopojasnog pristupa internetu uključe ciljeve uvođenja 5G mreža do 2025. i 2030., kao i mjere koje će biti potrebne za njihovo ostvarenje; i

(c) poduprijeti države članice u rješavanju pitanja koordiniranja spektra sa susjednim zemljama izvan EU-a, na primjer zalaganjem za to da je ta tema na dnevnom redu svakog relevantnog sastanka.

Rok provedbe: prosinac 2022.

84. Sigurnosni aspekti 5G mreža tek su nedavno postali jedan od glavnih problema na razini EU-a. Europsko vijeće istaknulo je 2019. povezanu potrebu za djelovanjem na razini EU-a pozivajući na usklađen pristup i suradnju među državama članicama na tom prekograničnom pitanju. Komisija je u suradnji s državama članicama brzo reagirala na nova sigurnosna pitanja u vezi s 5G mrežama. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava donijela je 2020. paket instrumenata EU-a za kibersigurnost 5G mreža u kojemu se navodi niz strateških i tehničkih mjera te mjera potpore za suočavanje sa sigurnosnim prijetnjama 5G mrežama i utvrđuju akteri odgovorni za svaku od tih mjera. Nekoliko od tih mjera odnosi se na pitanje visokorizičnih dobavljača 5G opreme. Paket instrumenata potom su odobrili Komisija i Europsko vijeće (vidjeti odlomke ***45***. – ***47***.). Budući da je paket instrumenata dio neobvezujućeg prava, predmetne mjere nemaju obvezujući učinak na države članice. Paket instrumenata EU-a za kibersigurnost 5G mreža u novije se vrijeme spominje u novoj europskoj strategiji za poticanje pametnih, čistih i sigurnih veza u digitalnim sustavima diljem svijeta kao alat za usmjeravanje ulaganja u digitalnu infrastrukturu (vidjeti odlomak ***50***.).

85 Kriterijima u paketu nudi se operativni okvir koristan za obavljanje procjene profila rizičnosti dobavljača na usklađen način u svim državama članicama. No obavljanje te procjene istodobno je i dalje u nadležnosti država članica (vidjeti odlomak ***54***.).

86 Otkako je paket donesen, ostvaren je napredak u jačanju sigurnosti 5G mreža i u većini država članica primjenjuju se ograničenja na visokorizične dobavljače ili je u tijeku proces primjene takvih ograničenja. Do listopada 2021., uzimajući u obzir taj okvir, 13 država članica donijelo je ili izmijenilo zakonodavstvo o sigurnosti 5G mreža. Ostale države članice u procesu su predlaganja zakonodavstva kojim se u obzir uzimaju kriteriji iz paketa instrumenata (vidjeti odlomke ***54***. i ***75***.).

87 Paket instrumenata donesen je u ranoj fazi uvođenja 5G mreža, no niz operatora pokretnih mreža u tom je trenutku već bio odabrao svoje dobavljače 5G opreme (vidjeti odlomak ***52***.). Nevođenje računa o sigurnosnim pitanjima pri osmišljavanju politike donosi opasnost od negativnog učinka na njezinu provedbu, kao što je taj da bi se troškom otklanjanja prijetnji (primjerice troškom borbe protiv kiberkriminala) mogle narušiti očekivane koristi (primjerice rast BDP-a) (vidjeti odlomke ***02***. i ***04***.).

88 Paketom instrumenata uzimaju se u obzir nacionalne ovlasti i relevantni čimbenici svojstveni za svaku zemlju. Revizijom koju je obavio Sud utvrđeno je da su države članice dosad primjenjivale različite pristupe u pogledu upotrebe opreme visokorizičnih dobavljača ili opsega ograničenja (na primjer, samo osnovna 5G mreža ili njezini ključni dijelovi ili pristupna radijska mreža ili jedan njezini dio) (vidjeti odlomke ***74***. i ***75***.).

89 U narednim godinama zakonodavstvom o sigurnosti 5G mreža koje države članice donesu na temelju paketa instrumenata mogao bi se postići usklađeniji pristup prema visokorizičnim dobavljačima 5G opreme. Međutim, budući da nijedna od mjera utvrđenih u tom paketu instrumenata nije pravno obvezujuća, Komisija nema ovlasti za jamčenje njihova provođenja. Stoga i dalje postoji rizik da se samim paketom instrumenata neće moći zajamčiti usklađen pristup država članica u rješavanju pitanja sigurnosnih aspekata (vidjeti odlomke ***49***. – ***.75***).

90. Brojni dobavljači 5G opreme nalaze se izvan EU-a te stoga posluju u skladu s okvirom zakonodavstava trećih zemalja koja se mogu znatno razlikovati od standarda na razini EU-a, na primjer u pogledu djelotvorne zaštite podataka za građane i općenito načina na koji se zakonodavnim ili demokratskim sustavom provjere i ravnoteže jamči neovisnost pravosuđa. Činjenica da 5G mreže pretežito pokreće softver može također biti poseban razlog za zabrinutost ako su kontrolni centri takvog softvera smješteni u zemljama izvan EU-a, zbog čega se na građane EU-a potencijalno može primjenjivati zakonodavstvo trećih zemalja. Komisija se počela baviti tim pitanjima uzimajući u obzir da bi svako poduzeće koje pruža usluge građanima EU-a trebalo poštovati pravila i

vrijednosti EU-a. Komisija je započela dijaloge s nekoliko zemalja kako bi zajamčila snažnu zaštitu privatnosti osobnih podataka (vidjeti odlomke ***56***. – ***62***.).

91. Unatoč prekograničnoj naravi sigurnosnih pitanja u vezi s 5G mrežama, nedovoljno je dostupnih javnih informacija o načinu na koji države članice pristupaju sigurnosnim pitanjima i svojoj ovisnosti o visokorizičnim dobavljačima. Komisija prati provedbu paketa instrumenata i o njoj izvješćuje. Međutim, u izvješćima se ne predstavljaju detaljne i usporedive informacije o tome kako države članice pristupaju sigurnosnim pitanjima u vezi s 5G mrežama. Osim toga, prema stanje u rujnu 2021. ne planira se buduće izvješćivanje. Taj nedostatak informacija otežava razmjenu saznanja među državama članicama i mogućnost primjene usklađenih mjera. On ujedno ograničava mogućnost Komisije da predlaže poboljšanja u pogledu sigurnosti 5G mreža (vidjeti odlomke ***68***. – ***73***.).

2. preporuka – Potrebno je poticati primjenu usklađenog pristupa država članica sigurnosti 5G mreža

Komisija bi trebala:

(a) pružiti dodatne smjernice ili mjere potpore za ključne elemente paketa instrumenata EU-a za kibersigurnost 5G mreža, npr. za kriterije za procjenu dobavljača 5G opreme i njihovo svrstavanje u skupinu visokorizičnih dobavljača te za pitanja u vezi sa zaštitom podataka.

Rok provedbe: prosinac 2022.

(b) zajamčiti transparentnost pristupa sigurnosti 5G mreža u državama članicama, i to praćenjem provedbe sigurnosnih mjera paketa instrumenata EU-a za kibersigurnost 5G mreža te izvješćivanjem o njoj. To bi se trebalo obavljati s pomoću zajedničkog skupa pokazatelja uspješnosti.

Rok provedbe: prosinac 2022.

(c) zajedno s državama članicama procijeniti za koje je aspekte sigurnosti 5G mreža potrebno utvrditi zahtjeve čije se ispunjavanje može zajamčiti i, prema potrebi, poticati donošenje zakonodavstva.

Rok provedbe: prosinac 2022.

92. Komisija je započela rješavanje pitanja povezanih navoda o nepravednoj gospodarskoj prednosti zbog stranih subvencija. Takve subvencije mogu narušiti

unutarnje tržište i na taj način stvoriti neravnopravne uvjete među dobavljačima 5G opreme s mogućim posljedicama za sigurnost (vidjeti odlomak ***78***.).

93. Komisija ne raspolaže dovoljnim informacijama o postupanju država članica u pogledu potencijalnih troškova zamjene koji bi mogli nastati u slučaju u kojem bi operatori pokretnih mreža trebali ukloniti opremu visokorizičnih dobavljača iz mreža EU-a bez prijelaznog razdoblja. Razlikama u postupanju može se narušiti poslovna sigurnost i ugroziti pravodobno uvođenje 5G mreža (vidjeti odlomke ***79***. i ***80***.). Istodobno, pristupi sigurnosti 5G mreža u državama članicama, a posebno činjenica da na razini EU-a ne postoji usklađen pristup, mogu se odraziti na djelotvorno funkcioniranje jedinstvenog tržišta. Komisija dosad nije obavila procjenu tog pitanja (vidjeti odlomke ***74***. – ***76***.).

3. preporuka – Potrebno je pratiti pristupe država članica sigurnosti 5G mreža i procijeniti učinak razlika u njihovim pristupima na djelotvorno funkcioniranje jedinstvenog tržišta

Komisija bi trebala:

(a) promicati transparentan i usklađen pristup u postupanju država članica u pogledu podmirivanja troškova operatora pokretnih mreža za zamjenu 5G opreme nabavljene od visokorizičnih dobavljača, i to redovnim praćenjem tog pitanja i izvješćivanjem o njemu u okviru provedbe paketa instrumenata EU-a za kibersigurnost 5G mreža.

(b) procijeniti kakav bi učinak na jedinstveno tržište imali slučajevi u kojima bi pojedina država članica svoje 5G mreže uspostavila s pomoću opreme dobavljača koji se u drugoj državi članici smatra visokorizičnim.

Rok provedbe: prosinac 2022.

Ovo je izvješće usvojilo II. revizijsko vijeće, kojim predsjeda članica Revizorskog suda Iliana Ivanova, u Luxembourgu 15. prosinca 2021.

Za Revizorski sud

Klaus-Heiner Lehne
predsjednik

Prilozi

Prilog I. – Glavne mogućnosti i rizici 5G tehnologije

Izvor: Sud, na temelju Službe Europskog parlamenta za istraživanja – Europski centar za znanstvene medije.

Prilog II. – Primjeri učinka ometanja telekomunikacijskih mreža i kibersigurnosnih incidenata

Prekid telefonskih linija za hitne službe u Francuskoj[66,67]

01 Dana 3. lipnja 2021. prekid rada mreže najvećeg francuskog telekomunikacijskog društva Orange onemogućio je hitne pozive tijekom razdoblja od nekoliko sati. Premda je kibernapad isključen kao uzrok, predmetni incident primjer je mogućeg učinka poremećaja u radu ključne mrežne infrastrukture.

Napad *ransomwarea* na sustav irskog javnog zdravstva[68,69,70]

02. U svibnju 2021. irska uprava za javno zdravstvo (eng. Health Service Executive) isključila je sve svoje IT sustave zbog napada *ransomwarea*. Napad je pogodio sve aspekte skrbi o pacijentima jer je prouzročio poteškoće u pristupu zdravstvenim kartonima pacijenata, čime se povećala opasnost od kašnjenja i pogrešaka. Iako prema informacijama koje raspolažu irski službenici podatci pacijenata nisu bili ugroženi, dijeljenje zdravstvenih kartona moglo je dovesti do bilo koje vrste potencijalnih kaznenih djela, kao što su prijevara i ucjena. Glavni direktor uprave za javno zdravstvo smatra da će procijenjeni troškovi oporavka vjerojatno iznositi 500 milijuna eura (600 milijuna američkih dolara).

---

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-11 620 998 875

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/hr/blog_DataBreachTodayinRSS Syndication-in-299 786a86ffeab5aec16d55 392d94 819.20 210 624.en.html

Solarwinds[71,72,73]

03. Solarwinds je američko društvo koje razvija softvere kako bi pomoglo poduzećima te državnim i saveznim agencijama u upravljanju njihovim mrežama, sustavima i infrastrukturom informacijske tehnologije. Početkom 2020. Solarwinds je bio žrtva softverskog napada. Hakeri su uspjeli proširiti napade na klijente društva Solarwinds nadogradnjama softvera koje su sadržavale zlonamjerne kodove. Na temelju njih omogućen je „pristup sa stražnjeg ulaza" u korisničke platforme, što je otvorilo mogućnost lakih napada i postavljanja dodatnih zlonamjernih i špijunskih softvera.

[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

Prilog III. – Pravni okvir i okvir politike

Europska komisija

Europsko Vijeće Vijeće EU-a

Zakonodavstvo

Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava

2016. Direktiva NIS, srpanj 2016. – Pružanje pravnih mjera za jačanje ukupne razine kibersigurnosti u EU-u.

2016. Akcijski plan za 5G, rujan 2016. – Cilj je pokretanje 5G usluga u svim državama članicama najkasnije do kraja 2020., nakon čega slijedi brza uspostava kako bi se zajamčila kontinuirana pokrivenost 5G mrežama u gradskim područjima i duž glavnih prometnih pravaca do 2025.

2018. Europski zakonik elektroničkih komunikacija, prosinac 2018. – Cilj je uspostava unutarnjeg tržišta u području mreža i usluga elektroničke komunikacije.

2019. Zaključci Europskog vijeća, ožujak 2019. – Ususret preporuci Komisije o usklađenom pristupu sigurnosti 5G mreža.

2019. Preporuka o kibersigurnosti 5G mreža, ožujak 2019. – Preporuka državama članicama da na nacionalnoj razini procjenjuju kibersigurnosne rizike koji utječu na 5G mreže i poduzimaju potrebne sigurnosne mjere.

2019. Zaključci Vijeća o važnosti mreža 5G za europsko gospodarstvo, prosinac 2019. – Naglašava se da je brzo i sigurno uvođenje 5G mreža ključno za jačanje konkurentnosti EU-a i zahtijeva se usklađen pristup u EU-u.

2020. Paket instrumenata za sigurnost 5G mreža, siječanj 2020. – Utvrđuju se moguće zajedničke mjere za ublažavanje glavnih kibersigurnosnih rizika koji proizlaze iz 5G mreža.

2020. Sigurno uvođenje 5G mreža u EU-u – Provedba paketa instrumenata EU-a za kibersigurnost 5G mreža, siječanj 2020. – Europska komisija odobrava paket instrumenata i utvrđuje daljnje korake (npr. izvješće o provedbi do lipnja 2020.).

2020. Zaključci Vijeća o oblikovanju digitalne budućnosti Europe, lipanj 2020. – Podupire se potreba da se zajamči i provede usklađen pristup za ublažavanje glavnih rizika za sigurno uvođenje 5G mreža u EU-u.

2020. Zaključci Europskog vijeća, listopad 2020. – Odobravanje paketa instrumenata za kibersigurnost 5G mreža, posebno potrebe za primjenu relevantnih ograničenja na visokorizične dobavljače.

2020. Preporuka o (...) pristupu radiofrekvencijskom spektru za mreže 5G, rujan 2020. – Utvrđivanje smjernica za razvoj najboljih praksi za poticanje povezivosti i pružanje pravodobnog i investicijski poticajnog pristupa radiofrekvencijskom spektru za 5G mreže.

2020. Strategija EU-a za kibersigurnost za digitalno desetljeće, prosinac 2020. – Dokument neobvezujućeg prava u kojem se utvrđuju prioriteti Komisije i planirane mjere za kibersigurnost u cjelini, uključujući 5G mreže.

2020. Prijedlog direktive NIS 2, prosinac 2020. – Cilj dokumenta je modernizacija i širenje područja primjene aktualne direktive te također eksplicitnije obuhvaćanje kibersigurnosti 5G mreža.

2020. Prijedlog direktive o otpornosti kritičnih subjekata, prosinac 2020. – Cilj je ublažiti ranjivosti kritične infrastrukture koja je ključna za funkcioniranje društva i gospodarstva EU-a.

2020. Digitalni kompas 2030.: europski pristup za digitalno desetljeće, ožujak 2021. – Zacrtavanje puta prema zajedničkoj viziji i koracima koje Europa mora poduzeti za uspjeh digitalnog desetljeća.

2021. Zaključci Vijeća o Strategiji EU-a za kibersigurnost za digitalno desetljeće, ožujak 2021. – Podupiranje daljnjih koraka koje je potrebno poduzeti za kibersigurnost 5G mreža, kako je utvrđeno u strategiji Komisije za kibersigurnost.

Prilog IV. – Primjeri projekata sufinanciranih iz EFSU-a

Projekti EFSU-a povezani s 5G mrežama

Dva projekta EFSU-a koje je Sud pregledao odnosila su se na ulaganja u području istraživanja, razvoja i inovacija za razvoj portfelja proizvoda 5G mreža. Oba su uključivala razvoj hardvera i softvera za pristupnu radijsku mrežu kao i za osnovnu mrežu. Oba su projekta doprinijela gušćem postavljanju ćelija, poduprla su standardizaciju i olakšala ključne tehnološke eksperimente.

Projekti su započeli 2018. i završili u prosincu 2020. Ukupni troškovi ulaganja za ta dva projekta iznosili su 3,9 milijardi eura, uključujući financijska sredstva u iznosu od 1 milijarde eura iz EFSU-a.

Prilog V. – Primjeri projekata u okviru programa Obzor 2020. i EFRR-a

Projekt programa Obzor 2020. povezan s 5G mrežama

U tom projektu, u kojemu se upotrebljava oprema triju glavnih dobavljača 5G opreme (Ericsson, Huawei i Nokia), ispituju se 5G tehnologije na prekograničnom koridoru koji povezuje gradove Metz (Francuska), Merzig (Njemačka) i Luxembourg. Započeo je u studenome 2018. i trebao je trajati 31 mjesec. EU je odobrio 12,9 milijuna eura za namirenje ukupnog proračunom predviđenog troška od 17,1 milijun eura.

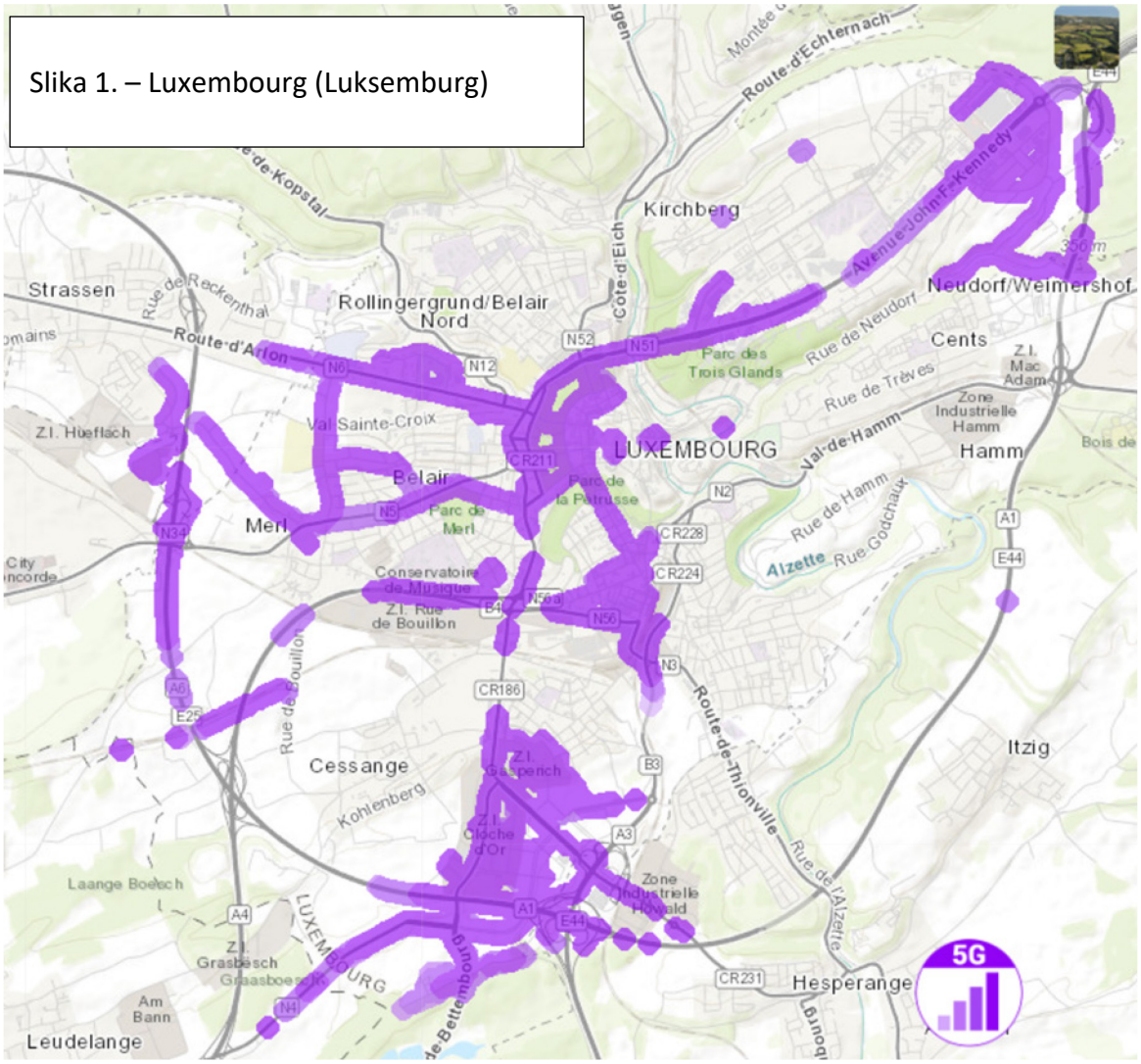
Projekt EFRR-a povezan s 5G mrežama

Tim se projektom u Španjolskoj žele pružiti uvidi u uvođenje 5G mreža. Projekt uključuje eksperimentiranje s tehnikama upravljanja mrežama koje omogućuje 5G tehnologija, kao što su virtualizacija mrežnih funkcija, računalstvo na rubu mreže, dinamična dodjela mrežne usluge i segmentiranje mreže te razvoj slučajeva primjene 5G mreža. Projekt je započeo 2019. i trebao je trajati 30 mjeseci. EU je pružio doprinos u iznosu od 2,2 milijuna eura za namirenje ukupnog očekivanog troška od 7,1 milijun eura.

Prilog VI. – Pokrivenost 5G mrežama u odabranim gradovima

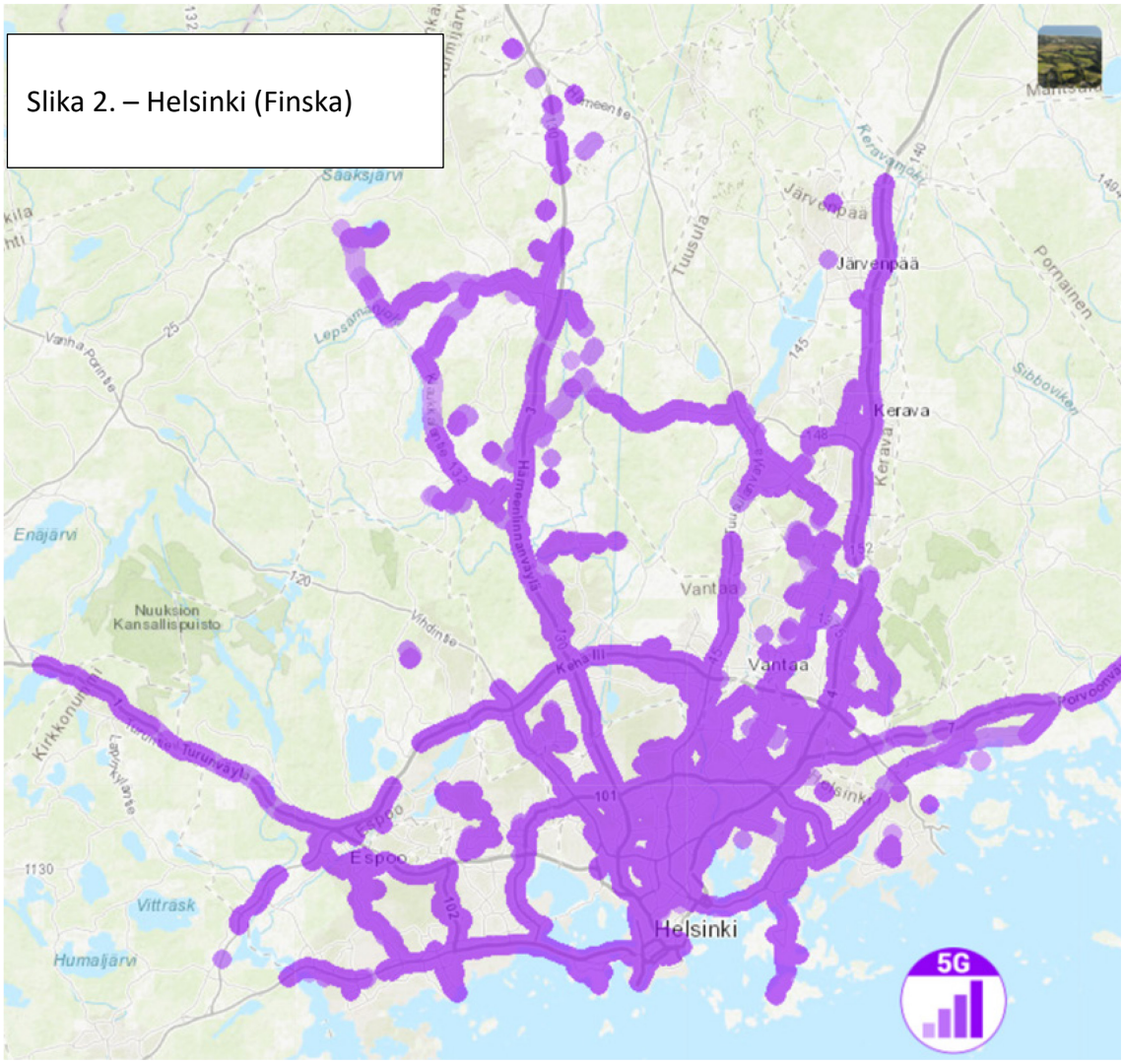
Podatci u nastavku temelje se na podatcima o mobilnoj širokopojasnoj vezi koji su prikupljeni iz testova koje su proveli korisnici aplikacije Nperf. Područja u kojima su otkrivene 5G mreže nisu nužno komercijalno dostupna. Budući da uspješnost mreža ovisi o pojedinačnim operatorima pokretnih mreža, zemljovidi u nastavku preuzeti 4. listopada 2021., prikazuju samo pokrivenost, ali ne i stupanj funkcionalnosti, kao što su brzina i latencija.

Slika 1. – Luxembourg (Luksemburg)

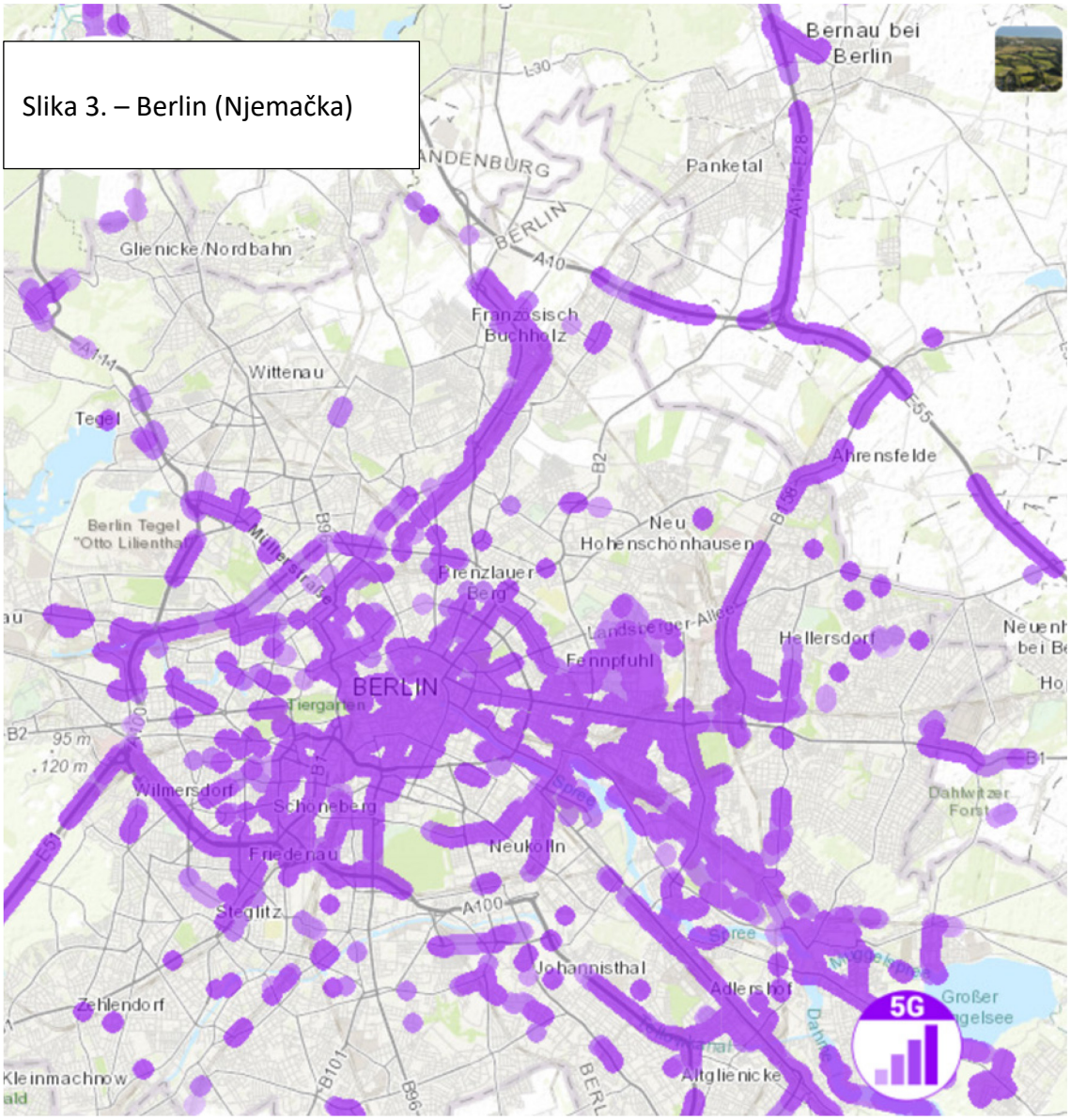


© nPerf.

Slika 2. – Helsinki (Finska)

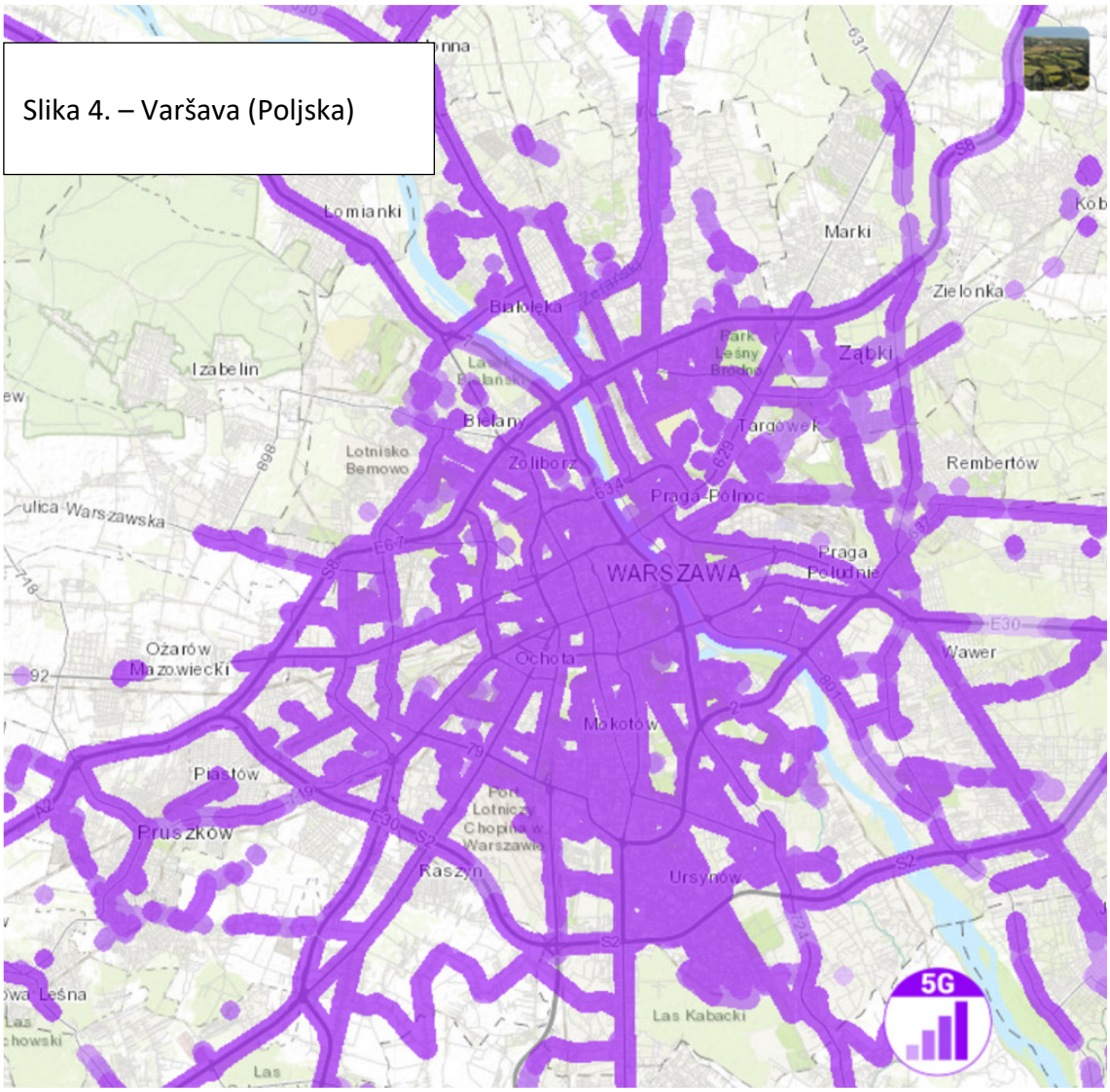


© nPerf.

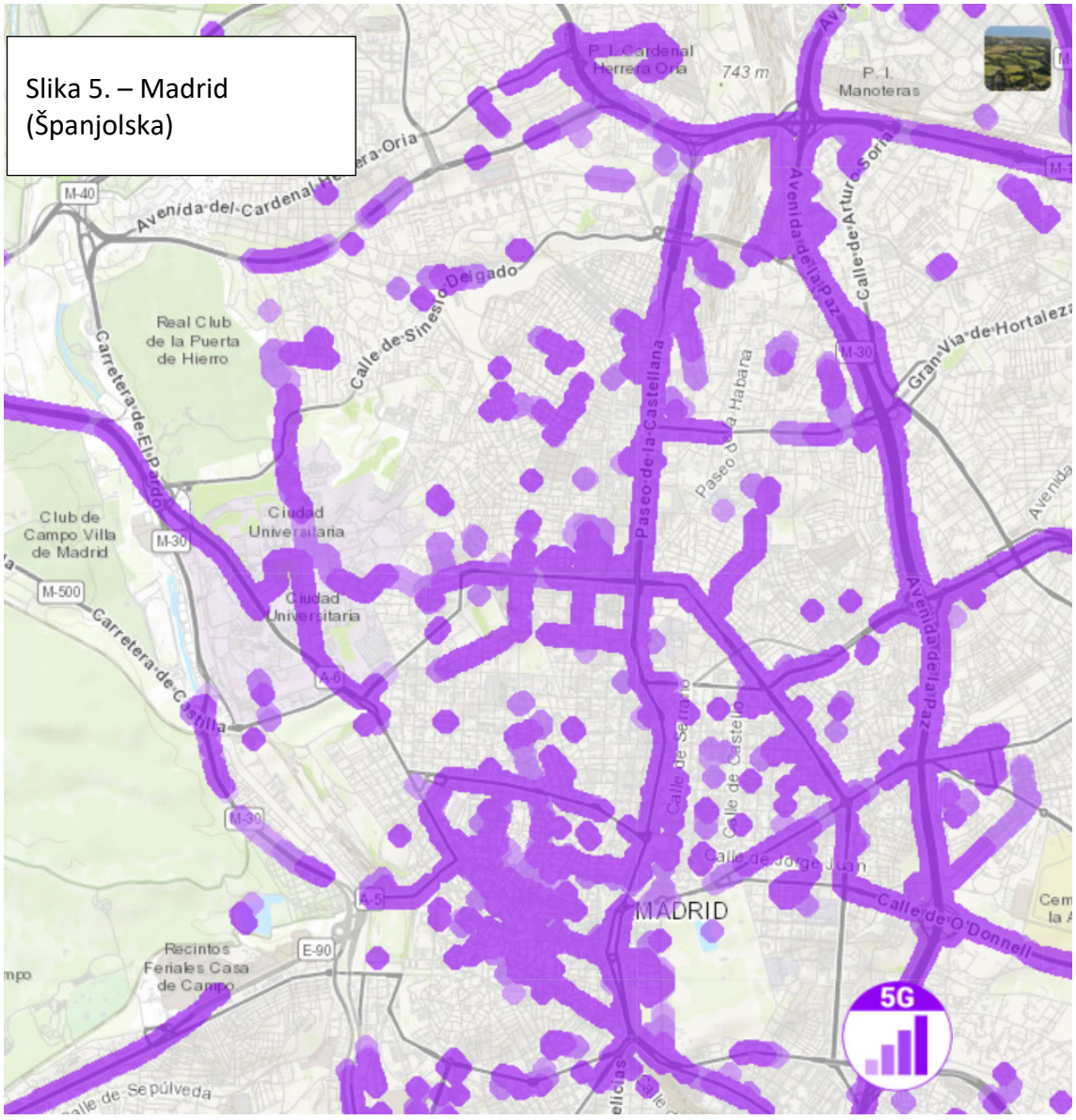


Slika 3. – Berlin (Njemačka)

© nPerf.


Slika 4. – Varšava (Poljska)
Łomianki
Marki
Zielonka
Izabelin
Bielany
Ząbki
Lotnisko Bemowo
Żoliborz
Targówek
Rembertów
Praga-Północ
ulica Warszawska
WARSZAWA
Praga-Południe
Ochota
Wawer
Ożarów Mazowiecki
Piastów
Mokotów
Pruszków
Raszyn
Ursynów
Las Kabacki
5G

© nPerf.



Slika 5. – Madrid (Španjolska)

Prilog VII. – Paket instrumenata EU-a za kibersigurnost 5G mreža

Paket instrumenata EU-a za kibersigurnost 5G mreža koji je donijela Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava i koji je odobrila Komisija uključuje tri vrste neobvezujućih mjera (strateške i tehničke mjere te mjere potpore) koje trebaju provesti različiti akteri, kako je sažeto u nastavku.

Mjere	Relevantni akteri				
	Tijela država članica	Operatori pokretnih mreža	Europska komisija	ENISA	Dionici (uključujući dobavljači)
Strateške mjere					
SM01 – Jačanje uloge nacionalnih tijela	✓	✓			
SM02 – Obavljanje preispitivanja operatora i zahtjev za informacijama	✓	✓			
SM03 – Procjena profila rizičnosti dobavljača i primjena ograničenja na dobavljače koji se smatraju visokorizičnima, uključujući neophodna isključenja radi djelotvornog ublažavanja rizika za ključnu imovinu	✓	✓			
SM04 – Kontroliranje korištenja podrškom treće razine pružatelja upravljanih usluga i dobavljača opreme	✓	✓			
SM05 – Jamčenje raznolikosti dobavljača za pojedinačne operatore pokretnih mreža odgovarajućim strategijama nabave od više dobavljača	✓	✓			
SM06 – Jačanje otpornosti na nacionalnoj razini	✓	✓			
SM07 – Utvrđivanje ključne imovine i poticanje raznolikog i održivog 5G ekosustava u EU-u	✓		✓		
SM08 – Održavanje i izgradnja raznolikosti i kapaciteta EU-a u budućim mrežnim tehnologijama	✓		✓		✓
Tehničke mjere					
TM01 – Jamčenje primjene osnovnih sigurnosnih zahtjeva (sigurna izrada i arhitektura mreže)	✓	✓			
TM02 – Jamčenje i ocjenjivanje provedbe sigurnosnih mjera u postojećim standardima za 5G mreže	✓	✓			✓
TM03 – Jamčenje strogih kontrola pristupa	✓	✓			
TM04 – Povećanje sigurnosti virtualiziranih mrežnih funkcija	✓	✓			
TM05 – Jamčenje sigurnog upravljanja 5G mrežama te njihovog sigurnog rada i praćenja	✓	✓			

Mjere	Relevantni akteri				
	Tijela država članica	Operatori pokretnih mreža	Europska komisija	ENISA	Dionici (uključujući dobavljači)
TM06 – Povećanje fizičke sigurnosti	✓	✓			
TM07 – Jačanje softverskog integriteta, ažuriranja i postupanja sa sigurnosnim zakrpama	✓	✓			
TM08 – Povećanje sigurnosnih standarda u procesima dobavljača utvrđivanjem dobro definiranih uvjeta nabave	✓	✓			✓
TM09 – Upotreba certifikacije EU-a za sastavnice 5G mreža, opremu korisnika i/ili procese dobavljača	✓	✓	✓	✓	✓
TM10 – Upotreba certifikacije EU-a za druge proizvode i usluge IKT-a koji nisu specifični za 5G mrežu (povezani uređaji, usluge u digitalnom oblaku)	✓		✓	✓	✓
TM11 – Jačanje otpornosti i planovi kontinuiteta	✓	✓			✓
Mjere potpore					
PM01 – Preispitivanje ili razvoj smjernica i najboljih praksi za mrežnu sigurnost	✓	✓		✓	
PM02 –Povećanje sposobnosti ispitivanja i preispitivanja na nacionalnoj razini i razini EU-a	✓		✓	✓	
PM03 – Podupiranje i oblikovanje standardizacije 5G tehnologije	✓	✓	✓	✓	✓
PM04 – Razvoj smjernica za provedbu sigurnosnih mjera u postojećim standardima za 5G mreže	✓			✓	
PM05 – Jamčenje primjene standardnih tehničkih i organizacijskih sigurnosnih mjera u okviru posebnog sustava certifikacije na razini EU-a	✓			✓	✓
PM06 – Razmjena najboljih praksi provedbe strateških mjera, posebno nacionalnih okvira za procjenu profila rizičnosti dobavljača	✓				
PM07 – Poboljšanje usklađenosti u odgovoru na incidente i upravljanju krizama	✓			✓	
PM08 – Provedba preispitivanja međuovisnosti 5G mreža i drugih ključnih usluga	✓				
PM09 – Poboljšanje mehanizama suradnje, koordinacije i razmjene informacija	✓			✓	
PM10 – Jamčenje toga da se u projektima 5G mreža koji se financiraju javnim sredstvima uzimaju u obzir kibersigurnosni rizici	✓		✓		

Izvor: Paket instrumenata EU-a za kibersigurnost 5G mreža.

Pokrate i kratice

BDP: bruto domaći proizvod

BEREC: Tijelo europskih regulatora za elektroničke komunikacije

EFRR: Europski fond za regionalni razvoj

EFSU: Europski fond za strateška ulaganja

EIB: Europska investicijska banka

ENISA: Agencija Europske unije za mrežnu i informacijsku sigurnost

RSPG: Skupina za politiku radiofrekvencijskog spektra

Pojmovnik

Agencija Europske unije za kibersigurnost: agencija EU-a osnovana za razvoj i održavanje mrežne i informacijske sigurnosti visoke razine u svim sektorima privatne i javne sfere.

Eksabajt: mjera za kapacitet pohrane digitalnih informacija jednakovrijedna 1 milijardi gigabajta.

Europski fond za strateška ulaganja: mehanizam za potporu ulaganjima koji su uvele Europska investicijska banka (EIB) i Komisija u sklopu Plana ulaganja za Europu, i to s ciljem privlačenja privatnih ulaganja u projekte koji su strateški važni za EU.

Internet stvari: fizički predmeti u koje su ugrađeni senzori, softveri i druge tehnologije koji im omogućuju da se bežično spoje i razmjenjuju podatke s drugim uređajima i sustavima.

Latencija: u računalnim mrežama, vrijeme potrebno da skup podataka dospije od jedne točke do druge.

Nacionalni planovi za razvoj širokopojasnog pristupa internetu: dokumenti država članica koji sadržavaju strateške ciljeve za dosezanje ciljnih vrijednosti EU-a u području širokopojasnog pristupa internetu.

Operator pokretne mreže: telekomunikacijsko poduzeće koje osigurava bežičnu glasovnu i podatkovnu komunikaciju za pretplaćene korisnike mobitela.

Pristupna radijska mreža: velik dio moderne telekomunikacijske tehnologije kojim se pojedinačni uređaji povezuju s drugim dijelovima mreže s pomoću radijskih veza.

Radiofrekvencijski spektar: dio elektromagnetskog spektra koji odgovara radijskim frekvencijama.

***Ransomware*:** zlonamjerni program koji žrtvama onemogućuje pristup računalnom sustavu ili čitanje datoteka te ih prisiljava da plate otkupninu za ponovno stjecanje pristupa.

Skupina za politiku radiofrekvencijskog spektra: savjetodavna skupina na visokoj razini koju čine predstavnici država članica i koja pomaže institucijama EU-a i savjetuje ih u pogledu razvoja jedinstvenog tržišta u području bežičnih proizvoda i usluga.

Skupina za suradnju u području mrežnih i informacijskih sustava: tijelo osnovano na temelju Direktive NIS za jamčenje suradnje i razmjene informacija među državama članicama koje se sastoji od predstavnika država članica EU-a, Europske komisije i Agencije EU-a za kibersigurnost.

Širokopojasni pristup: vrlo brzi istodobni prijenos više informacijskih formata (kao što su podatci, glas i videozapis).

Tijelo europskih regulatora za elektroničke komunikacije: tijelo koje čine predstavnici nacionalnih regulatornih tijela država članica i koje pomaže tim tijelima i Komisiji u provedbi regulatornog okvira EU-a u cilju stvaranja jedinstvenog tržišta za elektroničke komunikacije.

Udruga za globalni sustav pokretnih telekomunikacija (GSMA): organizacija predmetnog sektora koja zastupa interese mobilnih operatora diljem svijeta, kao i poduzeća i organizacija za proizvodnju i pružanje usluga s interesima u području mobilne infrastrukture.

Odgovori Komisije

https://www.eca.europa.eu/hr/Pages/DocItem.aspx?did=60 614

Kronologija

https://www.eca.europa.eu/hr/Pages/DocItem.aspx?did=60 614

Revizorski tim

U tematskim izvješćima Suda iznose se rezultati revizija koje su provedene za politike i programe EU-a ili teme povezane s upravljanjem u posebnim proračunskim područjima. U odabiru i oblikovanju takvih revizijskih zadataka Sud nastoji postići što veći učinak uzimajući u obzir rizike za uspješnost ili usklađenost, vrijednost predmetnih prihoda ili rashoda, predstojeće razvojne promjene te politički i javni interes.

Ovu reviziju uspješnosti provelo je II. revizijsko vijeće, kojim predsjeda članica Suda Iliana Ivanova i koje je specijalizirano za rashodovna područja ulaganja u koheziju, rast i uključivanje. Reviziju je predvodila članica Suda Annemie Turtelboom, a potporu su joj pružali voditeljica njezina ureda Florence Fornaroli i ataše u njezinu uredu Dželil Išik, rukovoditelj Niels-Erik Brokopp, voditelj radnog zadatka Paolo Pesce te revizori Jussi Bright, Rafal Gorajski, Zuzana Gullová, Alexandre Tan, Aleksandar Latinov i Nils Westphal.

Annemie Turtelboom

Florence Fornaroli

Celil Ishik

Niels-Erik Brokopp

Paolo Pesce

Jussi Bright

Rafal Gorajski

Zuzana Gullová

Aleksandar Latinov

Nils Westphal

PDF	ISBN 978-92-847-7409-8	ISSN 2315-2230	doi:10.2865/535339	QJ-AB-21-029-HR-N
HTML	ISBN 978-92-847-7380-0	ISSN 2315-2230	doi:10.2865/177612	QJ-AB-21-029-HR-Q

Očekuje se da bi doprinos 5G mreža europskom BDP-u u razdoblju 2021. – 2025. mogao dosegnuti iznos do 1 bilijuna eura uz potencijal za otvaranje ili preobrazbu do 20 milijuna radnih mjesta u svim sektorima gospodarstva. Sud je utvrdio da se zbog kašnjenja dovodi u pitanje ostvarivanje ciljeva EU-a u području uvođenja 5G mreža i da je potrebno uložiti dodatne napore u rješavanje sigurnosnih pitanja. Sud u ovom izvješću iznosi niz preporuka Komisiji u cilju poticanja pravodobnog i usklađenog uvođenja sigurnih 5G mreža u EU-u.

Tematsko izvješće Suda u skladu s člankom 287. stavkom 4. drugim podstavkom UFEU-a.

EUROPSKI REVIZORSKI SUD

Ured za publikacije Europske unije

EUROPSKI REVIZORSKI SUD
12, rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel.: +352 4398-1

Upiti: eca.europa.eu/hr/Pages/ContactForm.aspx
Internetske stranice: eca.europa.eu
Twitter: @EUAuditors