EUROPSKA
KOMISIJA

Bruxelles, 29.1.2020.
COM(2020) 50 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA

Sigurno uvođenje 5G mreža u EU-u – Provedba paketa instrumenata EU-a

1. *Uvod*

Peta generacija telekomunikacijskih mreža (5G) trebala bi imati ključnu ulogu u razvoju europskog društva i gospodarstva. Očekuje se da će pružiti znatne gospodarske mogućnosti i biti važan temelj digitalne i zelene transformacije u područjima kao što su promet, energetika, proizvodnja, zdravstvo, poljoprivreda i mediji.

Stoga 5G tehnologija može utjecati na sve aspekte života građana EU-a. Kibersigurnost 5G mreža kritična je ne samo radi zaštite naših gospodarstava, društva i demokratskih procesa, nego i kao jamstvo pouzdane digitalne transformacije društva u korist svih građana EU-a.

Zbog ovisnosti mnogih ključnih usluga o 5G mrežama posljedice sustavnih i raširenih poremećaja bile bi iznimno ozbiljne, a s obzirom na međusobnu povezanost digitalnih ekosustava, mogle bi se znatno osjetiti i izvan nacionalnih granica. Zbog toga je, u vrijeme kada su kibernapadi sve brojniji, sofisticiraniji nego ikad i potječu od raznovrsnih aktera prijetnji, osobito iz trećih zemalja ili aktera koji imaju potporu države, kibersigurnost 5G mreža strateški bitna za Uniju. Kad je riječ o sigurnosti kritičnih infrastruktura kao što su 5G mreže, odlučeno je da će se po prvi put utvrditi zajednički europski pristup. Tim se pristupom u potpunosti poštuje otvorenost unutarnjeg tržišta EU-a pod uvjetom da se poštuju sigurnosni zahtjevi EU-a koji se temelje na procjeni rizika.

Europsko vijeće pozvalo je 22. ožujka 2019. na usklađeni pristup sigurnosti 5G mreža. Komisija je 26. ožujka 2019. donijela Preporuku (EU) 2019/534 o kibersigurnosti 5G mreža[1]. U Preporuci se države članice pozivaju da dovrše nacionalne procjene rizika i preispitaju nacionalne mjere te da na razini EU-a surađuju radi koordinirane procjene rizika i pripreme paketa instrumenata mogućih mjera za smanjivanje rizika. Ova je Komunikacija sastavni dio Komisijine sveobuhvatne europske digitalne strategije, na koju je pozvalo Europsko vijeće.

2. *Uvođenje 5G tehnologije u EU-u*

Uvođenje 5G mreža u Europi od primarne je važnosti za europsku industrijsku strategiju i konkurentnost. Komisija smatra da je uvođenje 5G mrežnih tehnologija glavni pokretač budućih digitalnih usluga. Komisija je 2016. donijela akcijski plan za 5G kako bi se u Uniji osigurala infrastruktura za povezivost koja je potrebna za digitalnu transformaciju do 2020. i za sveobuhvatno uvođenje u gradskim područjima i glavnim prometnim putovima do 2025.[2] U Komunikaciji o gigabitnom društvu iznesena je ambicija da se pristup mobilnoj podatkovnoj povezivosti omogući svugdje[3], uključujući ruralna i udaljena područja.

Kad je riječ o dodjeli frekvencija, države članice dodijelile su 16 % početnih frekvencijskih pojaseva 5G mreže[4]. U sljedećih nekoliko mjeseci očekuje se dovršetak savjetovanja o postupcima dodjele s obzirom na pravnu obvezu dopuštanja uporabe svih početnih frekvencijskih pojaseva 5G do kraja godine.

[1] Preporuka Komisije (EU) 2019/534 – Kibersigurnost 5G mreža, SL L 88, 29.3.2019., str. 42.–47.
[2] COM(2016) 588 od 14. lipnja 2016., 5G za Europu: Akcijski plan
[3] Povezivošću do konkurentnog jedinstvenog digitalnog tržišta – Ususret europskom gigabitnom društvu, COM(2016) 587.
[4] http://www.5GObservatory.eu

Kad je riječ o komercijalnom uvođenju 5G usluga, Europa je jedna od najnaprednijih regija svijeta[5]. Trenutačno se očekuje da će prve 5G usluge biti dostupne u 138 europskih gradova do kraja 2020. Prve 5G mreže temelje se na trenutačnoj 4. generaciji (4G) mrežnih tehnologija. 5G usluge uglavnom se pružaju široj javnosti, bilo kao poboljšanje kapaciteta i brzine 4G ili kao troškovno učinkovita bežična alternativa fiksnim mrežama[6].

Kad je riječ o mogućnostima u vezi s novim uslugama među poduzećima, primjerice u sektorima energetike, prehrane i poljoprivrede, zdravstva, proizvodnje ili prometa, Europa je ostvarila dobar napredak ulaganjem u iznosu od 1 milijarde EUR, uključujući 300 milijuna EUR sredstava EU-a u kontekstu javno-privatnog partnerstva za 5G u okviru programa Obzor 2020. To ulaganje obuhvaća više od 160 opsežnih ispitivanja 5G mreža definiranih na razini Europe, uključujući deset prekograničnih koridora za autoceste za opsežna ispitivanja usluga povezane i automatizirane mobilnosti temeljenih na 5G mrežama. Ispitivanja uključuju aplikacije na temelju 5G tehnologije u rasponu od održive zdravstvene skrbi i automatizirane mobilne resursno učinkovite poljoprivrede do pametnih elektroenergetskih mreža i industrije 4.0. Usto je Europska investicijska banka (EIB), uz sredstva iz Europskog fonda za strateška ulaganja, dodijelila zajmove za ubrzanje istraživanja i razvoja 5G tehnologije.

Europski zakonik elektroničkih komunikacija („Zakonik”)[7], koji će se primjenjivati od 21. prosinca 2020., važan je temelj za stvaranje okruženja pogodnog za ulaganja u 5G mreže i šire. Nadalje, programima javnog financiranja, kao što je Instrument za povezivanje Europe u digitalnom sektoru[8] ili europski strukturni i investicijski fondovi, pružat će se neophodna potpora i budućem uvođenju 5G mreža, osobito povezivanjem zajednica s uslugama na temelju 5G (škole, bolnice, gradovi i lokalne uprave).

S obzirom na strateške mogućnosti Europe u području 5G usluga za razne industrije, od ključne je važnosti da operatori i pružatelji usluga ulažu u naprednu 5G mrežu i uslužna rješenja. Tu nije riječ samo o novim radijskim 5G mrežama, nego i novim „samostalnim” osnovnim 5G mrežama kako bi se omogućile napredne funkcionalnosti 5G tehnologije, kao što su segmentiranje mreže[9] i računalstvo na rubu mreže[10].

Komisija će i dalje pružati punu potporu uspješnom uvođenju 5G mreža u EU-u, među ostalim suradnjom s državama članicama i dionicima kako bi se iskoristile mogućnosti koje 5G tehnologija nudi. U obzir će se uzeti relevantni zdravstveni aspekti na temelju načela

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

[6] Neke od novih funkcionalnosti mreže 5G uvodit će se postupno. U prvoj fazi (u kratkom ili vrlo kratkom roku) uvođenje 5G mreže odnosit će se uglavnom na „nesamostalne” mreže, u kojima je samo radijska pristupna mreža proširena na 5G tehnologiju, a inače se i dalje oslanja na postojeće osnovne 4G mreže, čime se krajnjim korisnicima poboljšavaju mobilne širokopojasne usluge. U sljedećim fazama (kratkoročne/srednjoročne do dugoročne) bit će potrebno uvesti „samostalne” 5G mreže, uključujući funkcije osnovne 5G mreže, što će s vremenom dovesti do bitno opsežnijih promjena u mrežnoj strukturi.

[7] Direktiva (EU) 2018/1972 Europskog parlamenta i Vijeća o Europskom zakoniku elektroničkih komunikacija (preinaka).

[8] Prijedlog uredbe Europskog parlamenta i Vijeća od 6 lipnja 2018. o uspostavljanju Instrumenta za povezivanje Europe i stavljanju izvan snage uredbi (EU) br. 1316/2013 i (EU) br. 283/2014 (COM/2018/438 final).

[9] Segmentiranjem 5G mreže postiže se visok stupanj razdvajanja između različitih razina usluga na istoj fizičkoj mreži, čime se povećavaju mogućnosti ponude diferenciranih usluga u cijeloj mreži.

[10] Računalstvo na rubu mreže jest distribuirano računalstvo kojim se računalstvo i pohrana podataka približavaju mjestima na kojima su potrebni kako bi se poboljšalo vrijeme odziva i smanjila upotreba pojasne širine.

predostrožnosti[11], u suradnji s nadležnim međunarodnim organizacijama i znanstvenom zajednicom.

3. Usklađena procjena rizika na razini EU-a za kibersigurnost 5G mreža

Zajedničkim radom u okviru Skupine za suradnju u području mrežne i informacijske sigurnosti[12] sve države članice dovršile su nacionalne procjene rizika svojih 5G mrežnih infrastruktura i do početka srpnja 2019. dostavila rezultate Komisiji i ENISA-i, Agenciji Europske unije za kibersigurnost.

Na temelju tih nacionalnih procjena rizika Skupina za suradnju u području mrežne i informacijske sigurnosti, koju čine predstavnici država članica, Komisije i ENISA-e, objavila je 9. listopada 2019. izvješće o usklađenoj procjeni rizika na razini EU-a za kibersigurnost 5G mreža[13]. U izvješću se navode najvažnije prijetnje i akteri koji ih uzrokuju, najosjetljivija infrastruktura, glavne slabosti (uključujući tehničke i druge vrste slabosti) koji utječu na 5G mreže. Na temelju toga u izvješću je utvrđen i niz kategorija strateški važnih rizika iz perspektive EU-a, ilustriranih konkretnim scenarijima rizika u kojima se odražavaju relevantne kombinacije različitih parametara (slabosti, prijetnje i akteri prijetnji) u odnosu na različitu infrastrukturu (vidjeti Dodatak).

ENISA je kao nadopunu ovom izvješću i kao dodatni doprinos paketu instrumenata sastavila poseban pregled prijetnji[14], koji sadržava detaljnu analizu određenih tehničkih aspekata, a posebno identificiranje mrežne infrastrukture i prijetnji koje utječu na njih.

U izvješću o usklađenoj procjeni rizika na razini EU-a ističe se niz aspekata važnih za 5G mreže. Konkretno:

a) Tehnološke promjene uvedene 5G tehnologijom povećat će sveukupnu površinu napada i broj potencijalnih ulaznih točaka za napadače:

– pojačana funkcionalnost na rubu mreže i manja centraliziranost arhitekture u odnosu na prijašnje generacije mobilnih mreža znači da neke funkcije osnovnih mreža mogu biti integrirane u druge dijelove mreža, što povećava osjetljivost odgovarajuće opreme (npr. baznih stanica ili funkcija MANO);

– zbog povećane uloge softvera u 5G opremi povećavaju se rizici povezani s razvojem softvera i postupcima ažuriranja, nastaju novi rizici od pogrešaka u konfiguraciji, a u analizi sigurnosti povećava se važnost odluka koje svaki operator pokretne mreže donese u fazi uvođenja mreže;

b) Zbog tih novih tehnoloških obilježja znatno će se povećati ovisnost operatora pokretne mreže o neovisnim dobavljačima i njihova uloga u lancu opskrbe tehnologijom 5G.

[11] Preporuka Vijeća od 12. srpnja 1999. o ograničavanju izloženosti stanovništva elektromagnetskim poljima (od 0 Hz do 300 GHz) (1999/519/EZ)

[12] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (Direktiva NIS). Skupina za suradnju u području mrežne i informacijske sigurnosti uspostavljena je Direktivom NIS radi osiguravanja strateške suradnje i razmjene informacija među državama članicama EU-a u području kibersigurnosti.

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

[14] Europska agencija za mrežnu i informacijsku sigurnost (ENISA), Pregled prijetnji u području 5G mreža: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

To će zauzvrat dovesti do povećanja broja putova napada koje bi mogli iskoristiti akteri prijetnje, posebno akteri iz trećih zemalja ili akteri koji imaju potporu države, zbog svojih kapaciteta (namjera i resursa) za izvođenje napada na telekomunikacijske mreže država članica EU-a, kao i moguće težine posljedica takvih napada.

U tom kontekstu povećane izloženosti napadima kojoj pridonose neovisni dobavljači, profil rizika pojedinačnog dobavljača postaje posebno važan, naročito ako dobavljač ima znatnu prisutnost u mrežama ili područjima.

c) Velika ovisnost o jednom dobavljaču povećava izloženost tom dobavljaču i posljedice njegova mogućeg poslovnog neuspjeha. Pojačavaju se i potencijalne posljedice slabosti i ranjivosti te mogućnost da ih iskoriste akteri prijetnje, posebno ako je mreža ovisna o dobavljaču visokog rizika.

d) Ako se ostvare, neki od zamišljenih novih slučajeva primjene 5G mreža naposljetku će postati važan dio lanca opskrbe mnogih ključnih IT aplikacija. Osim zahtjeva povezanih s povjerljivošću i privatnošću, bitan sigurnosni problem na nacionalnoj razini i iz perspektive EU-a postat će i integritet i dostupnost tih mreža.

Izvor: Usklađena procjena rizika na razini EU-a

U izvješću o usklađenoj procjeni rizika na razini EU-a zaključuje se nadalje da ti izazovi stvaraju novu sigurnosnu paradigmu, zbog čega je potrebno ponovno procijeniti aktualni politički i sigurnosni okvir za sektor tehnologije 5G i njegov ekosustav, a države članice trebale bi poduzeti potrebne mjere za smanjivanje rizika.

Potreban je sveobuhvatan pristup za učinkovito uklanjanje utvrđenih rizika i jačanje sigurnosti i otpornosti 5G mreža, što podrazumijeva provedbu skupa ključnih mjera te povezanih popratnih mjera kojima se istodobno mogu ukloniti rizici. Usklađena procjena rizika na razini EU-a pružila je osnovu za utvrđivanje mjera za smanjivanje rizika koje se mogu primijeniti na nacionalnoj i europskoj razini.

U zaključcima Vijeća od 3. prosinca 2019. izražava se podrška rezultatima usklađene procjene rizika i ističe „važnost koordiniranog pristupa i učinkovite provedbe Preporuke kako bi se izbjegla fragmentacija na jedinstvenom tržištu”.[15] U tu svrhu Vijeće je pozvalo države članice, Komisiju i ENISA-u da „poduzmu sve potrebne mjere u okviru svojih nadležnosti kako bi se osiguralo sigurnost i cjelovitost elektroničkih komunikacijskih mreža, posebno mreža 5G, te da nastave jačati koordinirani pristup rješavanju sigurnosnih izazova povezanih s tehnologijama 5G.”

4. Paket instrumenata EU-a za kibersigurnost 5G mreža

[15] Zaključci Vijeća o važnosti mreža 5G za europsko gospodarstvo i potrebi za smanjivanjem sigurnosnih rizika povezanih s mrežama 5G. 3. prosinca 2019., 14517/19: https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

Skupina za suradnju u području mrežne i informacijske sigurnosti objavila je 29. siječnja 2020. paket instrumenata EU-a za smanjivanje rizika[16]. Paket obuhvaća sve rizike utvrđene u usklađenom izvješću o procjeni rizika.

U paketu instrumenata EU-a utvrđuje se i opisuje skup strateških i tehničkih mjera, kao i odgovarajuće mjere potpore za jačanje njihove učinkovitosti, koje se mogu uspostaviti radi smanjenja utvrđenih rizika. **Strateške mjere** obuhvaćaju mjere za povećanje regulatornih ovlasti nadležnih tijela u nadzoru nabave i uvođenja mreže, posebne mjere za uklanjanje rizika povezanih s netehničkim ranjivostima te moguće inicijative za promicanje održivog i raznovrsnog lanca opskrbe i vrijednosti 5G tehnologije kako bi se izbjegli sustavni rizici od dugoročne ovisnosti. **Tehničke mjere** uključuju mjere za jačanje sigurnosti 5G mreža i opreme uklanjanjem rizika koji proizlaze iz tehnologija, procesa te ljudskih i fizičkih čimbenika. Osim toga, za svako područje rizika koje je utvrđeno u usklađenoj procjeni rizika na razini EU-a predviđeni su **planovi za smanjenje rizika** na temelju najdjelotvornijih mjera.

U zaključcima paketa instrumenata EU-a, kako je dogovoreno u Skupini za suradnju u području mrežne i informacijske sigurnosti, preporučuje se skup **ključnih mjera** koje trebaju provesti sve države članice i Komisija, na sljedeći način:

Zaključci paketa instrumenata EU-a

U paketu instrumenata EU-a navodi se niz mjera i aktivnosti koje, ako se na odgovarajući način kombiniraju i učinkovito provedu, čine temelj usklađenog pristupa u tom području. S obzirom na širok raspon područja rizika utvrđenih u usklađenoj procjeni rizika na razini EU-a i njihovu raznovrsnost, samo jednom vrstom mjera neće se moći obuhvatiti sva ključna područja rizika – umjesto toga bit će potrebno primijeniti pravilnu kombinaciju skupa mjera.

Preporuke iz ovog paketa instrumenata, koje se temelje na procjeni mogućih planova za smanjenje rizika i utvrđivanju najdjelotvornijih mjera, jesu sljedeće:

1. Sve države članice trebale bi osigurati uspostavu mjera (uključujući ovlasti nacionalnih tijela) za odgovarajući i razmjeran odgovor na utvrđene i buduće rizike, a posebno bi se trebale pobrinuti da, primjenom pristupa koji se temelji na procjeni rizika, imaju mogućnost ograničiti, zabraniti i/ili odrediti posebne zahtjeve ili uvjete za opskrbu, uvođenje i rad 5G mrežne opreme iz sigurnosnih razloga.

Posebno bi trebale:

- *Postrožiti **sigurnosne zahtjeve** za operatore pokretnih mreža (npr. stroge kontrole pristupa, pravila o sigurnom radu i nadzoru, ograničenja vanjskih pružatelja određenih funkcija itd.);*

- *Ocijeniti profil rizičnosti dobavljača; u skladu s tim, **primijeniti odgovarajuća ograničenja za dobavljače koji se smatraju visokorizičnima, uključujući potrebna isključenja kako bi se djelotvorno smanjili rizici, za ključnu infrastrukturu** koja je u usklađenoj procjeni rizika na razini EU-a definirana kao kritična i osjetljiva (npr. funkcije osnovne mreže, funkcije upravljanja mrežom i orkestracije te pristupne mrežne funkcije);*

[16] Kibersigurnost 5G mreža – paket instrumenata EU-a za smanjivanje rizika, 29. siječnja 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

 Pobrinuti se da svaki operator ima odgovarajuću strategiju za više prodavatelja kako bi se ***izbjegla ili ograničila bilo kakva znatna ovisnost*** *o jednom dobavljaču (ili dobavljačima sličnog profila rizičnosti), osigurati odgovarajuću ravnotežu dobavljača na nacionalnoj razini i* ***izbjeći ovisnost o dobavljačima koji se smatraju visokorizičnima****; to podrazumijeva i izbjegavanje svih ovisnosti o jednom dobavljaču te promicanje veće interoperabilnosti opreme.*

2. Doprinos Komisije, zajedno s državama članicama, trebao bi se odnositi na sljedeće:

 Održavanje ***raznovrsnog i održivog 5G lanca opskrbe*** *kako bi se izbjegla dugotrajna ovisnost, među ostalim:*

o potpunim iskorištavanjem postojećih alata i instrumenata EU-a, a osobito provjerom potencijalnih ***izravnih stranih ulaganja*** *povezanih s ključnom infrastrukturom 5G mreža te izbjegavanjem* ***narušavanja*** *tržišta opskrbe za 5G koje proizlazi iz mogućeg dampinga ili subvencija; i*

o daljnjim jačanjem ***kapaciteta EU-a u području 5G tehnologija i tehnologija nakon 5G*** *upotrebom relevantnih programa i financiranja EU-a.*

 Olakšavanje koordinacije među državama članicama u vezi sa ***standardizacijom*** *kako bi se ostvarili posebni sigurnosni ciljevi i razvoj* ***relevantnih certifikacijskih programa na razini EU-a*** *radi promicanja sigurnijih proizvoda i postupaka.*

3. Kako bi se osigurala dugotrajna relevantnost tog usklađenog pristupa, potrebno je proširiti mandat Skupine za suradnju u području sigurnosti mrežnih i informacijskih sustava, kao i suradnju s drugim relevantnim tijelima i subjektima, posebno radi:

 Periodičkog preispitivanja – uz potporu Komisije i ENISA-e – ***nacionalnih procjena rizika i procjene rizika na razini EU-a*** *o sigurnosti 5G mreža i generacija mreža nakon 5G, dodatne razrade i usklađivanja prihvaćene metodologije i prilagodbe razvoju 5G tehnologije;*

 Detaljnog i redovitog ***praćenja i ocjenjivanja provedbe paketa instrumenata*** *na temelju strukturiranih izvješća država članica;*

 Koordinacije i potpore provedbi ***mjera potpore*** *za koje je neophodna suradnja na razini EU-a, posebno u vezi s izradom smjernica i razmjenom najboljih praksi za različite mjere;*

 Potpore daljnjoj koordinaciji na razini EU-a, gdje je to primjereno, posebno kako bi se omogućila daljnja konvergencija ***tehničkih i organizacijskih sigurnosnih zahtjeva za mrežne operatore.***

Izvor: Paket instrumenata EU-a

Zaključci iz paketa instrumenata pokazuju snažnu odlučnost država članica da zajednički odgovore na sigurnosne izazove 5G mreža. To je presudno za sigurnost u državama članicama i za cijeli EU, za nacionalna gospodarstva te za unutarnje tržište EU-a i tehnološku suverenost Europe. Usklađena procjena rizika na razini EU-a i paket instrumenata EU-a upućuju na veliku vrijednost zajedničkog rada u okviru Skupine za suradnju u području mrežne i

informacijske sigurnosti, uz intenzivnu suradnju predstavnika svih država članica, Komisije i ENISA-e.

Paket instrumenata omogućuje zajednički pristup EU-a kibersigurnosti 5G mreža, veću dosljednost na cijelom unutarnjem tržištu primjenom politika i koordinacije na razini EU-a te izvršavanje nadležnosti država članica, posebno u pogledu nacionalne sigurnosti. Mjere i planovi za smanjivanje rizika u paketu omogućuju primjeren, učinkovit i razmjeran odgovor EU-a na zajedničke kibersigurnosne izazove u području 5G mreža.

Komisija pozdravlja objavljivanje paketa instrumenata EU-a za kibersigurnost 5G mreža i u potpunosti podržava sve njegove zaključke.

Komisija poziva države članice i relevantne institucije, agencije i druga tijela Unije da:

i. u skladu s paketom instrumenata EU-a osiguraju brzu provedbu djelotvornih i primjerenih strategija smanjivanja rizika diljem EU-a i

ii. poduzmu sve potrebne daljnje korake kako bi se osigurala koordinacija na razini Unije, među ostalim kontinuiranim radom u okviru Skupine za suradnju u području mrežne i informacijske sigurnosti i uspostavom pouzdanog mehanizma za praćenje provedbe paketa instrumenata EU-a, kako bi se osigurala djelotvornost mjera i neometano funkcioniranje unutarnjeg tržišta.

5. Provedba paketa instrumenata

Za vjerodostojan i uspješan europski pristup sigurnosti 5G mreža presudna je odlučnost država članica da u potpunosti iskoriste paket instrumenata. Iako će države članice o prikladnosti pojedinih mjera odlučivati s obzirom na nacionalne okolnosti, kako bi se uklonili utvrđeni rizici apsolutno je neophodno da svaka od njih uspostavi **skup ključnih mjera koje je preporučila Skupina za suradnju u području mrežne i informacijske sigurnosti (vidjeti prethodno navedene zaključke o paketu instrumenata), dok je neke mjere potrebno uspostaviti na razini EU-a**.

Komisija im je spremna nastaviti pružati punu potporu u sljedećim fazama te države članice poziva da:

– **do 30. travnja 2020.** poduzmu konkretne i mjerljive korake kako bi provele skup ključnih mjera preporučenih u zaključcima iz paketa instrumenata EU-a;

– **do 30. lipnja 2020.** u okviru Skupine za suradnju u području mrežne i informacijske sigurnosti izrade izvješće o stanju provedbe tih ključnih mjera u svakoj državi članici na temelju redovitog izvješćivanja i praćenja koje se provodi, osobito u okviru te skupine, uz potporu Komisije i ENISA-e.

5.1. Usklađeni pristup za dobavljače 5G tehnologije koji se temelji na procjeni rizika

S obzirom na krajnji cilj, a to je sigurnost, otpornost i održivost 5G mreža, države članice složile su se da je za ključnu infrastrukturu potrebno procijeniti profil rizika pojedinačnih dobavljača te na temelju toga primijeniti odgovarajuća ograničenja za dobavljače koji se smatraju visokorizičnima, uključujući potrebna isključenja radi djelotvornog smanjenja rizika,

kako je navedeno u paketu instrumenata. Komisija je spremna podržati države članice u provedbi tih mjera.

Za potrebe potpore provedbi tih mjera diljem EU-a, u usklađenoj procjeni rizika na razini EU-a i paketu instrumenata pružaju se smjernice za 1. procjenu profila rizika dobavljača[17] i 2. osjetljivost mrežnih elemenata i funkcija[18], kao i druge infrastrukture. Mjere iz usklađene procjene rizika i iz paketa instrumenata pokrivaju rizike povezane s dobavljačima opreme i usluga za 5G mreže. One se ne odnose na druge proizvode ili usluge koje ti ili drugi dobavljači mogu pružati.

Kako je definirano u točki 2.37. usklađene procjene rizika na razini EU-a, profil rizika pojedinačnih dobavljača može se procijeniti na temelju nekoliko čimbenika.

Procjena profila rizika dobavljača trebala bi se provoditi isključivo iz razloga sigurnosti i na temelju objektivnih kriterija. Kako bi se olakšao koordinirani pristup provedbi tih mjera, u paketu se preporučuje da države članice razmjenjuju informacije o nacionalnim pristupima i najboljim praksama. Nadalje, Komisija smatra da bi te aktivnosti trebale biti jedan od prvih prioriteta sljedeće faze rada u okviru Skupine za suradnju u području mrežne i informacijske sigurnosti, u suradnji s Komisijom i ENISA-om.

Važno je da se ograničenja za dobavljače koji se smatraju visokorizičnima, uključujući potrebna isključenja radi djelotvornog smanjenja rizika, te mjere za izbjegavanje ovisnosti o tim dobavljačima pravovremeno provedu. Ako se to ostvari u najranijoj fazi, uključujući po mogućnosti kada je riječ o postupcima izdavanja dozvola za 5G frekvencije, tržišnim operatorima pružit će se veća predvidivost, čime će se pridonijeti brzom uvođenju 5G mreža, njihovoj dugoročnoj sigurnosti i otpornost njihova opskrbnog lanca.

Istovremeno se za provedbu tih mjera na nacionalnoj razini mogu odrediti različiti vremenski okviri, ako je to potrebno i opravdano, posebno ako postoji visoka razina oslanjanja na opremu ili usluge dobavljača koji su ocijenjeni kao visokorizični (npr. uzimajući u obzir cikluse nadogradnje opreme, posebno prelazak s „nesamostalnih" na „samostalne" 5G mreže). Države članice mogle bi pri utvrđivanju provedbenih planova razmotriti uvođenje odgovarajućih prijelaznih razdoblja za predmetne mrežne operatore. U tom kontekstu prijelazna razdoblja trebalo bi utvrditi tako da se zadrže ili čak ojačaju poticaji za ulaganje u modernu mrežnu opremu, uključujući ubrzano uvođenje potpunih („samostalnih") osnovnih 5G mreža i zamjenu postojeće 4G opreme u drugim dijelovima mreže (npr. u radijskoj pristupnoj mreži), u skladu s ciljevima akcijskog plana za 5G[19].

Osim toga, zbog složenosti 5G mreža, koje se temelje na softveru, telekomunikacijski operatori mogu se sve više oslanjati na nepovezane subjekte za obavljanje određenih zadaća, kao što su održavanje i modernizacija 5G mreža i softvera, te druge eksternalizirane usluge, uz pružanje mrežne opreme. Kao što je opisano u usklađenoj procjeni rizika na razini EU-a, to je izvor ozbiljnog sigurnosnog rizika. Stoga tom aspektu treba posvetiti posebnu pozornost. Neophodno je provesti i temeljitu sigurnosnu procjenu profila rizika dobavljača zaduženih za

[17] Točka 2.37. usklađene procjene rizika na razini EU-a

[18] U točki 2.21. usklađene procjene rizika na razini EU-a predstavljene su glavne kategorije elemenata i funkcija te njihova ukupna razina osjetljivosti, uz popis ključnih elemenata koje su države članice utvrdile za svaku od tih kategorija, dok se u točkama 2.28. i 2.29. navode druge vrste osjetljive infrastrukture odnosno osjetljivih područja (npr. posebni subjekti ili geografska područja).

[19] COM(2016) 588 od 14. rujna 2016., 5G za Europu – Akcijski plan.

pružanje tih usluga, posebno ako se te zadaće ne obavljaju u EU-u. Kako bi se očuvao dugoročni integritet 5G infrastrukture, potrebno je poduzeti odgovarajuće mjere u skladu s mjerama iz paketa instrumenata za smanjenje rizika, uključujući primjenu ograničenja posebno u osjetljivim dijelovima 5G mreža odnosno potrebna isključenja visokorizičnih subjekata.

5.2. Potporna uloga Komisije u provedbi paketa instrumenata

Komisija će i dalje podupirati provedbu pristupa EU-a u području kibersigurnosti 5G tehnologije općenito, te poduzimati konkretne inicijative povezane s mjerama i ciljevima paketa instrumenata u kojima može ostvariti dodanu vrijednost. Komisija će u potpunosti iskoristiti svoje nadležnosti i relevantne instrumente, u mjeri u kojoj je to potrebno za rješavanje utvrđenih pitanja sigurnosti. Na taj način i djelujući u suradnji s državama članicama i privatnim sektorom, Komisija nastoji poduprijeti strateške mjere kojima će se pridonijeti osiguranju tehnološke suverenosti i vodstva EU-a u budućem razvoju mrežnih tehnologija, tehnologija kibersigurnosti i svih relevantnih sastavnica o kojima ovisi naše cjelokupno gospodarstvo i sigurnost.

Konkretnije, Komisija će u područjima za koja je nadležna poduzeti sljedeće kako bi osigurala provedbu odgovarajućih mjera za smanjenje rizika iz paketa instrumenata:

Očuvanje kibersigurnosti 5G mreža i raznolikosti vrijednosnog lanca 5G tehnologije:

– **suradnja u području kibersigurnosti**: nastaviti pružati potporu državama članicama radi učinkovite, koordinirane i pravodobne provedbe nacionalnih mjera u okviru Skupine za suradnju u području mrežne i informacijske sigurnosti

– **propisi o telekomunikacijama i kibersigurnosti**: pružiti potporu provedbi mjera iz paketa instrumenata koje se odnose na sigurnosne zahtjeve, posebno relevantnih odredbi europskih propisa o elektroničkim komunikacijama, i razmotriti dodanu vrijednost mogućih provedbenih akata kojima se uređuju pojedinosti o tehničkim i organizacijskim sigurnosnim mjerama kako bi se upotpunili nacionalni propisi i povećala učinkovitost i dosljednost sigurnosnih mjera kojim podliježu operatori

– **standardizacija**: poduzeti mjere za održavanje i, prema potrebi, povećanje europskog sudjelovanja u odgovarajućim tijelima za standardizaciju kako bi se ostvarili europski ciljevi u pogledu sigurnosti i interoperabilnosti. Konkretnije, Komisija će s državama članicama ocjenjivati i promicati tehničke specifikacije i standarde kojima se omogućuje interoperabilnost dobavljača 5G opreme u različitim dijelovima mreže, uključujući u naslijeđenim mrežama, kako bi se omogućilo istinsko okruženje s više prodavatelja, na primjer putem otvorenih, interoperabilnih sučelja

– **certifikacija**: podupirati razvoj programa za certifikaciju 5G tehnologije kojima će se nastojati odgovoriti na potrebe 5G mreža u okviru EU-ova okvira za kibersigurnosnu certifikaciju

– **provjera izravnih stranih ulaganja**: podupirati provedbu okvira EU-a za provjeru izravnih stranih ulaganja izradom pregleda vrijednosnog lanca 5G tehnologije, uključujući osjetljivu mrežnu infrastrukturu, i redovitim praćenjem izravnih stranih ulaganja u cijelom vrijednosnom lancu. U skladu s vremenskim okvirom za provjeru izravnih stranih ulaganja (od listopada 2020.) Komisija će pomno pratiti strana ulaganja u području 5G tehnologije u

skladu sa smjernicama iz Uredbe EU 2019/452, uzimajući u obzir usklađenu procjenu rizika na razini EU-a i paket instrumenata EU-a

– **instrumenti trgovinske zaštite**: pratiti sva relevantna tržišna kretanja u EU-u i trećim zemljama te primjenom mjera trgovinske zaštite štititi aktere EU-a na europskom tržištu 5G tehnologije od moguće prakse kojom se narušava trgovina (damping ili subvencioniranje), uključujući po potrebi pokretanjem preliminarnih istraga

– pravila tržišnog natjecanja: nadzirati funkcioniranje tržišta ponude hardvera i softvera za 5G kako bi se osigurali konkurentni ishodi, uključujući u odnosu na moguće situacije ovisnosti o jednom dobavljaču zbog ugovornih obveza ili tehničkih razloga

– **programi financiranja EU-a**: osigurati da sudjelovanje u programima financiranja EU-a u relevantnim tehnološkim područjima bude uvjetovano ispunjavanjem sigurnosnih zahtjeva, i to potpunim iskorištavanjem i daljnjom provedbom sigurnosnih uvjeta u programima istraživanja i razvoja, posebno u programima Obzor Europa i Digitalna Europa, Instrumentu za povezivanje Europe 2, europskim strukturnim i investicijskim fondovima i drugim relevantnim programima. Sličan pristup trebalo bi primijeniti i u vanjskim programima financiranja i financijskim instrumentima EU-a, uključujući financiranje putem međunarodnih financijskih institucija

– javna nabava: potaknuti javnu nabavu u području 5G mreža kako bi se poduprli utvrđeni ciljevi njihove sigurnosti, raznolikosti dobavljača i dugoročne održivosti, a posebno nastojati osigurati da se sigurnosni aspekti obvezno uzmu u obzir pri dodjeli ugovora o javnoj nabavi u području 5G mreža, u skladu s pravilima EU-a o javnoj nabavi

– **okvir za odgovor na incidente i upravljanje krizama (plan) te vježbe za provjeru kibersigurnosti**: u potpunosti iskoristiti plan EU-a[20] za koordinirani odgovor na kiberincidente velikih razmjera. Osim toga, u suradnji s ENISA-om razmotriti mogućnost provedbe vježbe za provjeru kibersigurnosti 5G mreža čim tržište za to bude spremno.

Usto, u nadležnosti Vijeća i Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku i potpredsjednika Komisije:

– **okvir za zajednički diplomatski odgovor EU-a na zlonamjerne kiberaktivnosti (instrument za kiberdiplomaciju)[21]**: u slučaju zlonamjernih kiberaktivnosti koje ugrožavaju integritet i sigurnost EU-a, države članice potiču se da upotrebljavaju relevantne mjere zajedničke vanjske i sigurnosne politike koje su dio instrumenta EU-a za kiberdiplomaciju (uključujući, prema potrebi, mjere ograničavanja) kako bi se potaknula suradnja, omogućilo smanjenje prijetnji i utjecalo na ponašanje potencijalnih napadača.

Nadalje, nizom programa pridonijet će se ciljevima izbjegavanja ili ograničavanja rizika od dugoročne ovisnosti, i to promicanjem raznolikog i održivog tržišta 5G tehnologije u skladu s međunarodnim obvezama EU-a, među ostalim zadržavanjem kapaciteta EU-a u vrijednosnom lancu 5G tehnologije i ulaganjem u inovacije.

[20] Preporuka Komisije o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (EU 2017/1584).
[21] Zaključci Vijeća od 20. studenoga 2017., 9916/17.

Promicanje inovacija i ulaganja u kibersigurnost i tehnologije mrežne infrastrukture:

– **programi financiranja EU-a**: povećati ulaganja u istraživanje, inovacije i uvođenje mrežnih tehnologija i njihovih relevantnih temeljnih sastavnica. Komisija je u sljedećem proračunskom okviru EU-a za razdoblje 2021.–2027. predložila ulaganja u kibersigurnosne tehnologije u iznosu od gotovo 3 milijarde EUR. To uključuje istraživanje i inovacije u okviru programa Obzor Europa te potporu kibersigurnosnim kapacitetima u okviru programa Digitalna Europa. Iz programa InvestEU može se osigurati i financijska potpora za istraživanje, razvoj i uvođenje 5G tehnologije.

Nadalje, u okviru sljedećeg programa Obzor Europa[22] Komisija je predložila uspostavu institucionaliziranog partnerstva EU-a za internet sljedeće generacije i 6G (NGI/6G, „pametne mreže i usluge") s industrijom i koordinaciju s državama članicama kako bi se dovršilo uvođenje 5G mreža i prvenstveno **kao priprema za 6G**, tj. sljedeću generaciju mobilne tehnologije. Iz proračuna EU-a (2021.–2027.) predložena su ulaganja u vrijednosti većoj od 2,5 milijarde EUR, uz najmanje 7,5 milijardi EUR privatnih ulaganja u tu inicijativu.

– industrijski razvoj i uvođenje: procijeniti moguće tržišne nedostatke ili nedostatke u vrijednosnom lancu 5G tehnologije, čime bi se opravdale ciljane intervencije u sljedećem dugoročnom proračunskom okviru ili mogući važni projekt od zajedničkog europskog interesa u području kibersigurnosti, u skladu s prijedlozima foruma na visokoj razini o važnim projektima od zajedničkog europskog interesa. Odluku o osmišljavanju i uspostavi važnih projekata od zajedničkog europskog interesa donose države članice i poduzeća. Propisi EU-a pružaju poticajni okvir, a Komisija je spremna olakšati potrebne kontakte i pružati smjernice.

[22] Financiranje se može osigurati i u okviru Instrumenta za povezivanje Europe (CEF) 2.0 i programa Digitalna Europa.

6. Zaključak

5G mreže trebale bi europskim građanima, društvu i gospodarstvu donijeti niz novih mogućnosti. Stoga je od presudne važnosti osigurati njihovu sigurnost i otpornost. Istodobno, prijetnje kibersigurnosti (uključujući rizik od uplitanja trećih zemalja ili aktera koji imaju potporu države) sve su veći izazov, koji dobiva na važnosti kako se sve više oslanjamo na tehnologiju i podatke. Zanemarivanje kibersigurnosti potkopalo bi povjerenje u razvoj digitalnog gospodarstva i društva, a EU-u onemogućilo da u potpunosti iskoristi njegove prednosti. To zahtijeva odgovarajući prilagođeni i pojačani odgovor.

Usklađen i dosljedan pristup kibersigurnosti u EU-u kada je riječ o ključnim tehnologijama i mrežama nužan je kako bi EU osigurao svoju tehnološku suverenost te zadržao i razvio industrijske kapacitete. Komisija će u potpunosti podupirati provedbu EU-ova pristupa kibersigurnosti 5G mreža i istodobno osigurati da tržišta EU-a ostanu otvorena za proizvode i usluge koji su u skladu sa sve većim zahtjevima u odnosu na kibersigurnost i povjerenje.

Stoga je važno zadržati iznimnu predanost svih dionika kada je riječ o sigurnosti 5G mreža, što će zahtijevati daljnju suradnju država članica, Komisije i ENISA-e.

Komisija poziva države članice da kao neposredni sljedeći korak, žurno, učinkovito i objektivno provedu mjere dogovorene u paketu instrumenata, kako je prethodno navedeno, te da uz potporu Komisije i ENISA-e nastave surađivati u cilju koordinacije na razini EU-a. Komisija će istodobno u područjima u svojoj nadležnosti pokrenuti sve relevantne aktivnosti kako bi pružila potporu provedbi i povećanje učinka paketa instrumenata u državama članicama.

Dodatak Kategorije rizika (Izvor: usklađena procjena rizika na razini EU-a)

	Kategorije rizika
Scenariji rizika povezani s nedovoljnim mjerama sigurnosti	*R1: Pogrešna konfiguracija mreža*
	R2: Nedovoljna kontrola pristupa
Scenariji rizika povezani s lancem opskrbe za 5G tehnologiju	*R3: Niska kvaliteta proizvoda*
	R4: Ovisnost pojedinih mreža o samo jednom dobavljaču ili nedovoljna raznolikost na razini države
Scenariji rizika povezani s načinom rada glavnih aktera koji su izvor prijetnje	*R5: Uplitanje države putem lanca opskrbe za 5G tehnologiju*
	R6: Organizirani kriminal iskorištava 5G mreže ili to čine organizirane kriminalne skupine kojima su meta krajnji korisnici
Scenariji rizika povezani s međuovisnosti 5G mreža i drugih ključnih sustava	*R7: Značajne smetnje u radu ključnih infrastruktura ili usluga*
	R8: Masovni pad mreža zbog prekida opskrbe električnom energijom ili drugih potpornih sustava
Scenariji rizika povezani s uređajima krajnjih korisnika	*R9: Iskorištavanje interneta stvari*