EVROPSKA
KOMISIJA

Bruselj, 29.1.2020
COM(2020) 50 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

Varna uvedba tehnologije 5G v EU - izvajanje nabora orodij EU

1. *Uvod*

Peta generacija (5G) telekomunikacijskih omrežij bo imela pomembno vlogo v razvoju evropske družbe in gospodarstva. Ta omrežja naj bi nudila veliko gospodarskih priložnosti in postala pomembna podlaga za digitalno in zeleno preobrazbo na področjih, kot so promet, energetika, proizvodnja, zdravje, kmetijstvo in mediji.

Zato bi lahko tehnologija 5G vplivala na takorekoč vse vidike življenja državljanov EU. Kibernetska varnost omrežij 5G je zato bistvenega pomena, ne samo za zaščito naših gospodarstev, družb in demokratičnih procesov, ampak tudi za zagotovitev verodostojne digitalne preobrazbe, ki bo koristila vsem državljanom EU.

Zaradi odvisnosti številnih kritičnih storitev od omrežij 5G bi bile posledice sistemskega, obsežnega izpada še posebej hude in bi njihov vpliv lahko presegel nacionalne meje, saj so digitalni ekosistemi medsebojno povezani. Zato je zagotovitev kibernetske varnosti omrežij 5G za Unijo strateškega pomena, saj je kibernetskih napadov vse več, so bolj prefinjeni kot kdaj koli prej in prihajajo od številnih akterjev, ki predstavljajo nevarnost, zlasti držav ali akterjev s podporo držav zunaj EU. Glede varnosti kritičnih infrastruktur, kot je 5G, je bila prvič doslej izbrana opredelitev skupnega evropskega pristopa. Ta pristop v celoti upošteva odprtost notranjega trga EU, dokler so izpolnjene varnostne zahteve EU na podlagi tveganja.

Evropski svet je 22. marca 2019 pozval k usklajenemu pristopu k varnosti omrežij 5G. Komisija je 26. marca 2019 sprejela Priporočilo (EU) 2019/534 o kibernetski varnosti omrežij 5G[1]. V priporočilu je države članice pozvala, da dokončajo nacionalne ocene tveganja, pregledajo nacionalne ukrepe, si na ravni EU skupaj prizadevajo za usklajeno oceno tveganja in pripravijo nabor orodij za zmanjševanje tveganja. To sporočilo je sestavni del Komisijine celovite evropske digitalne strategije, h kateri je pozval Evropski svet.

2. *Uvajanje omrežij 5G v EU*

Uvedba infrastrukture za omrežje 5G v Evropi je ključnega pomena za evropsko industrijsko strategijo in konkurenčnost. Komisija je uvedbo omrežnih tehnologij pete generacije (5G) priznala kot enega najpomembnejših dejavnikov, ki omogoča prihodnje digitalne storitve. Leta 2016 je sprejela Akcijski načrt za 5G, da bi zagotovila, da bo Unija imela infrastrukturo za povezljivost, potrebno za njeno digitalno preobrazbo od leta 2020 naprej ter za celovito uvedbo na mestnih področjih in ob glavnih prometnih poteh do leta 2025[2]. V sporočilu o gigabitni družbi je zastavljen visok cilj, da bi moral biti dostop do mobilne podatkovne povezljivosti na voljo povsod[3], tudi v podeželskih in najbolj oddaljenih območjih.

Kar zadeva dodelitev frekvenc, so države članice dodelile 16 % pionirskih pasov za 5G[4]. Glede na pravno obveznost, da se dovoli uporaba vseh pionirskih pasov 5G do konca leta, se v naslednjih nekaj mesecih pričakujejo posvetovanja za precej postopkov.

[1] Priporočilo (EU) 2019/534 o kibernetski varnosti omrežij 5G, UL L 88, 29.3.2019, str. 42.
[2] COM(2016) 588 z dne 14. junija 2016 z naslovom Akcijski načrt za 5G v Evropi.
[3] COM(2016) 587 z naslovom Povezljivost za konkurenčen enotni digitalni trg – evropski gigabitni družbi naproti.
[4] http://www.5GObservatory.eu.

Kar zadeva komercialno uvajanje storitev 5G, je Evropa med najnaprednejšimi regijami na svetu[5]. Trenutno se pričakuje, da bodo prve storitve 5G do konca leta 2020 na voljo v 138 evropskih mestih. Zgodnja omrežja 5G izhajajo iz sedanje četrte generacije (4G) omrežnih tehnologij, storitve 5G pa se v glavnem opravljajo za širšo javnost kot izboljšava tehnologije 4G glede zmogljivosti in hitrosti ali kot stroškovno učinkovita alternativa fiksnim omrežjem[6].

Pri priložnostih za nove storitve med podjetji, npr. v sektorjih energetike, hrane in kmetijstva, zdravstva, proizvodnje ali prometa, je Evropa zelo napredovala z naložbami v višini milijarde eurov, vključno s 300 milijoni eurov sredstev EU v okviru javno-zasebnega partnerstva za 5G v programu Obzorje 2020. Ta naložba zajema več kot 160 preizkusov tehnologije 5G v velikem obsegu, določenih v Evropi, med njimi deset čezmejnih avtocestnih koridorjev za preizkušanje storitev povezane in avtomatizirane mobilnosti na podlagi tehnologije 5G v velikem obsegu. Preizkusi zajemajo aplikacije, ki lahko uporabljajo tehnologijo 5G, na področjih od trajnostnega zdravstva, avtomatizirane mobilnosti in kmetijstva, gospodarnega z viri, do pametnih električnih omrežij in industrije 4.0. Poleg tega je EIB ob podpori Evropskega sklada za strateške naložbe dala na voljo posojila za pospešitev raziskav in razvoja tehnologije 5G.

Evropski zakonik o elektronskih komunikacijah (v nadaljnjem besedilu: Zakonik)[7], ki se bo uporabljal od 21. decembra 2020, je pomembna podlaga za ustvarjanje naložbam prijaznega okolja za omrežja 5G in omrežja, ki jih bodo nasledila. Bistvenega pomena za podporo prihodnji uvedbi omrežij 5G, zlasti s priključevanjem skupnosti na storitve, ki lahko uporabljajo tehnologijo 5G, kot so šole, bolnišnice, mesta in lokalne uprave, bodo tudi programi financiranja z javnimi sredstvi, kot so instrument za povezovanje Evrope – digitalno[8] ali evropski strukturni in investicijski skladi.

Glede na strateške priložnosti Evrope pri storitvah 5G v različnih panogah bo ključnega pomena, da operaterji in ponudniki storitev vlagajo v napredne rešitve na področju omrežja in storitev 5G. Zanje ne bodo potrebna samo nova radijska omrežja 5G, ampak tudi nova t. i. „samostojna“ jedrna omrežja 5G, da bi zagotavljala napredne funkcije 5G, kot je omrežno rezinjenje[9] in računalništvo na robu[10].

Komisija bo še naprej v celoti podpirala uspešno uvajanje tehnologije 5G v EU, tudi s spodbujanjem držav članic in zainteresiranih strani, da izkoristijo priložnosti, ki jih nudi

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

[6] Nekatere nove funkcije 5G bodo uvedene postopoma. V prvi fazi (zelo kratkoročno ali kratkoročno) bo uvedba 5G sestavljena predvsem iz „nesamostojnih“ omrežij, pri katerih bo na raven tehnologije 5G nadgrajeno zgolj radijsko dostopovno omrežje, sicer pa bodo še vedno temeljila na obstoječih jedrnih omrežjih 4G, kar bo končnim uporabnikom zagotavljalo izboljšano zmogljivost mobilnega širokopasovnega omrežja. V naslednjih fazah (kratkoročno/srednjeročno do dolgoročno) bo za uvedbo „samostojnih“ omrežij 5G vključno s funkcijami 5G jedrnega omrežja sčasoma potrebna veliko obsežnejša sprememba omrežne arhitekture.

[7] Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta o Evropskem zakoniku o elektronskih komunikacijah (prenovitev).

[8] Predlog uredbe COM(2018) 438 z dne 6. junija 2018 o vzpostavitvi instrumenta za povezovanje Evrope ter razveljavitvi uredb (EU) št. 1316/2013 in (EU) št. 283/2014.

[9] Omrežno rezinjenje 5G omogoča visoko stopnjo ločevanja med različnimi storitvenimi nivoji v istem fizičnem omrežju in tako daje več možnosti za ponudbo diferenciranih storitev v celotnem omrežju.

[10] Računalništvo na robu je paradigma porazdeljenega računalništva, ki računalniške operacije in shranjevanje podatkov približuje kraju, na katerem je potrebno, s čimer izboljšuje odzivni čas in omogoča prihranek pasovne širine.

tehnologija 5G. Upoštevani bodo ustrezni zdravstveni vidiki na podlagi previdnostnega načela[11] v sodelovanju z ustreznimi mednarodnimi organizacijami in znanstveno skupnostjo.

3. Usklajena ocena tveganja za kibernetsko varnost v omrežjih 5G v EU

V skupinskem sodelovanju v okviru skupine za sodelovanje na področju varnosti omrežij in informacij[12] je vsaka država članica do začetka julija 2019 izdelala svojo nacionalno oceno tveganja svojih infrastruktur za omrežje 5G ter rezultate poslala Komisiji in Agenciji Evropske unije za kibernetsko varnost (agencija ENISA).

Na podlagi teh nacionalnih ocen tveganja so skupina za sodelovanje na področju varnosti omrežij in informacij, ki jo sestavljajo predstavniki držav članic, Komisija in agencija ENISA 9. oktobra 2019 objavile poročilo o usklajeni oceni tveganja za kibernetsko varnost v omrežjih 5G v EU[13]. V poročilu so navedene glavne grožnje in akterji, ki predstavljajo nevarnost, najobčutljivejša sredstva in glavne šibke točke (tako tehnične kot druge vrste šibkih točk), ki zadevajo omrežja 5G. Na podlagi tega je v poročilu navedenih več strateško pomembnih kategorij tveganja z vidika EU; te kategorije so ponazorjene s konkretnimi scenariji tveganja, ki odražajo ustrezne kombinacije različnih parametrov (šibke točke, grožnje in akterji, ki predstavljajo grožnjo) glede na različna sredstva (glej Dodatek).

ENISA je kot dopolnilo tega poročila in dodaten prispevek k naboru orodij opravila podrobno kartiranje groženj[14], sestavljeno iz podrobne analize nekaterih tehničnih vidikov, predvsem določitve omrežnih sredstev in groženj, ki vplivajo nanje.

V usklajeni oceni tveganja v EU je poudarjenih več vidikov pomembnosti omrežij 5G. Natančneje:

a) S tehnološkimi spremembami, ki jih uvajajo omrežja 5G, se bosta povečala splošna napadna površina in število možnih vstopnih točk za napadalce:

– razširjene funkcije na robu omrežja in arhitektura mobilnih omrežij, ki je manj centralizirana od prejšnjih generacij, pomeni, da je mogoče nekatere funkcije jedrnih omrežij vključiti v druge dele omrežij, zaradi česar je zadevna oprema občutljivejša (npr. bazne postaje ali funkcije upravljanja in orkestracije omrežja);

– pomembnejša vloga programske opreme v opremi za 5G prinaša večja tveganja v zvezi s postopki razvoja in posodabljanja programske opreme in nova tveganja napak pri konfiguraciji, s tem pa daje pomembnejšo vlogo varnostni analizi odločitev vsakega mobilnega operaterja v fazi razvoja omrežja.

[11] Priporočilo Sveta z dne 12. julija 1999 o omejevanju izpostavljenosti javnosti elektromagnetnim poljem (0 Hz do 300 GHz) (1999/519/ES).

[12] Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (direktiva o varnosti omrežij in informacij). Skupina za sodelovanje na področju varnosti omrežij in informacij je bila ustanovljena z direktivo o varnosti omrežij in informacij za zagotovitev strateškega sodelovanja in izmenjave informacij na področju kibernetske varnosti med državami članicami EU.

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

[14] Poročilo agencije ENISA o naravi groženj (ENISA Threat landscape for 5G networks): https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

b) Zaradi teh novih tehnoloških lastnosti bo za omrežne operaterje mobilne telefonije vse pomembnejša odvisnost od tretjih dobaviteljev in njihova vloga v dobavni verigi tehnologije 5G.

Zato se bo povečalo število napadnih poti, ki bi jih lahko izkoristili akterji, ki predstavljajo nevarnost, zlasti države ali akterji s podporo držav zunaj EU, saj imajo zmogljivosti (tako namen kot vire) za napade na telekomunikacijska omrežja držav članic EU, pa tudi učinek takih napadov bi lahko bil hujši.

Glede na večjo izpostavljenost napadom, ki je še večja zaradi tretjih dobaviteljev, bo postal posebno pomemben individualni profil tveganja dobaviteljev, zlasti če je kakšen dobavitelj močno prisoten v omrežjih ali na območjih.

c) Velika odvisnost od enega samega dobavitelja pomeni večjo izpostavljenost zaradi morebitnega stečaja tega dobavitelja in hujše posledice takega stečaja. Zaradi tega bi bile hujše tudi morebitne posledice slabosti ali šibkih točk in njihovega morebitnega izkoriščanja s strani akterjev, ki predstavljajo nevarnost, zlasti kadar gre za odvisnost od dobavitelja z visoko stopnjo tveganja.

d) Če se bodo uresničili nekateri primeri nove uporabe, predvidene za tehnologijo 5G, bodo omrežja 5G postala pomemben del dobavne verige številnih kritičnih aplikacij IT, to pa ne bo le vplivalo na zahteve za zaupnost in zasebnost, temveč bosta nedotaknjenost in razpoložljivost teh omrežij postala pomembni vprašanji nacionalne varnosti in velik varnostni izziv z vidika EU.

Vir: Usklajena ocena tveganja v EU.

V usklajeni oceni tveganja v EU se nadalje ugotavlja, da ti izzivi ustvarjajo novo varnostno paradigmo, saj je treba zaradi njih ponovno oceniti sedanjo politiko in varnostni okvir, ki se uporablja za sektor 5G in njegov ekosistem, države članice pa morajo nujno sprejeti ustrezne ukrepe za zmanjšanje tveganja.

Za učinkovito zmanjšanje ugotovljenih tveganj ter krepitev varnosti in odpornosti omrežij 5G je potreben celosten pristop, v katerem je treba vzpostaviti niz ključnih ukrepov ter z njimi povezanih podpornih dejavnosti, s katerimi je mogoče hkratno zmanjševanje tveganj. Usklajena ocena tveganja v EU je podlaga za določitev ukrepov za zmanjšanje tveganja, ki jih je mogoče uporabiti na nacionalni in evropski ravni.

V sklepih Sveta z dne 3. decembra 2019 je bila dana podpora ugotovitvam usklajene ocene tveganja in poudarjen „pomen usklajenega pristopa in učinkovitega izvajanja priporočila, da bi se izognili razdrobljenosti enotnega trga“[15]. Zato je Svet pozval države članice, Komisijo in agencijo ENISA, da sprejmeta vse potrebne ukrepe v okviru njunih pristojnosti za zagotovitev varnosti in celovitosti elektronskih komunikacijskih omrežij, predvsem omrežij 5G, in še naprej utrjujeta usklajen pristop za reševanje varnostnih izzivov, povezanih s tehnologijami 5G.

[15] Sklepi Sveta o pomenu omrežij 5G za evropsko gospodarstvo in dejstvu, da je treba zmanjšati varnostna tveganja, povezana z njimi. 3. december 2019, 14517/19 https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52019XG1210(02)&qid=1580220142360.

4. Nabor orodij EU za kibernetsko varnost tehnologije 5G

Skupina za sodelovanje na področju varnosti omrežij in informacij je 29. januarja 2020 objavila nabor orodij za zmanjševanje tveganja[16]. V njem so obravnavana vsa tveganja, ugotovljena v poročilu o usklajeni oceni tveganja.

Nabor orodij EU določa in opisuje niz strateških in tehničnih ukrepov ter ustrezne podporne dejavnosti za krepitev njihove učinkovitosti, ki bi jih bilo mogoče uvesti za zmanjšanje ugotovljenih tveganj. **Strateški ukrepi** zajemajo ukrepe, ki zadevajo krepitev regulativnih pooblastil organov, da lahko podrobno pregledajo nabavo in uvedbo omrežja, posebne ukrepe za reševanje tveganj v zvezi z netehničnimi šibkimi točkami ter možne pobude za spodbujanje trajnostne in raznolike dobavne in vrednostne verige tehnologije 5G, da bi se izognili sistemskim tveganjem dolgoročne odvisnosti. **Tehnični ukrepi** zajemajo ukrepe za krepitev varnosti omrežij in opreme 5G z zmanjševanjem tveganj, ki izhajajo iz tehnologije, postopkov ter človeških in fizičnih dejavnikov. Poleg tega so v njem za vsako področje tveganja, ugotovljeno v usklajeni oceni tveganja EU, podani **načrti za zmanjšanje tveganja**, ki temeljijo na najučinkovitejših ukrepih.

Med njimi se v sklepnih ugotovitvah v naboru orodij EU, o katerem se je dogovorila skupina za sodelovanje na področju varnosti omrežij in informacij, priporoča niz **ključnih ukrepov**, ki bi jih izvedle vse države članice in Komisija, in sicer:

Sklepne ugotovitve v naboru orodij EU

V naboru orodij EU so določeni številni ukrepi, ki (v ustrezni kombinaciji in ob učinkovitem izvajanju) dajejo podlago za usklajen pristop na tem področju. Glede na širok razpon območij tveganja, ugotovljenih v usklajeni oceni tveganja v EU, in njihovo različno naravo namreč ne bo zadostoval noben posamezen ukrep, temveč bo za obravnavo vseh ključnih območij tveganja potrebna vrsta ukrepov v primerni kombinaciji.

Na podlagi ocene možnih načrtov za zmanjšanje tveganja in določitve najučinkovitejših ukrepov se v tem naboru orodij priporoča:

1. Vse države članice bi morale zagotoviti uvedbo ukrepov (vključno s pooblastili za nacionalne organe) za ustrezen in sorazmeren odziv na trenutno ugotovljena in prihodnja tveganja, zlasti pa bi morale zagotoviti, da so sposobne po pristopu na podlagi tveganja omejiti, prepovedati in/ali naložiti posebne zahteve ali pogoje za dobavo, uvedbo in delovanje opreme za omrežje 5G na podlagi vrste razlogov v zvezi z varnostjo.

Morale bi zlasti:

- *okrepiti **varnostne zahteve** za omrežne operaterje mobilne telefonije (npr. strog nadzor nad pristopom, pravila za varno delovanje in spremljanje, omejitve zunanjega izvajanja določenih funkcij itd.);*

- *oceniti profil tveganja in na podlagi tega **uporabiti ustrezne omejitve za dobavitelje, ki se štejejo za visoko tvegane, za ključna sredstva,** opredeljena v usklajeni oceni tveganja v EU kot kritična in občutljiva (npr. funkcije jedrnega omrežja, funkcije upravljanja in orkestracije omrežja ter funkcije dostopovnega omrežja), tudi potrebne izključitve za učinkovito zmanjšanje tveganja;*

[16] Kibernetska varnost omrežij 5G – nabor orodij EU za zmanjševanje tveganja, 29 januar 2020 (https://ec.europa.eu/digital-single-market/en/nis-cooperation-group).

 zagotoviti, da bo imel vsak operater ustrezno večdobaviteljsko strategijo, da se bo ***izognil preveliki odvisnosti*** *od enega samega dobavitelja (ali dobaviteljev s podobnim profilom tveganja), zagotovil primerno ravnotežje dobaviteljev na nacionalni ravni in* ***preprečil odvisnost od dobaviteljev, ki se štejejo za visoko tvegane****; iz tega razloga se je treba izogibati tudi primerom izključne vezanosti na enega samega ponudnika, tudi s spodbujanem večje interoperabilnosti opreme.*

2. Evropska komisija bi morala skupaj z državami članicami prispevati:

 k vzdrževanju ***raznolike in trajnostne dobavne verige 5G****, da bi preprečile dolgoročno odvisnost, med drugim tudi:*

o tako, da bodo v celoti izkoristile obstoječa orodja in instrumente EU, zlasti s pregledom možnih ***neposrednih tujih naložb****, ki bi vplivale na ključna sredstva 5G, in s preprečevanjem* ***izkrivljanja*** *dobavnega trga tehnologije 5G zaradi možnega dumpinga ali subvencioniranja, ter*

o tako, da se bodo z uporabo ustreznih programov in sredstev EU še naprej krepile ***zmogljivosti EU na področju tehnologij 5G in tehnologij naslednic 5G****;*

 tako, da bodo z omogočanjem boljšega usklajevanja med državami članicami glede ***standardizacije****, da bi dosegle določene varnostne cilje in razvile* ***ustrezne certifikacijske sheme za vso EU*** *ter tako spodbujale nastanek varnejših proizvodov in procesov.*

3. Da bi se ta usklajeni pristop lahko uveljavil, bi bilo treba podaljšati mandat za namensko delovno telo skupine za sodelovanje na področju varnosti omrežij in informacij ter sodelovanje z drugimi ustreznimi organi in subjekti, zlasti da bi:

 ob podpori Komisije in agencije ENISA občasno pregledovalo ***nacionalne ocene tveganja in ocene tveganja v EU*** *glede varnosti omrežij 5G in omrežij, ki bodo nasledila 5G, še naprej izpopolnjevalo in usklajevalo ocenjevalno metodologijo ter jo prilagajalo razvoju tehnologije 5G;*

 podrobno in redno ***spremljalo in ocenjevalo izvajanje*** *nabora orodij na podlagi strukturiranih poročil držav članic;*

 usklajevalo in podpiralo izvajanje ***podpornih dejavnosti****, za katere je potrebno sodelovanje na ravni EU, zlasti glede izpopolnjevanja navodil in izmenjave dobrih praks glede raznih ukrepov;*

 kjer je ustrezno, podpiralo možno nadaljnje sodelovanje na ravni EU, zlasti da bi dosegla še nadaljnje približevanje ***v zvezi s tehničnimi in organizacijskimi varnostnimi zahtevami za omrežne operaterje****.*

Vir: Nabor orodij EU.

Kot je razvidno iz sklepnih ugotovitev v naboru orodij, so države članice trdno odločene, da se bodo skupaj odzivale na varnostne izzive za omrežja 5G. To je temeljnega pomena za varnost v državah članicah in v celotni EU, pa tudi za nacionalna gospodarstva, notranji trg EU in tehnološko suverenost Evrope. Tako usklajena ocena tveganja EU kot nabor orodij EU kažeta, kako dragoceno delo je bilo opravljeno v skupini za sodelovanje na področju varnosti omrežij in informacij ob tesnem sodelovanju predstavnikov vseh držav članic, Komisije in agencije ENISA.

Nabor orodij omogoča skupen pristop EU h kibernetski varnosti na področju 5G, saj podpira usklajenost na celotnem notranjem trgu s pomočjo politik in usklajevanja na ravni EU ter izvajanja pristojnosti držav članic zlasti glede nacionalne varnosti. Ukrepi in načrti za

zmanjšanje tveganja, ki jih vsebuje, omogočajo primeren, učinkovit in sorazmeren odziv EU na skupne izzive kibernetske varnosti tehnologije 5G.

Komisija pozdravlja objavo nabora orodij EU za kibernetsko varnost tehnologije 5G in v celoti podpira vse navedene sklepne ugotovitve.

Komisija poziva države članice in ustrezne institucije, agencije in druge organe Unije, da:

(i) zagotovijo hitro izvajanje učinkovitih in primernih strategij za zmanjševanje tveganja v skladu z naborom orodij EU in

(ii) sprejmejo vse potrebne nadaljnje ukrepe za zagotovitev usklajevanja na ravni Unije, tudi z nadaljevanjem dela v skupini za sodelovanje na področju varnosti omrežij in informacij, in vzpostavijo trden mehanizem za spremljanje izvajanja nabora orodij EU, da bi zagotovile učinkovitost ukrepov in nemoteno delovanje notranjega trga.

5. Izvajanje nabora orodij

Odločenost držav članic, da v celoti izkoristijo nabor orodij, je bistvenega pomena za verodostojen in uspešen pristop EU k varnosti tehnologije 5G. O primernosti posameznih ukrepov bodo sicer odločale države članice na podlagi nacionalnih razmer, vendar je nujno, da se **niz ključnih ukrepov, ki jih priporoča skupina za sodelovanje na področju varnosti omrežij in informacij (gl. navedene sklepne ugotovitve iz nabora orodij), uvede v vsaki državi članici, nekateri ukrepi pa na ravni EU**, da bi bilo mogoče zmanjšati ugotovljena tveganja.

Komisija je pripravljena še naprej nuditi celotno podporo v naslednjih fazah in države članice poziva:

– da **do 30. aprila 2020** sprejmejo oprijemljive in merljive ukrepe za izvajanje vrste ključnih ukrepov, priporočenih v sklepnih ugotovitvah nabora orodij EU;

– da **do 30. junija 2020** pripravijo poročilo skupine za sodelovanje na področju varnosti omrežij in informacij o izvajanju teh ključnih ukrepov v vsaki državi članici, in sicer na podlagi rednega poročanja in spremljanja zlasti v skupini za sodelovanje na področju varnosti omrežij in informacij ob podpori Komisije in agencije ENISA.

5.1 Usklajen pristop do dobaviteljev tehnologije 5G na podlagi tveganja

Glede na končni cilj, ki je zagotoviti varnost in odpornost omrežij 5G ter njihovo trajnost, so se države članice sporazumele, da je treba oceniti profil tveganja posameznih dobaviteljev in nato uvesti ustrezne omejitve za dobavitelje, ki se štejejo za visoko tvegane, vključno s potrebnimi izključitvami, da bi učinkovito zmanjšali tveganje za ključna sredstva, kot je navedeno v naboru orodij. Komisija je pripravljena podpirati države članice pri izvajanju teh ukrepov.

Za pomoč njihovemu izvajanju povsod po EU so v usklajeni oceni tveganja v EU in naboru orodij EU podani napotki za (1) ocenjevanje profila tveganja dobaviteljev[17] in (2) občutljivost

[17] Odstavek 2.37 usklajene ocene tveganja v EU.

omrežnih elementov in funkcij[18] ter drugih sredstev. Usklajena ocena tveganja v EU in nabor orodij obravnavata tveganja v zvezi z dobavitelji omrežne opreme in omrežnih storitev 5G. Ne obravnavata drugih proizvodov in storitev, ki jih morda zagotavljajo ti ali drugi dobavitelji.

Kot je opredeljeno v odstavku 2.37 usklajene ocene tveganja v EU, je mogoče profil tveganja posameznih dobaviteljev oceniti na podlagi več dejavnikov.

Profil tveganja dobaviteljev bi bilo treba ocenjevati samo iz varnostnih razlogov in na podlagi objektivnih meril. Za lažji usklajen pristop k izvajanju teh ukrepov se v naboru orodij priporoča, da si države članice izmenjujejo informacije o nacionalnih pristopih in dobrih praksah. Poleg tega Komisija meni, da bi morala biti ta dejavnost med prvimi prednostnimi nalogami naslednje faze dela v skupini za sodelovanje na področju varnosti omrežij in informacij skupaj s Komisijo in agencijo ENISA.

Pomembno je, da se omejitve v zvezi z dobavitelji, ki se štejejo za visoko tvegane, vključno s potrebnimi izključitvami za učinkovito zmanjševanje tveganja, ter ukrepi za preprečevanje odvisnosti od teh dobaviteljev izvedejo pravočasno. Če se to izvede v najzgodnejši fazi, po možnosti tudi v zvezi s postopki dodeljevanja licenc za 5G, se bo močno povečala predvidljivost za udeležence na trgu, kar bo prispevalo k hitri uvedbi omrežij 5G ter zagotovilo dolgoročno varnost omrežij 5G in odpornost dobavne verige tehnologije 5G.

Hkrati se pri nacionalni izvedbi teh ukrepov, če je potrebno in utemeljeno, lahko določijo različni roki, zlasti v primeru trenutne močne odvisnosti od opreme ali storitev dobaviteljev, ki se štejejo za visoko tvegane (npr. z upoštevanjem ciklov posodabljanja opreme, zlasti prehoda z „nesamostojnih“ na „samostojna“ omrežja 5G). Države članice bi lahko razmislile o opredelitvi izvedbenih načrtov, ki bi vključevali prehodna obdobja za zadevne omrežne operaterje. V zvezi s tem bi bilo treba v skladu s cilji akcijskega načrta za 5G[19] opredeliti prehodna obdobja tako, da bi ohranili ali celo okrepili spodbude za naložbe v sodobno omrežno opremo, vključno s pospešitvijo uvedbe celovitih („samostojnih“) jedrnih omrežij 5G in nadomestitvijo obstoječe opreme 4G v drugih delih omrežij (npr. v radijskem dostopovnem omrežju).

Poleg tega bodo telekomunikacijski operaterji zaradi zapletenosti omrežij 5G, ki temeljijo na programski opremi, morda vse bolj odvisni od tretjih oseb za opravljanje nekaterih nalog, kot sta vzdrževanje in nadgradnja omrežij in programske opreme 5G, ter drugih upravljanih storitev poleg dobave omrežne opreme. Kot je opisano v usklajeni oceni tveganja v EU, je to izvor hudega varnostnega tveganja. Na ta vidik bi morali biti posebej pozorni. Bistveno je, da se opravi tudi temeljita varnostna ocena profila tveganja dobaviteljev, ki so zadolženi za te storitve, zlasti če se te naloge ne opravljajo v EU. Da bi infrastrukturo 5G dolgoročno ohranili nedotaknjeno, bi bilo treba sprejeti primerne ukrepe, tudi z uvedbo omejitev, predvsem v občutljivih delih omrežij 5G, ali s potrebno izključitvijo visoko tveganih subjektov v skladu z ukrepi za zmanjšanje tveganja iz nabora orodij.

5.2 Vloga Komisije pri podpori izvajanja nabora orodij

[18] V odstavku 2.21 usklajene ocene tveganja v EU so predstavljene glavne kategorije elementov in funkcij ter njihova splošna raven občutljivosti ter našteti ključni elementi, ki so jih države članice določile za vsako kategorijo, v odstavkih 2.28 in 2.29 pa je navedenih več drugih vrst občutljivih sredstev ali območij (npr. posebni subjekti ali geografska območja).
[19] COM(2016) 588 z dne 14. septembra 2016 z naslovom Akcijski načrt za 5G v Evropi.

Komisija bo še naprej podpirala izvajanje pristopa EU h kibernetski varnosti 5G na splošno in dajala posebne pobude v zvezi z ukrepi in cilji nabora orodij, če lahko zagotovi dodano vrednost. V celoti bo izkoristila svoje pristojnosti in ustrezne instrumente, kolikor bo potrebno za obravnavo ugotovljenih varnostnih vidikov. S tem in s sodelovanjem z državami članicami in zasebnim sektorjem želi Komisija podpreti strateške ukrepe, ki bodo prispevali k zagotovitvi tehnološke suverenosti EU in vodilne vloge v prihodnjem razvoju omrežnih tehnologij, na področju tehnologij kibernetske varnosti in pri vseh ustreznih gradnikih, od katerih sta odvisna naše celotno gospodarstvo in varnost.

Konkretneje bo Komisija, da bi zagotovila izvajanje ustreznih ukrepov za zmanjševanje tveganja iz nabora orodij na področjih, za katera je pristojna, izvedla dejavnosti, navedene v nadaljevanju.

Ohranjanje kibernetske varnosti omrežij 5G in raznolike vrednostne verige 5G

– Sodelovanje na področju kibernetske varnosti: še naprej bo podpirala države članice, da bi lahko učinkovito, usklajeno in pravočasno izvajale nacionalne ukrepe preko skupine za sodelovanje na področju varnosti omrežij in informacij.

– Telekomunikacije in pravila kibernetske varnosti: podpirala bo izvajanje ukrepov iz nabora orodij v zvezi z varnostnimi zahtevami, zlasti glede upoštevnih določb na podlagi evropskih predpisov o elektronskih komunikacijah, upoštevala dodano vrednost možnih izvedbenih aktov o podrobni določitvi tehničnih in organizacijskih varnostnih ukrepov kot dopolnitev nacionalnih predpisov ter izboljšala učinkovitost in usklajenost varnostnih ukrepov, naloženih operaterjem.

– Standardizacija: dejavno bo pomagala ohranjati in po potrebi krepiti evropsko udeležbo v zadevnih organih za standardizacijo, da bi bili doseženi evropski cilji glede varnosti in interoperabilnosti. Zlasti bo skupaj z državami članicami ocenjevala in spodbujala tehnične specifikacije in standarde, ki bodo omogočali interoperabilnost med dobavitelji opreme 5G v različnih delih omrežja, tudi v obstoječih omrežjih, da bi omogočila nastanek pravega večdobaviteljskega okolja, npr. preko odprtih, interoperabilnih vmesnikov.

– Certifikacija: podpirala bo razvoj shem certificiranja za 5G, ki bodo nudile rešitve za omrežja 5G v certifikacijskem okviru EU za kibernetsko varnost.

– Pregledovanje neposrednih tujih naložb: podpirala bo izvajanje okvira EU za pregledovanje s kartiranjem vrednostne verige 5G vključno z občutljivimi omrežnimi sredstvi in redno spremljala neposredne tuje naložbe vzdolž vrednostne verige. V skladu s časovnico pregledovanja neposrednih tujih naložb (od oktobra 2020) bo podrobno pregledovala tuje naložbe na področju 5G v skladu s smernicami iz Uredbe (EU) 2019/452, pri čemer bo upoštevala usklajeno oceno tveganja v EU in nabor orodij EU.

– Instrumenti trgovinske zaščite: spremljala bo vse ustrezne spremembe na trgu v EU in tretjih državah ter z ukrepi trgovinske zaščite akterje EU na evropskem trgu tehnologije 5G varovala pred morebitnimi praksami, ki izkrivljajo trgovino (dumping ali subvencioniranje), po potrebi tudi s predhodnimi preiskavami.

– Pravila konkurence: spremljala bo delovanje trgov za dobavo strojne in programske opreme 5G, da bi zagotovila doseganje konkurenčnih rezultatov, tudi v zvezi z možnimi primeri pogodbene ali tehnične vezanosti na ponudnika.

– Programi financiranja EU: zagotavljala bo, da bo sodelovanje v programih financiranja EU na ustreznih tehnoloških področjih pogojeno z izpolnjevanjem varnostnih zahtev, in sicer tako, da bo v celoti uporabljala in še naprej razvijala pogoje glede varnosti v programih raziskav in inovacij, zlasti v programu Obzorje Evropa, programu za digitalno Evropo in instrumentu za povezovanje Evrope 2, evropskih strukturnih in naložbenih skladih ter drugih ustreznih programih. Podoben bi moral biti tudi pristop v programih in finančnih instrumentih EU za zunanje financiranje, tudi glede financiranja preko mednarodnih finančnih institucij.

– Javna naročila: spodbujala bo javna naročila na področju omrežij 5G, da bi podpirala zadane cilje varnosti, raznolikosti dobaviteljev in dolgoročne trajnosti omrežij 5G; predvsem si bo prizadevala zagotoviti ustrezno upoštevanje varnostnih vidikov pri oddaji javnih naročil v zvezi s področjem omrežij 5G v skladu s pravili EU o javnih naročilih.

– Odzivanje na incidente in obvladovanje krize (Načrt) ter vaje iz kibernetske varnosti: V celoti bo izkoristila razvoj Načrta EU[20] o usklajenem odzivu na velike kibernetske incidente. Poleg tega bo skupaj z agencijo ENISA razmislila o možni izvedbi vaje iz kibernetske varnosti 5G, brž ko bo trg to omogočal.

Ter v pristojnosti visokega predstavnika Unije za zunanje zadeve in varnostno politiko, podpredsednika Komisije in Sveta:

– Okvir za skupni diplomatski odziv EU na zlonamerne kibernetske dejavnosti (zbirka orodij za kibernetsko diplomacijo)[21]: v primeru zlonamernih kibernetskih dejavnosti, ki ogrožajo celovitost in varnost EU, se države članice pozivajo k uporabi ustreznih ukrepov skupne zunanje in varnostne politike iz zbirke orodij EU za kibernetsko diplomacijo (po potrebi tudi omejitvenih ukrepov) za spodbujanje sodelovanja, omogočanje lažjega zmanjševanja groženj in vpliv na vedenje možnih napadalcev.

Poleg tega bodo številni programi prispevali k ciljem preprečevanja ali omejevanja tveganja dolgoročne odvisnosti, saj bodo spodbujali nastanek raznolikega in trajnostnega trga za tehnologijo 5G, tudi z ohranjanjem zmogljivosti EU v vrednostni verigi 5G in naložbami v inovacije v skladu z mednarodnimi obveznostmi EU.

Spodbujanje inovacij ter naložbe v kibernetsko varnost in tehnologije omrežne infrastrukture:

– Programi financiranja EU: krepila bo naložbe v raziskave, inovacije in uvajanje omrežnih tehnologij ter ustreznih temeljnih gradnikov. Komisija je v naslednjem proračunu EU za obdobje 2021–2027 predlagala za skoraj 3 milijarde eurov naložb v tehnologije kibernetske varnosti. Mednje spadajo raziskave in inovacije v okviru programa Obzorje Evropa in podpora zmogljivostim kibernetske varnosti v okviru programa za digitalno Evropo. Tudi InvestEU lahko zagotovi finančno podporo za raziskave in razvoj na področju tehnologije 5G ter za podporo njeni uvedbi.

[20] Priporočilo Komisije (EU) 2017/1584 o usklajenem odzivu na velike kibernetske incidente in krize.
[21] Sklepi Sveta z dne 20. novembra 2017, 9916/17.

Poleg tega je Komisija v okviru naslednjega programa Obzorje Evropa[22] predlagala vzpostavitev institucionaliziranega partnerstva EU za NGI/6G („pametna omrežja in storitve“) v partnerstvu z industrijo ob usklajevanju z državami članicami, da bi dokončala razvoj tehnologije 5G, predvsem pa, da bi se **pripravila na 6G**, naslednjo generacijo mobilne tehnologije. Predlaganih je bilo več kot 2,5 milijarde eurov naložb EU iz proračuna EU (za obdobje 2021–27), ki naj bi jih dopolnilo najmanj 7,5 milijarde eurov zasebnih naložb v to pobudo.

– Razvoj in uvedba v industriji: ocenila bo možne tržne vrzeli vzdolž vrednostne verige 5G, ki bi upravičile ciljno usmerjene intervencije v okviru naslednjega dolgoročnega proračuna ali morda pomembnih projektov skupnega evropskega interesa na področju kibernetske varnosti v skladu s forumom na visoki ravni o pomembnih projektih skupnega evropskega interesa. Za odločitev za oblikovanje in vzpostavitev pomembnih projektov skupnega evropskega interesa so pristojne države članice in podjetja. Pravila EU nudijo okvir za omogočanje dejavnosti, Komisija pa je pripravljena olajševati potrebne stike in dajati napotke.

6. Zaključek

Omrežja 5G bodo evropskim državljanom, družbi in gospodarstvu prinesla vrsto priložnosti. Zagotavljanje varnosti in odpornosti omrežij 5G je zato bistvenega pomena. Hkrati pa so kibernetske grožnje (tudi nevarnost vmešavanja držav ali akterjev s podporo držav zunaj EU) vse večji izziv, katerega pomembnost narašča skupaj z vse večjo odvisnostjo od tehnologije in podatkov. Če zanemarimo kibernetsko varnost, bomo okrnili zaupanje v razvoj digitalnega gospodarstva in družbe, tako da ga EU ne bi mogla v celoti izkoristiti. Zato je potreben odziv, ki se ustrezno razvija in krepi.

Dosledno usklajen pristop h kibernetski varnosti kritičnih tehnologij in omrežij v EU je za EU bistvenega pomena za zagotovitev njene tehnološke suverenosti ter ohranjanja in razvoja njenih industrijskih zmogljivosti. Komisija bo v celoti podpirala izvajanje pristopa EU do kibernetske varnosti omrežij 5G, hkrati pa bo zagotavljala, da bodo trgi EU še naprej odprti za proizvode in storitve, ki upoštevajo spreminjajoče se zahteve za kibernetsko varnost in zaupanje.

Zato morajo vse zainteresirane strani na področju varnosti tehnologije 5G ostati neomajne, potrebno pa bo tudi nadaljnje sodelovanje med državami članicami, Komisijo in agencijo ENISA.

Kot je bilo že povedano, Komisija kot neposredni naslednji korak poziva države članice, da hitro ukrepajo za učinkovito in objektivno izvajanje ukrepov, sprejetih v okviru nabora orodij, in da si ob podpori Komisije in agencije ENISA še naprej skupaj prizadevajo za zagotovitev sodelovanja na ravni EU. Obenem bo v okviru svoje pristojnosti začela izvajati vse ustrezne dejavnosti za podporo izvajanja nabora orodij s strani držav članic in krepitev njegovega učinka.

[22] Možno je tudi financiranje preko instrumenta za povezovanje Evrope 2.0 in programa za digitalno Evropo.

Dodatek: Kategorije tveganja (vir: Usklajena ocena tveganja v EU)

	Kategorije tveganja
Scenariji tveganja v zvezi z nezadostnimi varnostnimi ukrepi	*T1: napačna konfiguracija omrežij*
	T2: pomanjkanje nadzora nad dostopom
Scenariji tveganja v zvezi z dobavno verigo 5G	*T3: slaba kakovost proizvodov*
	T4: odvisnost od enega samega dobavitelja v individualnih omrežjih ali pomanjkanje raznolikosti v nacionalnem okviru
Scenariji tveganja v zvezi z načinom delovanja glavnih akterjev, ki predstavljajo nevarnost	*T5: poseganje države preko dobavne verige 5G*
	T6: izkoriščanje omrežij 5G s strani organiziranega kriminala ali hudodelske združbe, katerih cilj so končni uporabniki
Scenariji tveganja v zvezi z medsebojno odvisnostjo med omrežji 5G in drugimi kritičnimi sistemi	*T7: hude motnje v kritični infrastrukturi ali storitvah*
	T8: prenehanje delovanja omrežij v velikem obsegu zaradi prekinitve oskrbe z električno energijo ali drugih podpornih sistemov
Scenariji tveganja v zvezi z napravami končnih uporabnikov	*T9: izkoriščanje IoT (interneta stvari)*