EIROPAS
KOMISIJA

Briselē, 29.1.2020.
COM(2020) 50 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI

Droša 5G ieviešana ES - ES rīkkopas īstenošana

1. *Ievads*

Piektās paaudzes (5G) telesakaru tīkliem būs būtiska nozīme Eiropas sabiedriskajā un ekonomiskajā attīstībā. Sagaidāms, ka tie pavērs milzīgas ekonomiskās izdevības un uz tiem lielā mērā balstīsies digitālā pārveide un zaļā pārkārtošanās tādās jomās kā transports, enerģētika, ražošana, veselības aprūpe, lauksaimniecība un plašsaziņa.

Tas nozīmē, ka 5G ir potenciāls iespaidot teju visas ES iedzīvotāju dzīves šķautnes. Tāpēc 5G tīklu kiberdrošība ir būtiska ne tikai tāpēc, lai pasargātu mūsu ekonomiku, sabiedrību un demokrātiskos procesus, bet arī tāpēc, lai nodrošinātu, ka digitālā pārveide norit uzticēšanās garā un nāk par labu ikvienam ES iedzīvotājam.

Tas, ka tik daudzi kritiski svarīgi pakalpojumi ir atkarīgi no 5G tīkliem, nozīmē, ka sistēmisku un plaši izvērstu pārrāvumu sekas būtu sevišķi smagas un, ņemot vērā digitālo ekosistēmu starpsavienotību, sniegtos pāri valstu robežām. Tāpēc 5G tīklu kiberdrošības nodrošināšana Savienībai ir stratēģiski svarīgs jautājums, sevišķi laikā, kad kiberuzbrukumi plešas plašumā un kļūst aizvien sarežģītāki, bet to realizētāji — aizvien daudzveidīgāki, turklāt to vidū aizvien biežāk ir ļaundari, kas tieši vai netieši pārstāv trešās valstis. Tāpēc pirmo reizi ir nolemts nospraust kopīgu Eiropas pieeju kritiskās infrastruktūras (pie tās pieder arī 5G) drošībai. Pieeja paredz, ka ES iekšējā tirgus atvērtība tiek pilnībā respektēta tiktāl, ciktāl tiek izpildītas ES drošības prasības, kas balstās uz risku novērtējumu.

Eiropadome 2019. gada 22. martā aicināja rast saskanīgu pieeju 5G tīklu drošībai. Komisija 2019. gada 26. martā pieņēma Ieteikumu (ES) 2019/534 par 5G tīklu kiberdrošību[1]. Ieteikumā Komisija aicināja dalībvalstis pabeigt nacionālos riska novērtējumus un pārskatīt nacionālos pasākumus, kā arī ES līmenī kopīgi strādāt pie koordinēta riska novērtējuma un sagatavot rīkkopu ar iespējamiem riska mazināšanas pasākumiem. Šis paziņojums ir neatņemama daļa no Komisijas visaptverošās Eiropas digitālās stratēģijas, kuru sagatavot aicinājusi Eiropadome.

2. *5G ierīkošana ES*

5G tīklu infrastruktūras ieviešana ir priekšnosacījums Eiropas rūpnieciskās stratēģijas realizēšanai un konkurētspējas saglabāšanai. Komisija ir atzinusi, ka bez 5G tīkla tehnoloģiju ieviešanas nebūs iespējams pilnvērtīgi ieviest nākotnes digitālos pakalpojumus. 2016. gadā Komisija pieņēma 5G rīcības plānu, kurā izklāstīts, kā panākt, lai jau no 2020. gada Savienībā būtu izveidota savienojamības infrastruktūra, kas nepieciešama gan digitālajai pārveidei, gan 5G pārklājuma nodrošināšanai pilsētu teritorijās un gar visiem galvenajiem transporta koridoriem no 2025. gada[2]. Paziņojumā par Gigabitu sabiedrību[3] izvirzīts mērķis nodrošināt iespēju pieslēgties mobilajiem datiem it visur, tostarp arī laukos un attālos reģionos.

Kas attiecas uz frekvenču piešķiršanu, dalībvalstis ir piešķīrušas 16 % no pirmapgūstamajām 5G frekvenču joslām[4]. Tā kā pastāv juridisks pienākums līdz gada beigām atļaut visu 5G

[1] Ieteikums (EU) 2019/534 par 5G tīklu kiberdrošību, OV L 88, 29.3.2019., 42.–47. lpp.
[2] COM(2016) 588, 2016. gada 14. jūnijs. "5G Eiropai. Rīcības plāns".
[3] COM(2016)587 "Konkurētspējīga digitālā vienotā tirgus savienojamība. Virzība uz Eiropas Gigabitu sabiedrību".
[4] http://www.5GObservatory.eu

pirmapgūstamo joslu izmantošanu, tuvākajos mēnešos tiks apspriestas vairākas piešķiršanas procedūras.

Runājot par 5G pakalpojumu ieviešanu komerciālām vajadzībām, šajā ziņā Eiropa ir viens no attīstītākajiem pasaules reģioniem[5]. Pašlaik paredzams, ka līdz 2020. gada beigām 138 Eiropas pilsētās būs pieejami pirmie 5G pakalpojumi. Pirmo 5G tīklu pamatā ir pašreizējās 4. paaudzes tīkla tehnoloģijas (4G), un 5G pakalpojumi galvenokārt tiek sniegti plašai sabiedrībai un izpaužas vai nu kā 4G pakalpojumu uzlabojums (jaudas un ātruma ziņā), vai kā izmaksefektīva bezvadu alternatīva fiksētajiem tīkliem[6].

Runājot par izdevībām, kas pavērsies jauniem B2B pakalpojumiem (uzņēmumu pakalpojumi uzņēmumiem) tādās jomās kā enerģētika, pārtikas rūpniecība un lauksaimniecība, veselības aprūpe, ražošana vai transports, Eiropa ir krietni pavirzījusies uz priekšu — investīcijas sasniedz 1 miljardu EUR, no kuriem 300 miljoni ir no programmas "Apvārsnis 2020" atbalstītās 5G publiskā un privātā sektora partnerības. Šīs investīcijas aptver vairāk nekā 160 liela mēroga 5G izmēģinājumus Eiropā, t. sk. desmit pārrobežu automaģistrāļu koridorus, kurā tiek lielā mērogā testēti 5G tehnoloģijās bāzētie satīklotas un automatizētas mobilitātes pakalpojumi. Pie izmēģinājuma projektiem var minēt arī 5G iespējotus lietojumus visdažādākajās jomās, sākot ar ilgtspējīgu veselības aprūpi, automatizētu mobilitāti un resursefektīvu lauksaimniecību un beidzot ar viedajiem elektrotīkliem un t. s. rūpniecību 4.0. Turklāt EIB ar Eiropas Stratēģisko investīciju fonda atbalstu ir piešķīrusi aizdevumus, lai paātrinātu 5G tehnoloģijas pētniecību un izstrādi.

Eiropas Elektronisko sakaru kodekss ("Kodekss")[7], kas būs piemērojams no 2020. gada 21. decembra, ir būtisks elements, uz kura bāzes radīt labvēlīgu vidi investīcijām 5G un nākamo paaudžu tīklos. Arī atbalstam no publiskā finansējuma programmām, piemēram, Eiropas infrastruktūras savienošanas instrumenta Digitālās programmas[8] vai Eiropas strukturālajiem un investīciju fondiem, būs ļoti liela nozīme turpmākā 5G tīklu ieviešanā, it īpaši tādos aspektos kā vietējo kopienu iespējas izmantot 5G iespējotus pakalpojumus (skolās, slimnīcās, pilsētās un pašvaldībās).

Ņemot vērā stratēģiskās iespējas, ko dažādās nozarēs Eiropai pavērs 5G pakalpojumi, ir sevišķi svarīgi, lai operatori un pakalpojumu sniedzēji investētu pašos modernākajos 5G tīkla un pakalpojumu risinājumos. Tas nozīmē, ka, lai nodrošinātu vismodernākās 5G funkcijas, piemēram, tīkla slāņošanu[9] un perifērdatošanu[10], vajadzīgi ne tikai jauni 5G radiotīkli, bet arī jauni t. s. savrupie 5G pamattīkli.

---

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

[6] Dažas no jaunajam 5G funkcionālajām iespējām tiks ieviestas pakāpeniski. Pirmajā posmā (pašā sākumā vai īstermiņā) 5G ieviešana lielākoties skars "nesavrupos tīklus", proti, 5G tehnoloģijas tiks ieviestas tikai radiopiekļuves tīklā, visam pārējam tiks izmantots esošais 4G pamattīkls, un tādējādi galalietotājiem būs pieejami uzlaboti mobilie platjoslas sakari. Nākamajos posmos (īstermiņā/vidējā termiņā un ilgtermiņā) tiks ieviesti savrupie 5G tīkli, t. sk. 5G pamattīkla funkcijas, kas nozīmē, ka tīkla arhitektūra būs daudz pamatīgāk jāpārveido un laika gaitā tas arī tiks panākts.

[7] Eiropas Parlamenta un Padomes Direktīva (ES) 2018/1972 par Eiropas Elektronisko sakaru kodeksa izveidi (pārstrādāta redakcija).

[8] Priekšlikums regulai, ar ko izveido Eiropas infrastruktūras savienošanas instrumentu un atceļ Regulu (ES) Nr. 1316/2013 un (ES) Nr. 283/2014 (COM(2018)438, 2018. gada 6. jūnijs).

[9] 5G tīkla slāņošana dod iespēju viena fiziska tīkla ietvaros ļoti efektīvi nošķirt dažādus pakalpojumu slāņus un tādējādi palielināt iespējas visā tīklā sniegt diferencētus pakalpojumus.

[10] Perifērdatošana ir izkliedētās datošanas paradigma, kad datošana un datu tuvāk vietai, kur tā ir vajadzīga, un tādējādi tiek uzlabots reakcijas laiks un patērēts mazāk platjoslas resursu.

Komisija arī turpmāk pilnībā atbalstīs sekmīgu 5G ierīkošanu ES, tostarp palīdzēs dalībvalstīm un ieinteresētajām personām lieti izmantot 5G pavērtās izdevības. Pienācīga ievērība tiks veltīta attiecīgiem veselības aspektiem — tas darāms, ievērojot piesardzības principu[11] un sadarbojoties ar relevantajām starptautiskām organizācijām un zinātniskajām aprindām.

3. ES koordinētais riska novērtējums par kiberdrošību 5G tīklos

Dalībvalstis, kopīgi darbodamās TID[12] sadarbības grupā, ir pabeigušas savus riska novērtējumus par 5G tīkla infrastruktūru un līdz 2019. gada jūlija sākumam ir to rezultātus nosūtījušas Komisijai un *ENISA* — Eiropas Savienības Kiberdrošības aģentūrai.

Pamatojoties uz šiem nacionālajiem riska novērtējumiem, 2019. gada 9. oktobrī TID sadarbības grupa, kuras sastāvā ir dalībvalstu, Komisijas un *ENISA* pārstāvji, publicēja ziņojumu par ES koordinēto riska novērtējumu par kiberdrošību 5G tīklos[13]. Tajā apzināti galvenie apdraudējumi un apdraudētāji, vissensitīvākie aktīvi un galvenās ievainojamības (tostarp tehniskās un citas), kas skar 5G tīklus. Tāpat ziņojumā apzinātas vairākas to risku kategorijas, kas no ES viedokļa ir stratēģiski svarīgi, un izklāstīti konkrēti riska scenāriji, kuri atspoguļo dažādo parametru (ievainojamības, draudi un apdraudētāji) relevantās kombinācijas attiecībā uz dažādiem aktīviem (sk. papildinājumu).

Lai ziņojumu papildinātu un savāktu rīkkopai nepieciešamo papildu informāciju, *ENISA* sagatavoja īpašu apdraudējumu karti[14], kurā sīkāk iztirzāti konkrēti ziņojumā aplūkotie tehniskie aspekti, jo īpaši tas, kā apzināt tīkla aktīvus un to apdraudējumus.

ES koordinētā riska novērtējuma ziņojumā apskatīti vairāki 5G tīkliem būtiski aspekti. Tie ir šādi.

a) Līdz ar 5G ieviestajām tehnoloģiskajām pārmaiņām paplašināsies kopējais uzbrukumu tvērums un potenciālo uzbrucējiem pieejamo ielaušanās punktu skaits:

- funkcionalitāte vairāk koncentrēsies tīkla perifērijā un tīkla arhitektūra kļūs decentralizētāka nekā iepriekšējo paaudžu mobilajos tīklos, un tas nozīmē, ka dažas pamattīkla funkcijas tiks integrētas citās tīkla daļās, kas savukārt palielinās attiecīgās aparatūras (piem., bāzes staciju vai MANO funkciju) sensitivitāti;

- tā kā 5G ierīcēs aizvien vairāk izmanto tieši programmatūru, tas gan palielina esošos riskus, kas saistīti ar programmatūras izstrādes un atjaunināšanas procesiem, gan rada jaunus riskus, kas saistīti ar kļūdainu konfigurāciju, tāpēc drošības analīzē daudz nozīmīgāku vietu ieņem tas, kādu izvēli izdarījis katrs mobilā tīkla operators tīkla ieviešanas posmā.

[11] Padomes Ieteikums 1999/519/EK (1999. gada 12. jūlijs) par ierobežojumiem plašas sabiedrības pakļaušanai elektromagnētisko lauku iedarbībai (0 Hz līdz 300 GHz).

[12] Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (TID direktīva). TID sadarbības grupa ir izveidota ar TID direktīvu, lai nodrošinātu stratēģisku sadarbību un informācijas apmaiņu kiberdrošības jautājumos starp ES dalībvalstīm.

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

[14] ENISA Threat landscape for 5G networks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

b) Šīs jaunās tehnoloģiskās iezīmes nozīmē, ka lielāka ievērība veltāma tam, kādā mērā mobilo tīklu operatori paļaujas uz piegādātājiem, kas ir trešās puses, un tam, kāda ir šo piegādātāju loma 5G piegādes ķēdē.

Tas savukārt vairo gan to iespējamo uzbrukuma ceļu skaitu, ko varētu izmantot apdraudētāji, jo īpaši trešo valstu aktori vai trešo valstu atbalstītie aktori, jo tie ir spējīgi (tiem ir nodoms un resursi) uzbrukt ES dalībvalstu telesakaru tīkliem, gan šādu uzbrukumu seku iespējamo smagumu.

Runājot par to, ka aizvien pieaug neaizsargātība pret tādiem uzbrukumiem, kurus atvieglinājuši piegādātāji, kas ir trešās puses, īpaši nozīmīgs būs katra atsevišķā piegādātāja riska profils, jo īpaši gadījumos, kad piegādātāja klātbūtne tīklos vai teritorijās ir ievērojama.

c) Jo lielāka ir atkarība no viena vienīga piegādātāja, jo lielāka ir neaizsargātība pret piegādātāja potenciālu komerciālu neveiksmi un smagākas ir sekas. Tas arī dara smagākas potenciālās sekas, kam par iemeslu ir vājās vietas un ievainojamības, un palielina iespēju, ka apdraudētāji šo aspektus varētu savtīgi izmantot, jo īpaši, ja runa ir par atkarību no tāda piegādātāja, kurš ir ļoti riskants.

d) Ja kādas jaunās ieceres par 5G izmantošanu realizēsies, 5G tīkli kļūs par būtisku posmu daudzu kritiski svarīgu IT lietojumu piegādes ķēdē, un tas ietekmēs ne tikai konfidencialitātes un privātuma prasības — šo tīklu integritāte un pieejamība kļūs par būtisku nacionālās drošības jautājumu un par sarežģītu drošības problēmu no ES viedokļa.

Avots: ES koordinētais riska novērtējums

ES koordinētā riska novērtējuma ziņojumā secināts, ka šie sarežģītie uzdevumi nesīs līdzi jaunu drošības paradigmu, kas liks pārskatīt pašreizējo 5G nozarei un tās ekosistēmai piemērojamo rīcībpolitiku un drošības regulējumu; tas nozīmē, ka dalībvalstīm katrā ziņā būs jāīsteno nepieciešamie riska mazināšanas pasākumi.

Lai efektīvi novērstu konstatētos riskus un stiprinātu 5G tīklu drošību un noturību, ir vajadzīga visaptveroša pieeja, proti, ir jāparedz virkne galveno pasākumu un vairāki papildpasākumi, lai būtu iespējams riskiem pievērsties vienlaikus. Uz ES koordinētā riska novērtējuma pamata var apzināt riska mazināšanas pasākumus, kurus var piemērot valstiskā un Eiropas līmenī.

Padomes 2019. gada 3. decembra secinājumos atzinīgi vērtētas koordinētā riska novērtējuma atziņas un uzsvērts, "cik svarīga ir koordinēta pieeja un ieteikuma efektīva īstenošana, lai izvairītos no vienotā tirgus sadrumstalotības"[15]. Tālab Padome aicināja dalībvalstis, Komisiju un *ENISA* "veikt visus vajadzīgos pasākumus savas kompetences ietvaros, lai nodrošinātu elektronisko sakaru tīklu, jo īpaši 5G tīklu, drošību un integritāti, un turpināt konsolidēt saskaņotu pieeju nolūkā risināt ar 5G tehnoloģijām saistītās drošības problēmas".

[15] Padomes secinājumi par 5G nozīmi Eiropas ekonomikā un nepieciešamību mazināt ar 5G saistītos drošības riskus. 2019. gada 3. decembris, 14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

4. ES rīkkopa 5G kiberdrošības jomā

2020. gada 29. janvārī TID sadarbības grupa publicēja ES rīkkopu, kas veltīta riska mazināšanas pasākumiem[16]. Tajā iztirzāti visi koordinētā riska novērtējuma ziņojumā apzinātie riski.

ES rīkkopā ir apzināti un aprakstīti vairāki stratēģiski un tehniski pasākumi, ko var izmantot apzināto risku mazināšanai, kā arī attiecīgas pasākumu efektivitāti vairojošas atbalsta darbības. **Stratēģiskie pasākumi** ir pasākumi, kas saistīti ar regulatīvo iestāžu aizvien plašākajām pilnvarām rūpīgi pārbaudīt tīkla iepirkšanu un ieviešanu, specifiski pasākumi, ar kuriem novērš ar netehniskām ievainojamībām saistītos riskus, un iespējamās ierosmes, kā veicināt ilgtspējīgu un daudzveidīgu 5G piegādes un vērtību ķēdi nolūkā nepieļaut atkarības izraisītus sistēmiskus ilgtermiņa riskus. **Tehniskie pasākumi** ir pasākumi, ar ko 5G tīklu un ierīču drošību stiprina, novēršot riskus, kuru cēlonis ir tehnoloģijas, procesi, cilvēciskie un fiziskie faktori. Bez tam attiecībā uz katru ES koordinētajā riska novērtējumā apzināto riska jomu tajā ir paredzēti **riska mazināšanas plāni**, kuru pamatā ir visefektīvākie pasākumi.

TIS sadarbības grupas pieņemtajos secinājumos par ES rīkkopu uzskaitīta virkne **galveno pasākumu**, kas jāīsteno visām dalībvalstīm un Komisijai; tie ir šādi.

ES rīkkopas secinājumi

ES rīkkopa paredz virkni pasākumu un darbību, kas — ja tos pienācīgi kombinē un efektīvi īsteno — ņemami par pamatu koordinētai pieejai šajā jomā. Tā kā ES koordinētajā riska novērtējumā apzinātas ļoti dažādas un daudzveidīgas riska jomas, ar viena veida pasākumiem nepietiks — lai risinātu problēmas visās nozīmīgākajās riska jomās, būs nepieciešams plašs pasākumu klāsts.

Rīkkopu sagatavojot, tika novērtēti iespējamie riska mazināšanas plāni un apzināti visefektīvākie pasākumi; tas ir pamatā tālāk uzskaitītajiem ieteikumiem.

1. Visām dalībvalstīm būtu jānodrošina, ka tās ir ieviesušas pasākumus (tostarp piešķirušas attiecīgas pilnvaras nacionālajām iestādēm), lai varētu pienācīgi un samērīgi reaģēt uz pašlaik apzinātajiem un nākotnē iespējamiem riskiem; jo īpaši tām būtu jānodrošina, ka tās spēj, ievērojot uz risku balstītu pieeju, ierobežot, aizliegt un/vai noteikt specifiskas prasības un nosacījumus 5G tīkla ierīču piegādei, ieviešanai un ekspluatācijai, pamatojoties virkni ar drošību saistītu iemesliem.

Konkrētāk, tām būtu:

- *jāpastiprina mobilo tīklu operatoriem izvirzītās **drošības prasības** (piem., jānosaka stingra piekļuves kontrole, jāparedz noteikumi par drošu ekspluatāciju un pārraudzību, jāierobežo specifisku funkciju nodošana ārpakalpojumu sniedzējiem utt.);*

- *jānovērtē piegādātāju riska profils; atkarībā no šī novērtējuma iznākuma **jāpiemēro pienācīgi ierobežojumi — tostarp, ja tas vajadzīgs risku efektīvai mazināšanai, piegādātāju izslēgšana — tiem piegādātājiem, kuri rada ļoti lielu risku galvenajiem aktīviem**, kas uzskatāmi par kritiskiem un sensitīviem (piemēram, pamattīkla funkcijas, tīkla pārvaldības un orķestrācijas funkcijas, piekļuves tīkla funkcijas);*

- *jānodrošina, ka katram operatoram ir pienācīga stratēģija, kas paredz izmantot vairākus piegādātājus, lai **novērstu vai ierobežotu pārmērīgu atkarību** no viena piegādātāja (vai vairākiem*

[16] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 2020. gada 29. janvāris. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

*piegādātājiem ar līdzīgu riska profilu), rastu pienācīgu piegādātāju sabalansētību nacionālā līmenī un **nepieļautu atkarību no ļoti riskantiem piegādātājiem**; tas arī nozīmē, ka jāvairās no tādām situācijām, kad nav iespējams atsvabināties no viena vienīga piegādātāja, tostarp ir jāveicina lielāka ierīču sadarbspēja.*

2. Eiropas Komisijai kopā ar dalībvalstīm būtu:

- *jāuztur **daudzveidīga un ilgtspējīga 5G piegādes ķēde**, lai izvairītos no ilgtermiņa atkarības, tostarp:*

  - *pilnībā jāizmanto esošie ES rīki un instrumenti, konkrētāk, rūpīgi jāizvērtē tie potenciālie **ārvalstu tiešie ieguldījumi** (FDI), kuri ietekmē 5G būtiskos aktīvus, un jāizvairās no dempinga un subsīdiju radītiem **kropļojumiem** 5G piegādes tirgū; un*

  - *vēl vairāk jāstiprina **ES spējas 5G un nākamo paaudžu tehnoloģijās**, izmantojot attiecīgās ES programmas un finansējumu;*

- *jāveicina dalībvalstu koordinācija **standartizācijas** laukā nolūkā sasniegt konkrētus drošības mērķus un izstrādāt **attiecīgas ES mēroga sertifikācijas shēmas**, tādējādi vairojot ražojumu un procesu drošību.*

3. Lai nodrošinātu, ka šī koordinētā pieeja iztur laika pārbaudi, būtu jāpaplašina TID sadarbības grupas attiecīgā novirziena apakšgrupas pilnvaras un jāizvērš sadarbība ar citām relevantām struktūrām un institūcijām ar mērķi:

- *ar Komisijas un ENISA atbalstu periodiski pārskatīt **nacionālos un ES riska novērtējumus** par 5G un nākamo paaudžu tīklu drošību, tostarp pilnveidot un salāgot izmantoto novērtēšanas metodiku un to pieskaņot 5G tehnoloģijas attīstībai;*

- *balstoties uz dalībvalstu sagatavotiem strukturētiem ziņojumiem, regulāri un sīki **sekot līdzi un novērtēt**, kā sokas ar rīkkopas **īstenošanu**;*

- *koordinēt un atbalstīt **atbalsta darbību** īstenošanu, kas nozīmē, ka ir vajadzīga sadarbība ES līmenī, jo īpaši pie norāžu izstrādes un paraugprakses apmaiņas par dažādajiem pasākumiem;*

- *vajadzības gadījumā atbalstīt vēl ciešāku iespējamo koordināciju ES līmenī, jo īpaši, lai panāktu tālāku konverģenci attiecībā uz **tīkla operatoriem izvirzītajām tehniskajām un organizatoriskajām drošības prasībām**.*

Avots: ES rīkkopa.

Rīkkopas secinājumi apliecina dalībvalstu stingro apņēmību kopīgi risināt 5G tīklu drošības problēmas. Tas ir izšķirīgi svarīgi šādu apsvērumu dēļ: drošība dalībvalstu iekšienē un visas ES līmenī; valstu tautsaimniecība un visas ES iekšējais tirgus; Eiropas tehnoloģiskā suverenitāte. Gan ES koordinētais riska novērtējums, gan ES rīkkopa atklāj, cik vērtīgs ir visu dalībvalstu pārstāvju, Komisijas un *ENISA* intensīvais kopīgais darbs TID sadarbības grupā.

Rīkkopa paver iespējas gan īstenot vienotu ES pieeju 5G kiberdrošībai, jo tā palīdzēs nodrošināt konsekvenci visā iekšējā tirgū, pateicoties ES rīcībpolitikām un koordinācijai, gan dalībvalstīm realizēt savu kompetenci nacionālās drošības jomā. Rīkkopā ietvertie riska mazināšanas pasākumi un plāni dod ES iespēju pienācīgi, iedarbīgi un samērīgi reaģēt uz kopējām 5G kiberdrošības problēmām.

Komisija atzinīgi vērtē publicēto ES rīkkopu par 5G kiberdrošību un pilnībā atbalsta visus iepriekš minētos secinājumus.

Komisija aicina dalībvalstis un attiecīgās Savienības institūcijas, aģentūras un citas struktūras:

i) nodrošināt, ka visā ES tiek bez kavēšanās īstenotas efektīvas un pienācīgas riska mazināšanas stratēģijas saskanīgi ar ES rīkkopu, un

ii) veikt visus vajadzīgos turpmākos pasākumus, lai nodrošinātu koordināciju Savienības līmenī, tostarp turpinot darbu TID sadarbības grupā un izveidojot stabilus mehānismus ES rīkkopas īstenošanas pārraudzībai, lai tā garantētu pasākumu efektivitāti un iekšējā tirgus netraucētu darbību.

5. Rīkkopas īstenošana

No dalībvalstu apņemšanās rīkkopu pilnvērtīgi izmantot ir atkarīgs, vai izdosies izveidot pārliecinošu un sekmīgu ES pieeju 5G drošībai. Lai gan dalībvalstis par konkrēta pasākuma lietderību lems atkarībā no saviem vietējiem apstākļiem, apzināto risku novēršana sekmēsies tikai tad, ja **ikvienā dalībvalstī tiks realizēts TID sadarbības grupas ieteikto galveno pasākumu kopums (sk. rīkkopas secinājumus augstāk) un arī ES līmenī tiks īstenoti vairāki pasākumi**.

Komisija ir gatava arī nākamajos posmos sniegt pilnīgu atbalstu un aicina dalībvalstis:

- **līdz 2020. gada 30. aprīlim** spert konkrētus un izmērāmus soļus, lai tiktu īstenots ES rīkkopas secinājumos ieteiktais galveno pasākumu kopums;

- **līdz 2020. gada 30. jūnijam** TID sadarbības grupā par šo galveno pasākumu īstenošanas gaitu katrā dalībvalstī sagatavot ziņojumu, kura pamatā ir regulārā ziņošana un pārraudzība, ar ko nodarbojas TID sadarbības grupa ar Komisijas un *ENISA* atbalstu.

5.1. Saskanīga, uz risku balstīta pieeja 5G piegādātājiem

Tā kā virsmērķis ir nodrošināt 5G tīklu drošību, noturību un ilgtspēju, dalībvalstis ir vienisprātis, ka — atbilstīgi rīkkopā secinātajam — ir nepieciešams novērtēt atsevišķu piegādātāju riska profilu un līdz ar to piemērot pienācīgus ierobežojumus — tostarp, ja tas vajadzīgs risku efektīvai mazināšanai, piegādātāju izslēgšanu — tiem piegādātājiem, kuri rada ļoti lielu risku galvenajiem aktīviem. Komisija ir gatava atbalstīt dalībvalstis šo pasākumu īstenošanā.

Šo pasākumu īstenošanā visā ES palīdzēs ES koordinētais riska novērtējums un ES rīkkopa, kur sniegtas norādes par 1) to, kā novērtēt piegādātāju riska profilu[17], un 2) to, cik sensitīvi ir tīklu un citu aktīvu elementi un funkcijas[18]. Gan ES koordinētais riska novērtējums, gan rīkkopas pasākumi aptver riskus, kas saistīti ar 5G tīkla aprīkojuma un tīkla pakalpojumu piegādātājiem. Tie neaptver citus produktus vai pakalpojumus, ko šie vai citi piegādātāji varētu piegādāt.

[17] ES koordinētā riska novērtējuma 2.37. punkts.

[18] ES koordinētā riska novērtējuma 2.21. punktā norādītas galvenās elementu un funkciju kategorijas un to vispārējais sensitivitātes līmenis, kā arī uzskaitīti vairāki dalībvalstu identificētie galvenie elementi katrā kategorijā; 2.28. un 2.29. punktā minēti vairāki citi sensitīvi aktīvi vai zonas (piem., specifiskas struktūras vai ģeogrāfiskie apgabali).

Kā definēts ES koordinētā riska novērtējuma 2.37. punktā, atsevišķu piegādātāju riska profilus var novērtēt, balstoties uz vairākiem faktoriem.

Piegādātāju riska profilu novērtējums būtu jāveic, vadoties tikai no drošības apsvērumiem un pamatojoties uz objektīviem kritērijiem. Lai atvieglinātu koordinētu pieeju šo pasākumu īstenošanai, rīkkopā ieteikts dalībvalstīm apmainīties ar informāciju par nacionālo pieeju un paraugpraksi. Turklāt Komisija uzskata, ka šim būtu jābūt vienam no pirmajiem jautājumiem, ko nākamajā darba posmā risina TID sadarbības grupā kopā ar Komisiju un *ENISA*.

Būtiski, lai ierobežojumi — tostarp, ja tas vajadzīgs risku efektīvai mazināšanai, piegādātāju izslēgšana — attiecībā uz tiem piegādātājiem, kuri rada ļoti lielu risku galvenajiem aktīviem, un pasākumi, kā izvairīties no atkarības no šādiem piegādātājiem, tiktu piemēroti laikus. Ja tas tiks izdarīts pēc iespējas agrākā posmā, tostarp, ja iespējams, vēl tad, kad notiek 5G frekvenču licencēšanas process, tirgus dalībniekiem būs skaidrāks priekšstats par nākotni, kas savukārt sekmēs strauju 5G tīklu ierīkošanu un ilgtermiņā nodrošinās 5G tīklu drošību un 5G piegādes ķēdes noturību.

Tajā pašā laikā nacionālie īstenošanas pasākumi var paredzēt dažādus termiņus (ja tas nepieciešams un ir pamatoti), jo īpaši gadījumos, kad patlaban tiek ļoti plaši izmantots ļoti riskantu piegādātāju aprīkojums vai pakalpojumi (piemēram, var ņemt vērā aprīkojuma modernizācijas ciklus, jo īpaši pāreju no "nesavrupiem" uz "savrupiem" 5G tīkliem). Dalībvalstis varētu izstrādāt īstenošanas plānus, kuros ir norādīti pienācīgi pārejas periodi attiecībā uz šādā situācijā esošiem tīkla operatoriem. Šajā sakarā pārejas periodi būtu jānosaka tā, lai ne tikai saglabātu, bet pat veicinātu investīcijas modernā tīkla aprīkojumā, tostarp paātrinot pilnvērtīgu ("savrupu") 5G pamattīklu ieviešanu un esošā 4G aprīkojuma nomaiņu citās tīklu daļās (piemēram, radiopiekļuves tīklā) atbilstīgi 5G rīcības plānā nospraustajiem mērķiem[19].

Tā kā 5G programmatūrā balstītie tīkli ir ļoti sarežģīti, telesakaru operatori aizvien biežāk var no trešām pusēm ne tikai iegādāties tīkla aprīkojumu, bet tām uzticēt arī citus uzdevumus, piemēram, 5G tīklu un programmatūras uzturēšanu un modernizēšanu, kā arī citus pārvaldības pakalpojumus. Kā norādīts ES koordinētajā riska novērtējumā, tas var radīt nopietnu drošības risku, tāpēc šim aspektam būtu jāpievērš īpaša uzmanība. Ir ļoti būtiski, lai, gatavojot to piegādātāju riska profilu, kam uzticēts sniegt šos pakalpojumus, tie tiktu rūpīgi izvērtēti arī no drošības viedokļa, jo īpaši gadījumos, kad uzdevumu izpilde nenotiek ES. Lai saglabātu 5G integritāti ilgtermiņā, būtu jāveic piemēroti pasākumi, tostarp jāpiemēro ierobežojumi īpaši sensitīvām G5 tīklu daļām vai jāizslēdz sevišķi riskantas struktūras, kā to paredz rīkkopā izklāstītie riska mazināšanas pasākumi.

5.2. Komisijas loma rīkkopas īstenošanā

Komisija arī turpmāk atbalstīs gan ES pieejas īstenošanu attiecībā uz 5G kiberdrošību kopumā, gan specifiskas iniciatīvas saistībā ar rīkkopas pasākumiem un mērķiem, ja tā varētu dot pievienoto vērtību. Komisija pilnvērtīgi izmantos savas pilnvaras un attiecīgos instrumentus tādā mērā, kādā tas vajadzīgs, lai risinātu apzinātos drošības jautājumus. Šādi rīkodamās kopā ar dalībvalstīm un privāto sektoru, Komisija vēlas atbalstīt stratēģiskus pasākumus, kas palīdzēs nodrošināt ES tehnoloģisko suverenitāti un vadošo lomu tīkla

[19] COM(2016) 588, 2016. gada 14. septembris. "5G Eiropai. Rīcības plāns".

tehnoloģiju turpmākajā izstrādē, kiberdrošības tehnoloģijās un attiecīgajās bāzes tehnoloģijās, kurās balstās mūsu ekonomika un drošība kopumā.

Konkrētāk, lai nodrošinātu, ka tās kompetences jomās tiek īstenoti attiecīgie rīkkopā paredzētie pasākumi, Komisija rīkosies šādi.

5G tīklu kiberdrošības un diversificētas 5G vērtību ķēdes sargāšana

-**Sadarbība kiberdrošības jomā**: TID sadarbības grupas ietvaros turpināt palīdzēt dalībvalstīm efektīvi, koordinēti un savlaicīgi īstenot nacionālos pasākumus.

- **Telesakaru uzņēmumi un kiberdrošības noteikumi**: palīdzēt īstenot ar drošības prasībām saistītos rīkkopas pasākumus, jo īpaši tos, kas saistīti ar Eiropas elektronisko sakaru regulējuma attiecīgajiem noteikumiem, un pārdomāt, kādu pievienoto vērtību varētu dot īstenošanas akti, kas paredzētu tehniskus un organizatoriskus drošības pasākumus un tādējādi papildinātu nacionālos noteikumus un vairotu to drošības pasākumu efektivitāti un konsekvenci, kurus uzdots pildīt operatoriem.

- **Standartizācija**: tiecoties sasniegt Eiropas drošības un sadarbspējas mērķus, rīkoties, lai palīdzētu saglabāt un vajadzības gadījumā palielināt Eiropas līdzdalību attiecīgajās standartizācijas organizācijās. Konkrētāk, Komisija kopā ar dalībvalstīm novērtēs un popularizēs tehniskās specifikācijas un standartus, kas nodrošina sadarbspēju starp 5G ierīču piegādātājiem dažādās tīkla daļās, tostarp vēsturiskajos tīklos, lai radītu apstākļus (piemēram, izmantojot atvērtas un sadarbspējīgas saskarnes), kuros patiešām tiek izmantoti vairāki piegādātāji.

- **Sertifikācija**: atbalstīt tādu 5G sertifikācijas shēmu veidošanu, kas atbilst 5G tīklu vajadzībām atbilstīgi ES kiberdrošības sertifikācijas satvaram.

- **Ārvalstu tiešo ieguldījumu izvērtēšana**: atbalstīt ES izvērtēšanas satvara īstenošanu, proti, kartēt 5G (t. sk. sensitīvo tīkla aktīvu) vērtību ķēdi un regulāri pārraudzīt ĀTI visā vērtību ķēdē. Saskaņā ar ĀTI izvērtēšanas grafiku (no 2020. gada oktobra) Komisija rūpīgi pārbaudīs ārvalstu ieguldījumus 5G jomā saskaņā ar Regulā (ES) 2019/452 sniegtajām vadlīnijām, ņemot vērā ES koordinēto riska novērtējumu un ES rīkkopu.

- **Tirdzniecības aizsardzības instrumenti**: sekot līdzi visām nozīmīgajām norisēm ES un trešo valstu tirgos un Eiropas 5G tirgū sargāt dalībniekus no ES, izmantojot tirdzniecības aizsardzības pasākumus, lai novērstu iespējamu tirdzniecību kropļojošu praksi (dempingu vai subsidēšanu), tostarp vajadzības gadījumā uzsākot iepriekšēju izmeklēšanu.

- **Konkurences noteikumi:** sekot līdzi 5G aparatūras un programmatūras piegādes tirgu darbībai, lai nodrošinātu, ka veidojas konkurenciāla vide, tostarp nerodas iespējama līgumiska vai tehnoloģiska iesīkste.

- **ES finansējuma programmas**: nodrošināt, ka dalība ES finansējuma programmās attiecīgajās tehnoloģiju jomās ir atkarīga no drošības prasību izpildes, pilnā mērā izmantojot jau esošos un ieviešot jaunus drošības nosacījumus pētniecības un inovācijas programmās, jo īpaši programmā "Apvārsnis Eiropa", programmā "Digitālā Eiropa", Eiropas infrastruktūras savienošanas instrumentā 2, Eiropas strukturālajos un investīciju fondos un citās relevantās programmās. Līdzīgu pieeju varētu izmantot arī ES ārējā finansējuma programmās un

finansēšanas instrumentos, tostarp attiecībā uz finansējumu, ko nodrošina ar starptautisku finanšu iestāžu starpniecību.

- Publiskais iepirkums: 5G tīklu jomā izmantot publisko iepirkumu kā sviru, ar kuras palīdzību var sasniegt izvirzītos mērķus — 5G tīklu drošību, piegādātāju daudzveidību un ilgtermiņa ilgtspēju; konkrētāk, censties nodrošināt, ka, slēdzot publiskā iepirkuma līgumus saistībā ar 5G tīkliem, saskaņā ar ES publiskā iepirkuma noteikumiem tiek pienācīgi ņemti vērā drošības aspekti.

- Reaģēšana uz incidentiem un krīžu pārvarēšana (plāns) un kiberdrošības mācības: pilnā mērā izmantot izstrādāto ES plānu[20], kā koordinēti reaģēt uz plašapmēra pārrobežu kiberdrošības incidentiem. Bez tam kopā ar *ENISA* apsvērt iespēju sarīkot 5G kiberdrošības mācības, tiklīdz tirgus tam būs gatavs.

Ievērojot, ka atbildība šajās jomās pieder Padomei un Savienības Augstajam pārstāvim ārlietās un drošības politikas jautājumos un Komisijas priekšsēdētāja vietniekam:

izmantot **satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām (kiberdiplomātijas instrumentu kopumu)[21]**: tādu ļaunprātīgu kiberdarbību gadījumā, kas apdraud ES integritāti un drošību, dalībvalstis tiek mudinātas izmantot attiecīgos kopējās ārpolitikas un drošības politikas pasākumus, kas ir daļa no ES kiberdiplomātijas instrumentu kopuma (tostarp vajadzības gadījumā ierobežojošus pasākumus), lai veicinātu sadarbību, atvieglotu draudu mazināšanu un ietekmētu potenciālo agresoru uzvedību.

Turklāt vairākas programmas palīdzēs sasniegt mērķus — novērst vai ierobežot ilgtermiņa atkarības risku —, veicinot daudzveidīgu un ilgtspējīgu 5G tirgu; tostarp tiks uzturēta ES veiktspēju 5G vērtību ķēdē un investēts inovācijā, tomēr ievērojot ES starptautiskās saistības.

Inovāciju veicināšana un investīcijas kiberdrošībā un tīkla infrastruktūras tehnoloģijās

- ES finansējuma programmas: kāpināt investīcijas pētniecībā, inovācijā un tīkla tehnoloģiju un attiecīgo bāzes tehnoloģiju ieviešanā. Komisija ir ierosinājusi 2021.–27. gada ES budžetā teju 3 miljardus euro atvēlēt investīcijām kiberdrošības tehnoloģijās. Te ietilpst pētniecība un inovācija programmas "Apvārsnis Eiropa" ietvaros, kā arī atbalsts kiberdrošības pilnveidošanai programmas "Digitālā Eiropa" paspārnē. Arī "InvestEU" var sniegt finansiālu atbalstu gan pētniecībai un izstrādei 5G jomā, gan 5G ieviešanai.

Tāpat Komisija ir ierosinājusi nākamās programmas "Apvārsnis Eiropa"[22] ietvaros izveidot NGI/6G veltītu institucionalizētu partnerību ("Viedie tīkli un pakalpojumi"), lai kopīgi ar nozari un dalībvalstīm pabeigtu 5G ieviešanu un **sagatavotos G6** — nākamās paaudzes mobilajām tehnoloģijām. Ierosināts 2021.–27. gada ES budžetā investīcijām atvēlēt vairāk nekā 2,5 miljardus euro, kas savukārt ļaus piesaistīt vismaz 7,5 miljardus euro privāto investīciju.

- Rūpnieciskā izstrāde un ieviešana: izvērtēt iespējamos tirgus robus vai nepilnības 5G vērtību ķēdē, kas varētu būt par iemeslu vai nu selektīvai intervencei nākamā ilgtermiņa

[20] Komisijas Ieteikums par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm (ES) 2017/1584.
[21] Padomes secinājumi, 2017. gada 20. novembris, 9916/17.
[22] Finansējums varētu būt pieejams arī no EISI 2 un programmas "Digitālā Eiropa".

budžeta ietvaros, vai iespējamam *IPCEI* (svarīgi projekti visas Eiropas interesēs) kiberdrošības jomā atbilstīgi ierosinājumiem *IPCEI* augsta līmeņa forumā. Lēmums par *IPCEI* sagatavošanu un izveidi ir dalībvalstu un uzņēmumu ziņā. ES noteikumi ir radījuši tiem labvēlīgu vidi, un Komisija ir gatava sekmēt savstarpējos kontaktus un dot norādījumus.

6. Secinājumi

5G tīkli Eiropas iedzīvotājiem, sabiedrībai un ekonomikai sniegs plašus ieguvumus. Tāpēc ir būtiski nodrošināt 5G tīklu drošību un noturību. Tajā pašā laikā kiberdrošības apdraudējumi (tostarp trešo valstu aktoru vai trešo valstu atbalstīto aktoru iejaukšanās risks) aizvien mainās; jo lielāka ir paļaušanās uz tehnoloģijām un datiem, jo lielākas bažas tas rada. Kiberdrošības atstāšana novārtā grautu uzticēšanos digitālās ekonomikas un sabiedrības veidošanai un līdz ar to liegtu ES pilnā mērā izmantot tās sniegtās priekšrocības. Tas nozīmē, ka arī mūsu pretpasākumiem jāņemas spēkā un jāmainās laikam līdzi.

ES nebūs iespējams garantēt savu tehnoloģisko suverenitāti un uzturēt un pilnveidot savus rūpnieciskos spēkus, ja netiks īstenota koordinēta un konsekventa pieeja ES kritisko tehnoloģiju un tīklu kiberdrošībai. Komisija pilnībā atbalstīs ES kiberdrošības pieejas īstenošanu attiecībā uz 5G tīkliem un tajā pašā laikā gādās par to, ka ES tirgi ir atvērti tiem ražojumiem un pakalpojumiem, kas atbilst aizvien spiedīgākajām kiberdrošības un uzticamības prasībām.

Tālab ir svarīga gan visu 5G drošībā ieinteresēto pušu nezūdoša apņēmība, gan pastāvīga sadarbība starp dalībvalstīm, Komisiju un *ENISA*.

Iepriekš jau minēts, kas darāms bez liekas kavēšanās — Komisija aicina dalībvalstis nekavējoties rīkoties, lai efektīvi un objektīvi īstenotu rīkkopā minētos pasākumus, un ar Komisijas un *ENISA* atbalstu turpināt kopīgo darbu, lai nodrošinātu koordināciju ES līmenī. Līdztekus Komisija sāks īstenot visus relevantos tās kompetencē esošos pasākumus, lai atbalstītu rīkkopas īstenošanu dalībvalstīs un pastiprinātu tās ietekmi.

Papildinājums. Riska kategorijas (avots: ES koordinētais riska novērtējums).

	Riska kategorija
Riska scenāriji, kas saistīti ar nepietiekamiem drošības pasākumiem	*R1: Tīklu nepareiza konfigurācija*
	R2: Nepietiekama piekļuves kontrole
Riska scenāriji, kas saistīti ar 5G piegādes ķēdi	*R3: Zema ražojumu kvalitāte*
	R4: Atkarība no viena vienīga piegādātāja atsevišķā tīklā vai nepietiekama dažādība valsts mērogā
Riski scenāriji, kas saistīti ar galveno apdraudētāju modus operandi	*R5: Valsts iejaukšanās ar 5G piegādes ķēdes starpniecību*
	R6: 5G tīklu savtīga izmantošana organizētās noziedzības labā vai organizētās noziedzības sarīkoti apdraudējumi galalietotājiem
Riska scenāriji, kas saistīti ar 5G tīklu un citu kritiski svarīgu sistēmu savstarpējo atkarību	*R7: Kritisko infrastruktūru vai pakalpojumu būtiski pārrāvumi*
	R8: Tīklu masveida atteice, ja ir pārtraukta elektroapgādes vai citu atbalsta sistēmu darbība
Riska scenāriji, kas saistīti ar galalietotāju ierīcēm	*R9: Lietiskā interneta savtīga izmantošana*