EUROPOS
KOMISIJA

Briuselis, 2020 01 29
COM(2020) 50 final

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

Saugaus 5G ryšio diegimas ES. ES priemonių rinkinio įgyvendinimas

1. *Įžanga*

Penktosios kartos (5G) telekomunikacijų tinklams neabejotinai teks svarbus vaidmuo plėtojant Europos visuomenę ir ekonomiką. Manoma, kad šie tinklai suteiks didelių ekonominių galimybių ir padės pagrindą perėjimui prie skaitmeninių ir ekologiškų technologijų tokiose srityse kaip transportas, energetika, gamyba, sveikatos priežiūra, žemės ūkis ir žiniasklaida.

Todėl 5G ryšys gali turėti įtakos beveik visiems ES piliečių gyvenimo aspektams. Taigi 5G tinklų kibernetinis saugumas yra labai svarbus ne tik siekiant apsaugoti mūsų ekonomiką, visuomenę ir demokratinius procesus, bet ir užtikrinant patikimą perėjimą prie skaitmeninių technologijų visų ES piliečių labui.

Dėl daugelio ypatingos svarbos paslaugų priklausomumo nuo 5G tinklų sisteminio ir plataus masto sutrikdymo pasekmės būtų ypač rimtos ir, atsižvelgus į skaitmeninių ekosistemų tarpusavio ryšį, galėtų daryti reikšmingą tarptautinį poveikį. Todėl šiuo metu, kai kibernetinių išpuolių daugėja, jie sudėtingesni nei bet kada anksčiau, o išpuolius rengia patys įvairiausi subjektai, ypač ne ES valstybių ar jų remiami subjektai, 5G tinklų kibernetinio saugumo užtikrinimas yra Europos Sąjungai strategiškai svarbus klausimas. Kalbant apie tokių ypatingos svarbos infrastruktūros objektų kaip 5G saugumą, pasirinktas metodas – pirmą kartą nustatyti bendrą Europos požiūrį. Šiuo požiūriu visapusiškai puoselėjamas ES vidaus rinkos atvirumas nenukrypstant nuo rizika pagrįstų ES saugumo reikalavimų.

2019 m. kovo 22 d. Europos Vadovų Taryba paragino siekti suderinto požiūrio į 5G tinklų saugumą. 2019 m. kovo 26 d. Komisija priėmė Rekomendaciją (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo[1]. Rekomendacijoje valstybės narės paragintos užbaigti nacionalinius rizikos vertinimus ir peržiūrėti nacionalines priemones, bendradarbiauti ES lygmeniu atliekant koordinuotą rizikos vertinimą ir parengti galimų rizikos mažinimo priemonių rinkinį. Šis komunikatas yra neatsiejama Komisijos visapusiškos Europos skaitmeninės strategijos, kurią paragino parengti Europos Vadovų Taryba, dalis.

2. *5G diegimas Europos Sąjungoje*

5G tinklų infrastruktūros diegimas Europoje yra labai svarbus Europos pramonės strategijai ir konkurencingumui. Komisija pripažino, kad 5G tinklo technologijų diegimas iš esmės sudarys sąlygas būsimoms skaitmeninėms paslaugoms. Siekdama užtikrinti, kad nuo 2020 m. Sąjunga turėtų skaitmeninei transformacijai reikalingą ryšio infrastruktūrą ir iki 2025 m. 5G būtų visapusiškai įdiegtas miestų teritorijose ir pagrindiniuose transporto keliuose, 2016 m. Komisija priėmė 5G veiksmų planą[2]. Gigabitinės visuomenės komunikate užsibrėžta prieigą prie judriojo ryšio duomenų teikti visur[3], be kita ko, ir kaimo vietovėse bei atokiuose regionuose.

Kalbant apie dažnių skyrimą, valstybės narės yra paskyrusios 16 % pradinių 5G juostų[4]. Atsižvelgiant į teisinį įsipareigojimą iki metų pabaigos leisti naudotis visomis 5G pradinėmis

[1] Rekomendacija (ES) 2019/534 dėl 5G tinklų kibernetinio saugumo, OL L 88, 2019 3 29, p. 42–47.
[2] COM(2016) 588, 2016 m. birželio 14 d., Europos 5G veiksmų planas.
[3] COM(2016) 587, Junglumas – bendrosios skaitmeninės rinkos pagrindas. Kelias į Europos gigabitinę visuomenę.
[4] http://www.5GObservatory.eu

juostomis, per kelis ateinančius mėnesius planuojama surengti konsultacijas dėl kelių paskyrimo procedūrų.

Pradėtų teikti komercinių 5G paslaugų požiūriu Europa yra vienas iš pažangiausių pasaulio regionų[5]. Šiuo metu numatoma, kad iki 2020 m. pabaigos pirmosiomis 5G paslaugomis bus galima naudotis 138 Europos miestuose. Pirmieji 5G tinklai grindžiami dabartinės 4-osios kartos (4G) tinklo technologijomis, o 5G paslaugos daugiausia teikiamos plačiajai visuomenei arba kaip didesnio pajėgumo ir spartos 4G paslaugos, arba kaip ekonomiškai efektyvi belaidė fiksuotojo ryšio tinklų alternatyva[6].

Kalbant apie naujų verslo verslui teikiamų paslaugų galimybes, kaip antai energetikos, maisto ir žemės ūkio, sveikatos priežiūros, gamybos ar transporto sektoriuose, Europa yra padariusi didelę pažangą: tam skirta 1 mlrd. EUR investicijų, iš kurių 300 mln. EUR ES finansavimo lėšų numatyta 5G viešojo ir privačiojo sektorių partnerystei pagal programą „Horizontas 2020“. Šiomis investicijomis finansuojama daugiau nei 160 didelio masto 5G ryšio bandymų, numatytų Europoje, įskaitant dešimtyje tarpvalstybinių greitkelių koridorių atliksimus didelio masto 5G grindžiamo susietojo ir automatizuoto judumo paslaugų bandymus. Bus išbandomos 5G grindžiamos programos tokiose srityse kaip tvari sveikatos priežiūra ir automatizuotas judumas efektyviai išteklius naudojančiame žemės ūkyje, išmanieji elektros tinklai ir „Pramonė 4.0“. Be to, siekdamas paspartinti 5G technologijų mokslinius tyrimus ir technologinę plėtrą, EIB kartu su Europos strateginių investicijų fondu suteikė paskolų.

Nuo 2020 m. gruodžio 21 d. taikysimas Europos elektroninių ryšių kodeksas (toliau – Kodeksas)[7] padėjo svarbų pamatą siekiant sukurti investicijoms palankią aplinką 5G tinklams ir ne tik. Be to, remiant 5G tinklų diegimą ateityje, visų pirma užtikrinant galimybę gauti 5G grindžiamas paslaugas bendruomenėms, pavyzdžiui, mokykloms, ligoninėms, miestams ir savivaldybėms, esminis vaidmuo teks viešojo finansavimo programoms, kaip antai Europos infrastruktūros tinklų priemonės skaitmeninio sektoriaus programai[8], taip pat Europos struktūriniams ir investicijų fondams.

Atsižvelgiant į strategines Europos galimybes, susijusias su 5G paslaugomis įvairioms pramonės šakoms, bus ypač svarbu, kad operatoriai ir paslaugų teikėjai investuotų į pažangius 5G tinklų ir paslaugų sprendimus. Pastariesiems prireiks ne tik naujų 5G radijo tinklų, bet ir naujų vadinamųjų autonominių 5G pagrindinių tinklų, kad būtų galima siūlyti pažangias 5G funkcijas, pavyzdžiui, tinklo padalijimo[9] (angl. *slicing*) ir tinklo paribio kompiuterijos[10] (angl. *edge computing*) funkcijas.

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

[6] Palaipsniui bus pasiūlytos kai kurios naujos 5G funkcijos. Per pirmą etapą (labai trumpą ar trumpalaikį) 5G bus iš esmės diegiamas kaip neautonominiai tinklai, kai 5G technologijų pagrindu atnaujinamas tik radijo prieigos tinklas, o visa kita ir toliau grindžiama dabartiniais 4G pagrindiniais tinklais. Tokie tinklai galutiniams naudotojams užtikrins geresnį judriojo plačiajuosčio ryšio veikimą. Per tolesnius etapus (trumpuoju ir vidutinės trukmės laikotarpiu iki ilgalaikio) diegiant autonominius 5G tinklus, įskaitant 5G pagrindinio tinklo funkcijas, ilgainiui prireiks kur kas didesnio masto tinklų struktūros pakeitimų.

[7] Europos Parlamento ir Tarybos direktyva (ES) 2018/1972, kuria nustatomas Europos elektroninių ryšių kodeksas (nauja redakcija).

[8] 2018 m. birželio 6 d. Pasiūlymas dėl Reglamento dėl Europos infrastruktūros tinklų priemonės, kuriuo panaikinami reglamentai (ES) Nr. 1316/2013 ir (ES) Nr. 283/2014 (COM(2018) 438).

[9] 5G tinklo padalijimas leidžia labai aiškiai atskirti skirtingus paslaugų lygmenis tame pačiame fiziniame tinkle, taip suteikiant daugiau galimybių siūlyti diferencijuotas paslaugas visame tinkle.

Komisija ir toliau visapusiškai rems sėkmingą 5G diegimą Europos Sąjungoje, be kita ko, bendradarbiaudama su valstybėmis narėmis ir suinteresuotaisiais subjektais, kad būtų pasinaudota 5G teikiamomis galimybėmis. Bendradarbiaujant su atitinkamomis tarptautinėmis organizacijomis bei mokslo bendruomene ir laikantis atsargumo principo[11], bus tinkamai atsižvelgta į sveikatos aspektus.

3. ES koordinuotas rizikos, susijusios su 5G tinklų kibernetiniu saugumu, vertinimas

Visos valstybės narės, bendradarbiaudamos su TIS[12] bendradarbiavimo grupe, parengė savo 5G tinklo infrastruktūros nacionalinius rizikos vertinimus ir iki 2019 m. liepos mėn. pradžios jų rezultatus perdavė Komisijai bei Europos Sąjungos kibernetinio saugumo agentūrai (ENISA).

2019 m. spalio 9 d. TIS bendradarbiavimo grupė, kurią sudaro valstybių narių, Komisijos ir ENISA atstovai, remdamasi šiais nacionaliniais rizikos vertinimais, paskelbė ataskaitą dėl ES koordinuoto rizikos, susijusios su 5G tinklų kibernetiniu saugumu, vertinimo[13]. Ataskaitoje nurodomos pagrindinės grėsmės ir grėsmę keliantys subjektai, pažeidžiamiausi objektai ir pagrindinės pažeidžiamos vietos (įskaitant techninius aspektus ir kitokio pobūdžio pažeidžiamumą), darantys poveikį 5G tinklams. Tuo remiantis ataskaitoje taip pat nustatyta kelių kategorijų Europos Sąjungai kylanti strateginės svarbos rizika, pavaizduota konkrečiais įvairiems objektams (žr. priedą) kylančios rizikos scenarijais, atitinkančiais aktualius skirtingų parametrų (pažeidžiamų vietų, grėsmių ir grėsmę keliančių subjektų) derinius.

Siekdama papildyti šią ataskaitą ir prisidėti prie priemonių rinkinio rengimo, ENISA parengė specialią grėsmių apžvalgą[14], sudarytą iš išsamios tam tikrų techninių aspektų, visų pirma tinklo objektų nustatymo ir šiems objektams kylančių grėsmių, analizės.

ES koordinuoto rizikos vertinimo ataskaitoje pabrėžiama keletas svarbių aspektų, susijusių su 5G tinklais. Konkrečiai:

a) 5G ryšio lemtos technologinės permainos padidins bendrą išpuolių potencialą, o išpuolių organizatoriams atvers daugiau įsilaužimo galimybių:

- dėl patobulintų tinklo paribio funkcijų ir mažiau centralizuotos struktūros nei ankstesnių judriojo ryšio tinklų atveju kai kurios pagrindinių tinklų funkcijos gali būti integruotos kitose tinklų dalyse, todėl atitinkama įranga (pvz., bazinės radijo ryšio stotys ar MANO funkcijos) taps pažeidžiamesnė;

- didesnė 5G įrangos programinės įrangos dalis lemia didesnę riziką, susijusią su programinės įrangos kūrimo ir atnaujinimo procesais, kelia naują konfigūravimo klaidų

[10] Tinklo paribio kompiuterija yra paskirstytosios kompiuterijos paradigma, leidžianti priartinti kompiuterinį apdorojimą ir duomenų saugojimą prie vietos, kurioje to reikia, taip sutrumpinant atsako trukmę ir taupant juostos plotį.

[11] 1999 m. liepos 12 d. Tarybos rekomendacija dėl elektromagnetinių laukų (0 Hz–300 GHz) poveikio plačiajai visuomenei ribojimo (1999/519/EB).

[12] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva). TIS direktyva įsteigtos TIS bendradarbiavimo grupės paskirtis – užtikrinti strateginį ES valstybių narių bendradarbiavimą ir keitimąsi informacija kibernetinio saugumo srityje.

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

[14] ENISA. Su 5G tinklais susijusių grėsmių apžvalga: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

riziką ir, atliekant saugumo analizę, verčia skirti daugiau dėmesio kiekvieno judriojo ryšio tinklo operatoriaus sprendimams tinklo diegimo etapu.

b) Dėl šių naujų technologinių savybių daug svarbesnė taps judriojo ryšio tinklo operatorių priklausomybė nuo trečiųjų šalių tiekėjų ir pastarųjų vaidmuo 5G tiekimo grandinėje.

Savo ruožtu dėl to atsiras daugiau būdų rengti išpuolius, kuriais galės pasinaudoti priešiški subjektai, visų pirma ne ES valstybių ar jų remiami subjektai, nes jie turi pajėgumų (tiek ketinimų, tiek išteklių) vykdyti išpuolius prieš ES valstybių narių telekomunikacijų tinklus, o galimas tokių išpuolių poveikio mastas padidės.

Šiomis aplinkybėmis, kai dėl trečiųjų šalių tiekėjų kaltės gali atsirasi daugiau išpuoliams atvirų spragų, taps ypač svarbu įvertinti atskirų tiekėjų rizikos profilius, ypač tais atvejais, kai tiekėjo veikla tinkluose ar srityse yra reikšminga.

c) Didelė priklausomybė nuo vienintelio tiekėjo didina tiek galimybę nukentėti, tiek padarinius šiam tiekėjui nutraukus tiekimą. Taip pat sunkėja galimi silpnų vietų ar pažeidžiamumo padariniai ir grėsmę keliančių subjektų galimybės jais pasinaudoti, ypač esant priklausomybei nuo didelę riziką keliančio tiekėjo.

d) Pavykus realizuoti kai kuriuos iš naujų 5G ryšio panaudojimo būdų 5G tinklai galiausiai taps svarbia daugelio ypatingos svarbos IT taikomųjų programų tiekimo grandinės dalimi, todėl bus ne tik daromas poveikis konfidencialumo ir privatumo reikalavimams, bet ir tų tinklų vientisumas ir prieinamumas taps vienu svarbiausių tiek nacionalinio, tiek ES lygmens saugumo iššūkiu.

Šaltinis: ES koordinuotas rizikos vertinimas.

Be to, ES koordinuoto rizikos vertinimo ataskaitoje daroma išvada, kad dėl tų iššūkių atsiranda nauja saugumo paradigma, verčianti iš naujo įvertinti dabartinę 5G sektoriui ir jo ekosistemai taikomą politiką ir saugumo sistemą, o valstybes nares įpareigojanti imtis būtinų rizikos mažinimo priemonių.

Siekiant veiksmingai šalinti nustatytą riziką ir didinti 5G tinklų saugumą ir atsparumą, būtinas visapusiškas požiūris, suponuojantis pagrindinių priemonių taikymą ir kartu susijusių potencialiai rizikos šalinimą palaikančių veiksmų įgyvendinimą. ES koordinuotas rizikos vertinimas tapo pagrindu vertinant rizikos mažinimo priemones, kurias būtų galima taikyti nacionaliniu ir Europos lygmenimis.

2019 m. gruodžio 3 d. Tarybos išvadose patvirtintos koordinuoto rizikos vertinimo išvados ir akcentuojama, kad „svarbu laikytis suderinto požiūrio ir veiksmingai įgyvendinti tą rekomendaciją siekiant išvengti bendrosios rinkos susiskaidymo“[15]. Todėl Taryba paragino valstybes nares, Komisiją ir ENISA „imtis visų būtinų priemonių pagal savo kompetenciją užtikrinti elektroninių ryšių tinklų, ypač 5G tinklų, saugumą bei vientisumą ir toliau stiprinti suderintą požiūrį siekiant spręsti su 5G technologijomis susijusius saugumo uždavinius“.

4. Europos Sąjungos 5G kibernetinio saugumo priemonių rinkinys

[15] Tarybos išvados dėl 5G svarbos Europos ekonomikai ir poreikio mažinti su 5G susijusią saugumo riziką. 2019 m. gruodžio 3 d., 14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

2020 m. sausio 29 d. TIS bendradarbiavimo grupė paskelbė ES rizikos mažinimo priemonių rinkinį[16]. Jame atsižvelgiama į visų rūšių, nustatytų ES koordinuoto rizikos vertinimo ataskaitoje, riziką.

ES priemonių rinkinyje įvardijamos ir aprašomos strateginės ir techninės priemonės, taip pat atitinkami jų veiksmingumui didinti reikalingi veiksmai, kurių galima imtis siekiant sumažinti nustatytą riziką. **Strateginės priemonės** apima priemones, susijusias su didesniais reguliavimo įgaliojimais valdžios institucijoms tikrinti tinklų viešuosius pirkimus ir diegimą, konkrečias priemones, skirtas su netechninio pobūdžio pažeidžiamumu susijusiai rizikai, ir galimas iniciatyvas, pagal kurias būtų skatinama tvari ir diversifikuota 5G tiekimo ir vertės grandinė, taip siekiant išvengti sisteminės ir ilgalaikės priklausomybės rizikos. **Techninės priemonės** apima priemones 5G tinklų ir įrangos saugumui didinti šalinant riziką, keliamą technologijų, procesų, žmogiškųjų ir fizinių veiksnių. Be to, kiekvienai iš rizikos sričių, nustatytų ES koordinuoto rizikos vertinimo ataskaitoje, priemonių rinkinyje numatomi **rizikos mažinimo planai**, grindžiami didžiausią veiksmingumą užtikrinančiomis priemonėmis.

TIS bendradarbiavimo grupės suderintose ES priemonių rinkinio išvadose rekomenduojama visoms valstybėms narėms ir Komisijai iš šių priemonių pirmiausia įgyvendinti šias **pagrindines priemones**:

ES priemonių rinkinio išvados

ES priemonių rinkinyje nustatomos įvairiausios priemonės ir veiksmai, kuriuos tinkamai derinant ir veiksmingai įgyvendinant būtų padėtas pagrindas suderintam šios srities požiūriui. ES koordinuotame rizikos vertinime nustatytų rizikos sričių yra tiek daug ir jų pobūdis yra toks įvairus, kad šalinant visų pagrindinių sričių riziką nepakaks jokių vienos rūšies priemonių, o prireiks jas tinkamai derinti.

Remiantis galimų rizikos mažinimo planų vertinimu ir nustačius pačias veiksmingiausias priemones, šiame priemonių rinkinyje pateikiamos tokios rekomendacijos:

1. Visos valstybės narės turėtų užtikrinti, kad būtų nustatytos priemonės (be kita ko, nacionalinių valdžios institucijų įgaliojimai), leidžiančios deramai ir proporcingai reaguoti į šiuo metu nustatytą ir būsimą riziką, ir visų pirma užtikrinti, kad įvairiausiais saugumo sumetimais, taikydamos rizika grindžiamą požiūrį, jos būtų pajėgios 5G tinklo įrangos tiekimą, diegimą ir veikimą apriboti, uždrausti ir (arba) nustatyti jam konkrečius reikalavimus ar sąlygas.

Visų pirma jos turėtų:

- *griežtinti judriojo ryšio tinklo operatoriams taikomus* ***saugumo reikalavimus*** *(pvz., griežta prieigos kontrolė, saugaus eksploatavimo ir stebėsenos taisyklės, specifinių funkcijų perdavimo rangovams apribojimai ir t. t.);*

- *vertinti tiekėjų rizikos profilį; tuo remiantis* ***taikyti atitinkamus apribojimus, be kita ko, veiksmingo rizikos mažinimo tikslu būtinus draudimus, tiekėjams, kurie vertinami kaip keliantys didelę riziką pagrindiniams objektams****, kurie ES koordinuotame rizikos vertinime*

[16] 5G tinklų kibernetinis saugumas. ES rizikos mažinimo priemonių rinkinys, 2020 m. sausio 29 d., https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

laikomi ypatingos svarbos ir slaptais (pavyzdžiui, pagrindinio tinklo funkcijos, tinklo valdymo ir derinimo funkcijos, tinklo prieigos funkcijos);

 užtikrinti, kad kiekvienas operatorius turėtų tinkamą kelių pardavėjų strategiją, kad ***išvengtų bet kokios didelės priklausomybės*** *nuo vienintelio tiekėjo (ar tiekėjų, kurių rizikos profilis panašus)* ***arba ją apribotų****, užtikrintų tinkamą tiekėjų pusiausvyrą nacionaliniu lygmeniu ir* ***vengtų priklausomybės nuo tiekėjų, kurie vertinami kaip keliantys didelę riziką****; tam taip pat reikia vengti susisaistymo su vieninteliu tiekėju, be kita ko, skatinant didesnę įrangos sąveiką.*

2. Kartu su valstybėmis narėmis Komisija turėtų padėti:

 išlaikyti ***diversifikuotą ir tvarią 5G tiekimo grandinę****, kad būtų išvengta ilgalaikės priklausomybės, be kita ko:*

o visapusiškai pasinaudodama esamomis ES priemonėmis, visų pirma tikrindama galimas ***tiesiogines užsienio investicijas*** *(TUI), darančias poveikį 5G pagrindiniams objektams, ir vengdama 5G tiekimo rinkos* ***iškraipymų****, atsirandančių dėl galimo dempingo ar subsidijų;*

o toliau stiprindama ***ES pajėgumus 5G ir vėlesnės kartos technologijų srityje*** *naudojant atitinkamas ES programas ir finansavimą;*

 palengvinti valstybių narių veiksmų koordinavimą ***standartų nustatymo*** *srityje, kad būtų pasiekti konkretūs saugumo tikslai, ir skatinant saugesnius produktus ir procesus parengti* ***atitinkamą (-as) ES masto sertifikavimo schemą (-as).***

3. Siekiant užtikrinti, kad šis suderintas požiūris išlaikytų laiko išbandymą, reikėtų išplėsti TIS bendradarbiavimo grupės įgaliojimus ir bendradarbiavimą su kitomis atitinkamomis įstaigomis ir subjektais, kad visų pirma būtų galima:

 remiant Komisijai ir ENISA periodiškai peržiūrėti 5G ir vėlesnės kartos tinklų ***nacionalinius ir ES rizikos vertinimus****, toliau tobulinant ir derinant taikomą vertinimo metodiką ir ją pritaikant prie kintančios 5G technologijos;*

 vykdyti išsamią ir reguliarią rinkinio priemonių ***įgyvendinimo stebėseną ir vertinimą*** *remiantis valstybių narių struktūrinėmis ataskaitomis;*

 koordinuoti ir remti ***paramos veiksmų****, kuriems būtinas ES lygmens bendradarbiavimas, įgyvendinimą, visų pirma rengiant gaires ir keičiantis geriausia praktika, susijusia su įvairiomis priemonėmis;*

 atitinkamais atvejais remti tolesnį galimą koordinavimą ES lygmeniu, visų pirma siekiant toliau vienodinti ***tinklo operatoriams taikomus techninius ir organizacinius saugumo reikalavimus.***

Šaltinis: ES priemonių rinkinys.

Priemonių rinkinio išvadose akivaizdus tvirtas valstybių narių pasiryžimas kartu spręsti 5G tinklų saugumo problemas. Tai itin svarbu saugumui valstybėse narėse ir ES mastu, šalių ūkiui, ES vidaus rinkai ir Europos technologiniam suverenumui. Tiek ES koordinuotame rizikos vertinime, tiek ES priemonių rinkinyje didelė reikšmė teikiama kolektyviniam darbui,

kurį atlieka TIS bendradarbiavimo grupė, kurioje intensyviai bendradarbiauja visų valstybių narių, Komisijos ir ENISA atstovai.

Priemonių rinkinys sudaro sąlygas nustatyti bendrą ES požiūrį į 5G kibernetinį saugumą ir padeda siekti ES politikos ir koordinavimo nuoseklumo visoje vidaus rinkoje, o valstybėms narėms leidžia naudotis savo kompetencija, visų pirma nacionalinio saugumo srityje. Rinkinyje nustatytos rizikos mažinimo priemonės ir planai suteikia galimybę ES tinkamai, veiksmingai ir proporcingai reaguoti į bendras 5G kibernetinio saugumo problemas.

Komisija palankiai vertina paskelbtą ES 5G kibernetinio saugumo priemonių rinkinį ir visapusiškai palaiko visas pirmiau pateiktas rinkinio išvadas.

Komisija ragina valstybes nares ir atitinkamas Sąjungos institucijas, agentūras ir kitas įstaigas:

i) pagal ES priemonių rinkinį užtikrinti spartų veiksmingų ir tinkamų rizikos mažinimo strategijų įgyvendinimą visoje ES;

ii) imtis visų būtinų tolesnių veiksmų siekiant užtikrinti koordinavimą Sąjungos lygmeniu, be kita ko, pasinaudojant TIS bendradarbiavimo grupėje nuolat vykdomu darbu ir sukuriant patikimą ES priemonių rinkinio įgyvendinimo stebėsenos mechanizmą, kad būtų užtikrintas priemonių veiksmingumas ir sklandus vidaus rinkos veikimas.

5. Rinkinio priemonių įgyvendinimas

Formuojant patikimą ir rezultatyvų Europos požiūrį į 5G saugumą yra itin svarbus valstybių narių pasiryžimas visapusiškai pasinaudoti rinkinio priemonėmis. Valstybės narės priims sprendimus dėl konkrečios priemonės tinkamumo atsižvelgdamos į nacionalines aplinkybes, tačiau siekiant pašalinti nustatytą riziką **pagrindines priemones, rekomenduotas TIS bendradarbiavimo grupės (žr. priemonių rinkinio išvadas pirmiau), absoliučiai privalu įdiegti kiekvienoje valstybėje narėje, o kai kurias priemones – ES lygmeniu**.

Komisija yra pasirengusi toliau teikti visapusišką paramą kitais etapais ir ragina valstybes nares:

- **iki 2020 m. balandžio 30 d.** imtis konkrečių ir įvertinamų veiksmų, kad įgyvendintų ES priemonių rinkinio išvadose rekomenduotas pagrindines priemones;

- **iki 2020 m. birželio 30 d.** TIS bendradarbiavimo grupėje, remiant Komisijai ir ENISA, parengti šių pagrindinių priemonių įgyvendinimo kiekvienoje valstybėje narėje pažangos ataskaitą, grindžiamą reguliariomis ataskaitomis ir stebėsena, visų pirma vykdyta TIS bendradarbiavimo grupėje.

5.1. Rizika grindžiamas suderintas požiūris į 5G ryšio tiekėjus

Atsižvelgusios į svarbiausią uždavinį – užtikrinti 5G tinklų saugumą, atsparumą ir tvarumą, valstybės narės susitarė, kad būtina įvertinti atskirų tiekėjų rizikos profilį ir, remiantis tuo vertinimu, taikyti atitinkamus apribojimus, be kita ko, veiksmingo rizikos mažinimo tikslu būtinus draudimus, tiekėjams, kurie vertinami kaip keliantys didelę riziką pagrindiniams objektams, kaip nurodyta priemonių rinkinyje. Komisija yra pasirengusi padėti valstybėms narėms šias priemones įgyvendinti.

Kad ES koordinuotą rizikos vertinimą ir ES priemonių rinkinį visoje Sąjungoje įgyvendinti būtų lengviau, abiejuose dokumentuose pateikiamos gairės dėl 1) tiekėjų rizikos profilio vertinimo[17] ir (2) tinklo elementų ir funkcijų[18] bei kito turto jautrumo. Tiek ES koordinuotame rizikos vertinime, tiek priemonių rinkinyje nustatytos priemonės yra skirtos 5G tinklo įrangos ir tinklo paslaugų tiekėjų keliamai rizikai valdyti. Šios priemonės netaikomos kitiems produktams ar paslaugoms, kurias šie ar kiti tiekėjai gali siūlyti.

Kaip nustatyta ES koordinuoto rizikos vertinimo 2 dalies 37 punkte, atskirų tiekėjų rizikos profiliai gali būti vertinami pagal kelis veiksnius.

Tiekėjų rizikos profilių vertinimas turėtų būti vykdomas vien saugumo sumetimais ir remiantis objektyviais kriterijais. Kad būtų lengviau suformuoti koordinuotą požiūrį į šių priemonių įgyvendinimą, priemonių rinkinyje valstybėms narėms rekomenduojama keistis informacija apie nacionalinius metodus ir geriausią praktiką. Be to, Komisijos nuomone, ši veikla turėtų būti vienas iš pirmųjų tolesnio TIS bendradarbiavimo grupės darbo bendradarbiaujant su Komisija ir ENISA etapo prioritetų.

Labai svarbu apribojimus tiekėjams, kurie vertinami kaip keliantys didelę riziką, be kita ko, veiksmingo rizikos mažinimo tikslu būtinus draudimus, ir priemones priklausomybei nuo šių tiekėjų išvengti taikyti laiku. Tai atlikus ankstyviausiame etape ir, kai įmanoma, 5G dažnių licencijavimo proceso metu taip pat padidės nuspėjamumas rinkos dalyviams, lemsiantis spartų 5G tinklų diegimą, ir bus užtikrintas 5G tinklų saugumas bei 5G tiekimo grandinės atsparumas.

Kartu šių priemonių įgyvendinimo nacionaliniu lygmeniu tvarkaraščiai gali skirtis, kai tai būtina ir pagrįsta, visų pirma atvejais, kai esama didelės priklausomybės nuo įrangos ar paslaugų, kurias tiekia ar teikia tiekėjai, vertinami kaip keliantys didelę riziką (pvz., atsižvelgiant į įrangos atnaujinimo ciklus, visų pirma perėjimą nuo neautonominių prie autonominių 5G tinklų). Valstybės narės galėtų apsvarstyti galimybę parengti įgyvendinimo planus, kuriuose atitinkamiems tinklo operatoriams būtų numatyti derami pereinamieji laikotarpiai. Šiomis aplinkybėmis pereinamuosius laikotarpius reikėtų nustatyti taip, kad būtų išlaikytos ar net padidintos paskatos investuoti į modernią tinklo įrangą, be kita ko, paspartinant visaverčių (autonominių) 5G pagrindinių tinklų diegimą ir pakeičiant esamą 4G įrangą kitose tinklų dalyse (pvz., radijo prieigos tinkle) pagal kitus 5G veiksmų plano[19] tikslus.

Be to, dėl 5G programine įranga grindžiamų tinklų sudėtingumo telekomunikacijų operatoriai gali ne tik trečiųjų šalių subjektams pavesti tiekti tinklo įrangą, bet ir iš esmės jais kliautis prireikus atlikti tam tikras užduotis, kaip antai 5G tinklų ir programinės įrangos priežiūrą ir atnaujinimą, ir teikti kitas užsakomąsias paslaugas. Kaip aprašyta ES koordinuotame rizikos vertinime, tai kelia rimtą saugumo riziką. Todėl šiam aspektui reikėtų skirti ypatingą dėmesį. Taigi būtina atlikti išsamų teikėjų, kuriems pavesta teikti šias paslaugas, rizikos profilio saugumo vertinimą, visų pirma atvejais, kai šios užduotys atliekamos už ES ribų. Siekiant užtikrinti ilgalaikį 5G infrastruktūros vientisumą, reikėtų imtis tinkamų priemonių, be kita ko,

[17] ES koordinuoto rizikos vertinimo 2 dalies 37 punktas.

[18] ES koordinuoto rizikos vertinimo 2 dalies 21 punkte nurodomos pagrindinės elementų ir funkcijų kategorijos ir bendras jų jautrumo lygis, taip pat išvardijami keli pagrindiniai elementai, kuriuos kiekvienai kategorijai nustatė valstybės narės, o 2 dalies 28 ir 29 punktuose nustatomos kelios kitos pažeidžiamiausių objektų ar sričių rūšys (pvz., specialūs subjektai ar geografinės vietovės).

[19] COM(2016) 588, 2016 m. rugsėjo 14 d., Europos 5G veiksmų planas.

didelės rizikos subjektams taikyti apribojimus, visų pirma jautriose 5G tinklų dalyse, arba būtinus draudimus pagal rinkinyje numatytas rizikos mažinimo priemones.

5.2. Komisijos vaidmuo remiant rinkinio priemonių įgyvendinimą

Komisija toliau apskritai rems ES požiūrio į 5G kibernetinį saugumą diegimą, o atvejais, kai galės užtikrinti pridėtinę vertę, imsis konkrečių iniciatyvų, susijusių su rinkinio priemonėmis ir tikslais. Komisija visapusiškai naudosis savo kompetencija ir atitinkamomis priemonėmis tiek, kiek tai bus būtina nustatytoms saugumo problemoms spręsti. Tiek veikdama viena, tiek kartu su valstybėmis narėmis ir privačiuoju sektoriumi Komisija siekia remti strategines priemones, padėsiančias užtikrinti ES technologinį suverenumą ir lyderystę ateityje plėtojant tinklų technologijas, kibernetinio saugumo technologijas ir visas susijusias sudedamąsias dalis, nuo kurių priklauso visa mūsų ekonomika ir saugumas.

Kalbant konkrečiau, siekdama užtikrinti rinkinyje numatytų atitinkamų rizikos mažinimo priemonių įgyvendinimą, savo kompetencijos srityse Komisija imsis šių veiksmų:

5G tinklų kibernetinio saugumo ir diversifikuotos 5G vertės grandinės užtikrinimas:

- **bendradarbiavimas kibernetinio saugumo klausimais**: per TIS bendradarbiavimo grupę toliau teiks paramą valstybėms narėms, kad nacionalinių priemonių įgyvendinimas vyktų veiksmingai, koordinuotai ir laiku;

- **telekomunikacijų ir kibernetinio saugumo taisyklės**: teiks paramą su saugumo reikalavimais susijusių rinkinio priemonių įgyvendinimui, ypač kiek tai bus susiję su atitinkamomis Europos elektroninių ryšių taisyklių nuostatomis, ir apsvarstys galimų įgyvendinimo aktų, kuriais nustatomos techninės ir organizacinės saugumo priemonės siekiant papildyti nacionalines taisykles ir padidinti operatoriams taikomų saugumo priemonių veiksmingumą ir nuoseklumą, pridėtinę vertę;

- **standartų nustatymas**: imsis veiksmų, kad padėtų palaikyti ir prireikus padidinti Europos dalyvavimą atitinkamų standartizacijos institucijų veikloje siekiant Europos saugumo ir sąveikumo tikslų. Visų pirma Komisija kartu su valstybėmis narėmis vertins ir skatins naudoti technines specifikacijas ir standartus, sudarančius sąlygas 5G įrangos tiekėjų sąveikai įvairiose tinklo dalyse, įskaitant senuosius tinklus, kad, pavyzdžiui, skatindama atviras sąveikias sąsajas, padėtų užtikrinti realią pardavėjų įvairovę;

- **sertifikavimas**: rems 5G sertifikavimo schemų, kuriomis atsižvelgiama į 5G tinklų poreikius pagal ES kibernetinio saugumo sertifikavimo sistemą, rengimą;

- **tiesioginių užsienio investicijų (TUI) atrankinė patikra**: rems ES atrankinės patikros sistemos įgyvendinimą, nustatydama 5G vertės grandinę, įskaitant jautrius tinklo objektus, ir vykdydama reguliarų TUI stebėjimą visoje vertės grandinėje. Laikydamasi TUI atrankinės patikros tvarkaraščio (nuo 2020 m. spalio mėn.) Komisija nagrinės užsienio investicijas į 5G sritį pagal Reglamente (ES) 2019/452 nustatytas gaires, atsižvelgdama į ES koordinuotą rizikos vertinimą ir ES priemonių rinkinį;

- **prekybos apsaugos priemonės**: stebės visus susijusius rinkos pokyčius ES ir trečiosiose valstybėse ir gins ES veiklos vykdytojus Europos 5G rinkoje prekybos apsaugos priemonėmis, kad būtų išvengta galimos prekybą iškreipiančios praktikos (dempingo arba subsidijavimo), be kita ko, prireikus atliks preliminarius tyrimus;

- **konkurencijos taisyklės:** stebės 5G aparatinės ir programinės įrangos tiekimo rinkų veikimą, kad užtikrintų jų konkurencinius rezultatus, be kita ko, atsižvelgiant į galimus sutartinio ar techninio susaistymo atvejus;

- **ES finansavimo programos**: užtikrins, kad dalyvauti atitinkamų technologijų sričių ES finansavimo programose būtų galima tik su sąlyga, kad laikomasi saugumo reikalavimų, visapusiškai taikydama ir toliau įgyvendindama mokslinių tyrimų ir inovacijų programų saugumo sąlygas, visų pirma kalbant apie programą „Europos horizontas“, Skaitmeninės Europos programą, 2-ąją Europos infrastruktūros tinklų priemonę, Europos struktūrinius ir investicijų fondus ir kitas atitinkamas programas. Panašus požiūris turėtų būti taikomas ir ES išorės finansavimo programoms ir finansinėms priemonėms, be kita ko, tarptautinių finansų įstaigų teikiamam finansavimui;

- **viešieji pirkimai:** darys sverto poveikį 5G tinklų srities viešiesiems pirkimams, siekdama padėti pasiekti nustatytus 5G tinklų saugumo tikslus, tiekėjų įvairovę ir ilgalaikį tvarumą; visų pirma sieks užtikrinti deramą dėmesį saugumo aspektams pasirašant viešųjų pirkimų sutartis, susijusias su 5G tinklais, laikantis ES viešųjų pirkimų taisyklių;

- **reagavimas į incidentus ir krizių valdymas (projektas) ir kibernetinės pratybos**: visapusiškai pasinaudos rengiamo ES koordinuoto atsako į didelio masto kibernetinio saugumo incidentus projekto[20] teikiama nauda. Be to, kartu su ENISA apsvarstys galimybę surengti 5G kibernetines pratybas, kai tik leis rinkos branda.

Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai ir Komisijos pirmininko pavaduotojo, taip pat Tarybos atsakomybe:

- **Bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistema („Kibernetinio saugumo diplomatijos priemonių rinkinys“)**[21]: kibernetinės kenkimo veiklos, keliančios pavojų ES vientisumui ir saugumui, atveju valstybės narės raginamos naudotis atitinkamomis bendros užsienio ir saugumo politikos priemonėmis, įtrauktomis į ES Kibernetinio saugumo diplomatijos priemonių rinkinį (prireikus ir ribojamosiomis priemonėmis), kad paskatintų bendradarbiavimą, padėtų mažinti grėsmes ir darytų įtaką potencialių agresorių elgesiui.

Be to, keliomis programomis skatinant diversifikuotą ir tvarią 5G ryšio rinką, be kita ko, išlaikant ES pajėgumus 5G vertės grandinėje ir investuojant į inovacijas pagal ES tarptautinius įsipareigojimus, bus padedama siekti tikslų išvengti ilgalaikės priklausomybės rizikos arba ją sumažinti.

Inovacijų ir investicijų į kibernetinį saugumą bei tinklo infrastruktūros technologijas skatinimas:

- ES finansavimo **programos**: didinti investicijas į mokslinius tyrimus, inovacijas ir tinklo technologijų bei atitinkamų sudedamųjų dalių diegimą. Iš kito ES biudžeto (2021–2027 m.) Komisija yra pasiūliusi beveik 3 mlrd. EUR skirti investicijoms į kibernetinio saugumo technologijas. Iš šių lėšų pagal programą „Europos horizontas“ bus finansuojami moksliniai tyrimai bei inovacijos, o pagal Skaitmeninės Europos programą teikiama parama kibernetinio

[20] Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.
[21] 2017 m. lapkričio 20 d. Tarybos išvados 9916/17.

saugumo pajėgumams. Finansinė parama 5G srities moksliniams tyrimams ir plėtrai, taip pat 5G tinklų diegimui gali būti teikiama ir pagal programą „InvestEU“.

Be to, Komisija yra pasiūliusi kitu programos „Europos horizontas“[22] etapu kartu su pramone įsteigti su valstybėmis narėmis koordinuojamą ES institucionalizuotą pažangiųjų tinklų ir paslaugų srities partnerystę (NGI/6G) siekiant užbaigti diegti 5G tinklus ir iš esmės **pasirengti 6G** – tolesnės kartos judriojo ryšio technologijos – diegimui. Šiai iniciatyvai iš ES biudžeto (2021–2027 m.) skiriama daugiau nei 2,5 mlrd. EUR ES investicijų suma siekiama pritraukti bent 7,5 mlrd. EUR privačiųjų investicijų.

- **Pramonės plėtra ir diegimas**: visoje 5G vertės grandinėje įvertinti galimas rinkos spragas ar nepakankamumą, dėl kurių būtų pateisinama imtis tikslinių intervencijų pagal kitą ilgalaikį biudžetą arba įgyvendinti galimus bendriems Europos interesams svarbius projektus (BEISP), susijusius su kibernetiniu saugumu, vadovaujantis BEISP aukšto lygio forumo pasiūlymais. Sprendimą dėl BEISP rengimo ir struktūros turi priimti valstybės narės ir įmonės. Pagal ES taisykles numatoma sukurti palankią sistemą, o Komisija yra pasirengusi sudaryti palankesnes sąlygas būtinoms sutartims ir teikti gaires.

6. Išvada

5G tinklai turėtų pasiūlyti įvairių galimybių Europos piliečiams, visuomenei ir ekonomikai. Todėl labai svarbu užtikrinti 5G tinklų saugumą ir atsparumą. Kartu su didėjančia priklausomybe nuo technologijų ir duomenų kelia rūpesčių kintančios kibernetinės grėsmės (be kita ko, ne ES valstybių ar jų remiamų subjektų kišimosi rizika). Neskiriant dėmesio kibernetiniam saugumui būtų pakirstas pasitikėjimas skaitmeninės ekonomikos ir visuomenės plėtra, o Europos Sąjungai užkirstas kelias visapusiškai pasinaudoti jos teikiama nauda. Tam būtinas atitinkamai lankstus ir griežtas atsakas.

Koordinuotas ir nuoseklus požiūris į ypatingos svarbos technologijų ir tinklų kibernetinį saugumą ES yra būtinas Europos Sąjungai, kad ji galėtų užtikrinti savo technologinį suverenumą, išlaikyti ir plėtoti pramonės pajėgumus. Komisija visapusiškai rems ES požiūrio į 5G tinklų kibernetinį saugumą įgyvendinimą ir kartu užtikrins, kad ES rinkos išliktų atviros produktams ir paslaugoms, atitinkantiems kintančius kibernetinio saugumo ir pasitikėjimo reikalavimus.

Todėl svarbu, kad visų suinteresuotųjų subjektų įsipareigojimas dėl 5G saugumo išliktų tvirtas, o valstybės narės, Komisija ir ENISA nuolatos bendradarbiautų.

Kaip nurodyta pirmiau, Komisija ragina valstybes nares neatidėliotinai imtis skubių veiksmų siekiant veiksmingai ir objektyviai įgyvendinti į rinkinį įtrauktas suderintas priemones ir toliau bendradarbiauti, remiant Komisijai ir ENISA, kad būtų užtikrintas ES lygmens koordinavimas. Tuo tarpu Komisija pradės vykdyti visus atitinkamus veiksmus pagal savo kompetenciją, kad valstybėms narėms padėtų įgyvendinti rinkinio priemones ir sustiprintų jų poveikį.

[22] Finansavimas gali būti teikiamas ir pagal 2-ąją Europos infrastruktūros tinklų priemonę bei Skaitmeninės Europos programą.

Priedas. Rizikos kategorijos (šaltinis: ES koordinuotas rizikos vertinimas)

	Rizikos kategorijos
Su nepakankamomis saugumo priemonėmis susiję rizikos scenarijai	*R1 – klaidingas tinklų konfigūravimas*
	R2 – prieigos kontrolės trūkumas
Su 5G tiekimo grandine susiję rizikos scenarijai	*R3 – prasta produktų kokybė*
	R4 – priklausomybė nuo vienintelio tiekėjo atskiruose tinkluose arba nepakankama jų įvairovė nacionaliniu lygmeniu
Su pagrindinių priešiškų subjektų modus operandi susiję rizikos scenarijai	*R5 – valstybės kišimasis naudojantis 5G tiekimo grandine*
	R6 – organizuoto nusikalstamumo grupuočių arba nusikalstamų organizacijų veikla pasinaudojant 5G tinklais, nukreipta prieš galutinius naudotojus
Su 5G tinklų ir kitų ypatingos svarbos sistemų tarpusavio priklausomybe susiję rizikos scenarijai	*R7 – didelis ypatingos svarbos infrastruktūros objektų ar paslaugų sutrikdymas*
	R8 – visiškas tinklų gedimas dėl elektros energijos tiekimo nutrūkimo ar kitų pagalbinių sistemų sustojimo
Su galutinių naudotojų įrenginiais susiję rizikos scenarijai	*R9 – daiktų interneto išnaudojimas*