Europos Sąjungos
Taryba

Briuselis, 2020 m. gruodžio 16 d.
(OR. en)

14133/20

Tarpinstitucinė byla:
2020/0305(NLE)

CYBER 280	**RECH 529**
JAI 1118	**COMPET 642**
JAIEX 121	**IND 273**
EJUSTICE 107	**COTER 115**
COSI 254	**ENFOPOL 350**
DATAPROTECT 154	**COPS 485**
COPEN 387	**MI 578**
TELECOM 269	**IXIM 139**
PROCIV 99	**POLMIL 201**
CSC 367	**HYBRID 48**
CIS 65	**CSCI 96**
RELEX 1019	**POLGEN 234**

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2020 m. gruodžio 16 d.
kam:	Europos Sąjungos Tarybos generaliniam sekretoriui Jeppe TRANHOLMUI-MIKKELSENUI
Komisijos dok. Nr.:	JOIN(2020) 18 final
Dalykas:	BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI. Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija

Delegacijoms pridedamas dokumentas JOIN(2020) 18 final.

Pridedama: JOIN(2020) 18 final

EUROPOS
KOMISIJA

SĄJUNGOS VYRIAUSIASIS
ĮGALIOTINIS UŽSIENIO
REIKALAMS IR
SAUGUMO POLITIKAI

Briuselis, 2020 12 16
JOIN(2020) 18 final

BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI

Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija

BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI

Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija

I. ĮVADAS. SAUGI KIBERNETINĖ SKAITMENINĖ TRANSFORMACIJA SUDĖTINGOJE GRĖSMIŲ APLINKOJE

Kibernetinis saugumas yra neatsiejama europiečių saugumo dalis. Nesvarbu, ar kalbama apie susietųjų įrenginių, elektros tinklų, ar bankų, orlaivių, viešojo administravimo institucijų arba ligoninių, kuriomis jie rečiau ar dažniau naudojasi, saugumą, žmonės turi teisę būti užtikrinti, kad bus apsaugoti nuo kibernetinių grėsmių. ES ekonomika, demokratija ir visuomenė labiau nei bet kada priklauso nuo saugių ir patikimų skaitmeninių priemonių ir ryšio. Todėl kibernetinis saugumas yra labai svarbus kuriant atsparią, žalią ir skaitmeninę Europą.

Transporto, energetikos ir sveikatos, telekomunikacijų, finansų, saugumo, demokratinių procesų, kosmoso ir gynybos sritys yra labai priklausomos nuo vis labiau tarpusavyje susijusių tinklų ir informacinių sistemų. Tarpsektorinė tarpusavio priklausomybė yra labai didelė, nes tinklai ir informacinės sistemos savo ruožtu priklauso nuo stabilaus elektros energijos tiekimo, kad galėtų veikti. Susietųjų įrenginių planetoje jau yra daugiau nei žmonių, ir prognozuojama, kad iki 2025 m. jų skaičius padidės iki 25 mlrd.[1] – ketvirtadalis šių prietaisų bus Europoje. Dėl COVID-19 pandemijos, per kurią 40 proc. ES darbuotojų pradėjo dirbti nuotoliniu būdu, paspartėjo darbo modelių skaitmeninimas ir tai greičiausiai turės ilgalaikį poveikį kasdieniam gyvenimui[2]. Dėl šios priežasties didėja pažeidžiamumas kibernetiniams išpuoliams[3]. Vartotojui dažnai pristatomi susietieji produktai, kurių pažeidžiamumai yra žinomi, taip dar labiau išplečiant išpuolių, susijusių su kibernetine kenkimo veikla, perimetrą[4]. ES pramonės aplinka vis labiau skaitmeninama ir sujungiama; tai taip pat reiškia, kad kibernetiniai išpuoliai pramonės šakoms ir ekosistemoms gali daryti daug didesnį poveikį nei kada nors anksčiau.

Grėsmių padėtį sunkina geopolitinė įtampa dėl pasaulinio atvirojo interneto ir technologijų kontrolės visoje tiekimo grandinėje[5]. Šią įtampą atspindi didėjantis tautinių

[1] Telekomunikacijų prekybos asociacijos GSMA vertinimu; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf. Remiantis Tarptautinės duomenų korporacijos prognozėmis, susietųjų mašinų, jutiklių ir kamerų bus 42,6 mlrd.; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Remiantis 2020 m. birželio mėn. atlikto tyrimo duomenimis, 47 proc. įmonių vadovų teigė ketinantys suteikti darbuotojams galimybę dirbti visą darbo dieną nuotoliniu būdu, net ir atsiradus galimybei grįžti į darbo vietą; 82 proc. įmonių vadovų ketino leisti dirbti nuotoliniu būdu bent dalį darbo laiko; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

[4] Viena iš didžiausią žalą iki šiol sukėlusių kenkimo programinių įrangų „Mirai“ sukūrė daugiau kaip 600 000 prietaisų botnetus, sutrikdžiusius daugelį pagrindinių interneto svetainių Europoje ir Jungtinėse Amerikos Valstijose.

[5] Įskaitant elektroninius elementus, duomenų analitiką, debesiją, greitesnius ir pažangesnius 5G ir naujesnius tinklus, šifravimą, dirbtinį intelektą (DI) ir naujas kompiuterines bei patikimo duomenų tvarkymo paradigmas, tokias kaip blokų grandinė, debesijos–tinklo paribio sprendimai ir kvantinė kompiuterija.

valstybių, statančių skaitmenines sienas, skaičius. Apribojimai nustatomi internetui ir internete, todėl kyla grėsmė pasaulinei ir atvirai kibernetinei erdvei, taip pat teisinės valstybės principui, pagrindinėms teisėms, laisvei ir demokratijai, t. y. esminėms ES vertybėms. Kibernetinė erdvė vis dažniau naudojama politiniais ir ideologiniais tikslais, o didėjanti poliarizacija tarptautiniu lygmeniu trukdo užtikrinti veiksmingą daugiašališkumą. Hibridinės grėsmės apima dezinformacijos kampanijas ir kibernetinius išpuolius prieš infrastruktūrą, ekonominius procesus ir demokratines institucijas, įskaitant galimybę padaryti fizinę žalą, gauti neteisėtą prieigą prie asmens duomenų, pavogti pramonės ar valstybės paslaptis, sėti nepasitikėjimą ir susilpninti socialinę sanglaudą. Ši veikla kenkia tarptautiniam saugumui ir stabilumui, taip pat privalumams, kuriuos kibernetinė erdvė suteikia ekonominei, socialinei ir politinei plėtrai.

Piktavališki veiksmai, nukreipti į ypatingos svarbos infrastruktūros objektus, kelia didžiulę pasaulinę riziką[6]. Internetas yra decentralizuotos architektūros, be jokios centrinės struktūros, ir nepavaldus įvairių suinteresuotųjų šalių valdžiai. Nors internetas nuolat yra piktavališkų bandymų sutrikdyti veiklą taikinys, sugebėta išlaikyti eksponentinį srauto apimties didėjimą[7]. Tuo pat metu vis labiau pasikliaujama pagrindinėmis pasaulinio atvirojo interneto funkcijomis, pavyzdžiui, domenų vardų sistema (DNS), ir esminėmis ryšių ir prieglobos, taikomųjų programų ir duomenų interneto paslaugomis. Šios paslaugos vis labiau telkiamos kelių privačių bendrovių rankose[8]. Todėl Europos ekonomika ir visuomenė yra neapsaugotos nuo ardomųjų geopolitinių ar techninių įvykių, kurie daro poveikį interneto struktūrai arba vienai ar kelioms iš šių bendrovių. Pandemijos metu dažniau pradėta naudotis internetu ir pasikeitė tokio naudojimo modeliai, todėl dar labiau padidėjo nuo šios skaitmeninės infrastruktūros priklausančių tiekimo grandinių pažeidžiamumas.

Susirūpinimas dėl saugumo yra pagrindinis veiksnys, atgrasantis nuo naudojimosi internetinėmis paslaugomis[9]. Apytiksliai du penktadaliai ES naudotojų patyrė su saugumu susijusių problemų, o trys penktadaliai jaučiasi nepajėgūs apsisaugoti nuo kibernetinių nusikaltimų[10]. Trečdalis naudotojų per pastaruosius trejus metus sulaukė apgaulingų elektroninių laiškų arba skambučių telefonu, kuriais buvo prašoma pateikti asmens duomenų, tačiau 83 proc. niekada nepranešė apie kibernetinius nusikaltimus. Nuo kibernetinių išpuolių nukentėjo kas aštunta įmonė[11]. Daugiau nei pusė įmonių ir vartotojų asmeninių kompiuterių,

---

[6] Pasaulio ekonomikos forumas, 2020 m. pranešimas dėl visuotinių grėsmių.

[7] Pasak Ekonominio bendradarbiavimo ir plėtros organizacijos, per pandemiją interneto srautas padidėjo 60 proc.; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Europos elektroninių ryšių reguliuotojų institucija ir Komisija nuolat skelbia ataskaitas, kuriose apžvelgia interneto pajėgumų statusą koronaviruso izoliavimo priemonių taikymo metu. Remiantis ENISA ataskaita, 2019 m. trečiąjį ketvirtį, palyginti su 2018 m. trečiuoju ketvirčiu, bendras paskirstytojo paslaugos trikdymo (DDoS) atakų skaičius padidėjo 241 proc. DDoS atakų intensyvumas didėja, o didžiausia ataka, įvykdyta 2020 m. vasario mėn., pasiektas didžiausias 2,3 terabito per sekundę srautas. 2020 m. rugpjūčio mėn. dėl „CenturyLink“ atjungimo, t. y. JAV interneto paslaugų teikėjo maršrutizavimo problemos, pasaulinis žiniatinklio srautas sumažėjo 3,5 proc.; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service.

[8] „Interneto draugija“, *The Global Internet Report: Consolidation in the Internet Economy*; https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/.

[9] https://data.europa.eu/euodp/lt/data/dataset/S2249_92_2_499_ENG.

[10] 2020 m. skaitmeninės ekonomikos ir visuomenės indeksas; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/lt/data/dataset/S2249_92_2_499_ENG.

[11] Eurostato pranešimas spaudai „Informacinių ir ryšių technologijų saugumo priemonės, kurių ėmėsi didžioji dauguma ES įmonių“, Nr. 6/2020, 2020 m. sausio 13 d. „Kibernetiniai išpuoliai prieš ypatingos svarbos

kurie vieną kartą buvo užkrėsti kenkimo programine įranga, yra pakartotinai užkrečiami tais pačiais metais[12]. Dėl duomenų saugumo pažeidimų kasmet prarandama šimtai milijonų apskaitos įrašų; 2018 m. vienos įmonės dėl pažeidimo patiriamos vidutinės išlaidos padidėjo iki daugiau nei 3,5 mln. EUR[13]. Kibernetinio išpuolio poveikis dažnai negali būti izoliuotas ir gali sukelti grandininę reakciją visoje ekonomikoje ir visuomenėje, nuo kurios nukenčia milijonai asmenų[14].

Beveik visų rūšių nusikaltimų tyrimas yra susijęs su skaitmeniniu aspektu. 2019 m. pranešta, kad kasmet incidentų skaičius trigubėjo. Priskaičiuota 700 mln. naujų kenkimo programinės įrangos, kuri dažniausiai naudojama kibernetiniam išpuoliui vykdyti, pavyzdžių[15]. Apskaičiuota, kad 2020 m. su kibernetiniais nusikaltimais susijusios metinės išlaidos pasaulio ekonomikai sudarys 5,5 trln. EUR, t. y. dvigubai daugiau nei 2015 m.[16] Tai yra didžiausias ekonominės gerovės perdavimas istorijoje, viršijantis pasaulinę prekybą narkotikais. Apskaičiuota, kad dėl vieno didelio incidento, t. y. 2017 m. išpuolio naudojant išpirkos reikalavimo programinę įrangą „WannaCry“, išlaidos pasaulio ekonomikai sudarė daugiau kaip 6,5 mlrd. EUR[17].

Skaitmeninės paslaugos ir finansų sektorius kartu su viešuoju sektoriumi ir gamyba, yra vieni iš dažniausių kibernetinių išpuolių taikinių, tačiau įmonių ir asmenų kibernetinė parengtis ir informuotumas tebėra menki[18], o kibernetinio saugumo įgūdžių darbo rinkoje labai trūksta[19]. 2019 m. įvyko beveik 450 kibernetinio saugumo incidentų, susijusių su Europos ypatingos svarbos infrastruktūros objektais, pavyzdžiui, finansų ir energetikos sektoriuose[20]. Pandemijos metu ypač stipriai nukentėjo sveikatos priežiūros organizacijos ir specialistai. Kadangi technologijos tampa neatsiejamos nuo fizinio pasaulio, kibernetiniai išpuoliai kelia pavojų pažeidžiamiausių asmenų gyvybei ir gerovei[21]. Daugiau nei du trečdaliai įmonių, visų pirma MVĮ, kibernetinio saugumo srityje laikomos naujokėmis, o Europos įmonės, manoma, yra ne taip gerai pasirengusios kaip Azijos ir Amerikos įmonės[22]. Remiantis skaičiavimais, Europoje trūksta 291 000 kibernetinio saugumo

---

infrastruktūros objektus tapo įprasti tokiuose sektoriuose kaip energetika, sveikatos priežiūra ir transportas“; Pasaulio ekonomikos forumas, 2020 m. pranešimas dėl visuotinių grėsmių.

[12] Šaltinis: „Comparitech“.

[13] Metinė išlaidų dėl duomenų pažeidimų ataskaita, 2020 m., „Ponemon Institute“, ir 524 neseniai padarytų pažeidimų 17-oje geografinių vietovių ir 17-oje pramonės šakų kiekybinė analizė; https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

[14] Jungtinio tyrimų centro (JRC) ataskaita „Kibernetinis saugumas, mūsų skaitmeninis ramstis“ (angl. *Cybersecurity, our digital anchor*); https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor.

[15] Šaltinis: „AV-TEST“, https://www.av-test.org/en/statistics/malware/.

[16] JRC, „Kibernetinis saugumas – mūsų skaitmeninis ramstis“.

[17] Šaltinis: „Cyence“.

[18] Įmonių, ypač MVĮ, informuotumas apie kibernetines komercinių paslapčių vagystes taip pat tebėra žemas; „PwC“ atliktas tyrimas „Pramoninio šnipinėjimo ir komercinių paslapčių vagysčių naudojant kibernetines priemones mastas ir poveikis“, 2018 m.

[19] Žr. ENISA, 2020 m. grėsmių padėtis. Taip pat žr. „Verizon“ 2020 m. duomenų pažeidimo tyrimų ataskaitą; https://enterprise.verizon.com/resources/reports/dbir/.

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f.

[21] Išpirkos reikalavimo programinė įranga naudota išpuoliams prieš ligonines ir medicinos dokumentus, pavyzdžiui, Rumunijoje (2020 m. birželio mėn.), Diuseldorfe (2020 m. rugsėjo mėn.) ir psichoterapijos klinikoje „Vastaamo“ (2020 m. spalio mėn.).

[22] „PwC“, *The Global State of Information Security 2018*; „ESI Thoughtlab“, *The Cybersecurity Imperative*, 2019 m.

specialistų. Kibernetinio saugumo ekspertų įdarbinimas ir mokymas yra lėtas procesas, dėl kurio organizacijoms kyla didesnė kibernetinio saugumo rizika[23].

ES trūksta kolektyvinio informuotumo apie kibernetinių grėsmių padėtį. Taip yra todėl, kad nacionalinės institucijos sistemingai nerenka informacijos, kurią, pavyzdžiui, turi privatusis sektorius ir kuri galėtų padėti įvertinti kibernetinio saugumo padėtį ES, ir ja nesidalija. Valstybės narės praneša tik apie dalį incidentų, o informacija nesidalijama nei sistemingai, nei visapusiškai[24]; be to, kibernetiniai išpuoliai gali būti tik vienas suderintų piktavališkų išpuolių prieš Europos visuomenę aspektas. Dabar valstybės narės viena kitai teikia tik ribotą savitarpio operatyvinę pagalbą, o didelio masto tarpvalstybinių kibernetinių incidentų ar krizių atvejams valstybės narės ir ES institucijos, agentūros ir įstaigos neturi jokių operatyvinių mechanizmų[25].

Todėl labai svarbu didinti kibernetinį saugumą, kad žmonės pasitikėtų inovacijomis, ryšiu ir automatizavimu, galėtų jais naudotis ir gauti iš jų naudos ir kad būtų apsaugotos pagrindinės teisės ir laisvės, įskaitant teisę į privatumą ir asmens duomenų apsaugą, žodžio ir informacijos laisvę. Kibernetinis saugumas yra būtinas tinklo junglumui ir pasauliniam atvirajam internetui, kuriuo turi būti grindžiama ekonomikos ir visuomenės pertvarka XXI a. 3-ame dešimtmetyje. Kibernetinis saugumas padeda kurti daugiau ir geresnių darbo vietų, didinti darbo sąlygų lankstumą, siekti veiksmingesnio ir darnesnio transporto ir ūkininkavimo, lengviau ir sąžiningesnėmis sąlygomis naudotis sveikatos priežiūros paslaugomis. Jis taip pat labai svarbus pereinant prie švaresnės energijos, kaip numatyta Europos žaliajame kurse[26], tam pasitelkiant tarpvalstybinius tinklus ir pažangiuosius skaitiklius ir vengiant nereikalingo duomenų saugojimo dubliavimo. Galiausiai kibernetinis saugumas yra būtinas tarptautiniam saugumui ir stabilumui užtikrinti, taip pat ekonomikos, demokratijos ir visuomenės vystymuisi visame pasaulyje. Todėl vyriausybės, įmonės ir asmenys skaitmeninės priemones privalo naudoti atsakingai ir saugiai. Kibernetinis sąmoningumas ir higiena turi būti kasdienio gyvenimo skaitmeninės transformacijos pagrindas.

Nauja ES skaitmeninio dešimtmečio kibernetinio saugumo strategija yra vienas pagrindinių Europos skaitmeninės ateities formavimo[27], Komisijos Europos ekonomikos gaivinimo plano[28], 2020–2025 m. saugumo sąjungos strategijos[29], Visuotinės ES užsienio ir saugumo politikos strategijos[30] ir Europos Vadovų Tarybos 2019–2024 m. strateginės darbotvarkės[31] elementų. Joje išdėstyta, kaip ES apsaugos savo gyventojus, įmones ir institucijas nuo kibernetinių grėsmių, kaip skatins tarptautinį bendradarbiavimą ir imsis iniciatyvos užtikrinti pasaulinį atvirąjį internetą.

---

[23] ES kibernetinio saugumo agentūra, „Kibernetinio saugumo įgūdžių ugdymas ES. Kibernetinio saugumo laipsnių sertifikavimas ir ENISA aukštojo mokslo duomenų bazė“ (angl. *Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database*), 2019 m. gruodžio mėn.

[24] Valstybės narės pagal Direktyvos dėl tinklų ir informacinių sistemų saugumo (Direktyva (ES) 2016/1148) 10 straipsnio 3 dalį TIS bendradarbiavimo grupei privalo pateikti metinę suvestinę ataskaitą apie gautus pranešimus.

[25] CSIRT tinklo narių savitarpio pagalbai taikomos standartinės veiklos procedūros.

[26] Europos žaliasis kursas, COM(2019) 640 *final*.

[27] Europos skaitmeninės ateities formavimas, COM(2020) 67 *final*.

[28] Proga Europai atsigauti ir paruošti dirvą naujai kartai, COM(2020) 98 *final*.

[29] 2020–2025 m. ES saugumo sąjungos strategija, COM(2020) 605 *final*.

[30] https://eeas.europa.eu/topics/eu-global-strategy_en.

[31] https://www.consilium.europa.eu/lt/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/.

II. MĄSTYTI GLOBALIAI, VEIKTI EUROPOS MASTU

Šia strategija siekiama užtikrinti pasaulinį atvirąjį internetą, aprūpintą veiksmingomis apsaugos priemonėmis rizikai, gresiančiai Europos gyventojų saugumui ir pagrindinėms teisėms bei laisvėms, šalinti. Atsižvelgiant į pažangą, padarytą įgyvendinant ankstesnes strategijas, joje pateikiami konkretūs pasiūlymai pasitelkti **tris pagrindines – reguliavimo, investavimo ir politines – priemones**, kurias įgyvendinant būtų imamasi **ES veiksmų trijose srityse: 1) atsparumo, technologinio suverenumo ir lyderystės, 2) veiklos pajėgumų, susijusių su prevencija, atgrasymu ir reagavimu, kūrimo ir 3) pasaulinės atviros kibernetinės erdvės plėtojimo**. Įgyvendindama naują technologijų ir pramonės politikos ir ekonomikos gaivinimo darbotvarkę, ES yra įsipareigojusi remti šią strategiją **per ateinančius septynerius metus skirdama precedento neturinčias investicijas į ES skaitmeninę pertvarką**, galbūt keturis kartus viršijančias ankstesnes investicijas[32].

Kibernetinio saugumo aspektą, naudojant paskatas, įsipareigojimus ir lyginamuosius standartus, būtina integruoti į visas šias skaitmenines investicijas, ypač į tokias pagrindines technologijas kaip dirbtinis intelektas (DI), šifravimas ir kvantinė kompiuterija. Šios investicijos gali paskatinti Europos kibernetinio saugumo sektoriaus augimą ir suteikti tikrumo, kurio reikia siekiant palengvinti laipsnišką senųjų sistemų atsisakymą. Europos gynybos fondas (EGF) rems Europos kibernetinės gynybos sprendimus, kurie yra Europos gynybos technologinės ir pramoninės bazės dalis. Kibernetinis saugumas įtrauktas į išorės finansavimo priemones, skirtas mūsų partneriams remti, visų pirma į Kaimynystės, vystomojo ir tarptautinio bendradarbiavimo priemonę. Netinkamo technologijų naudojimo prevencija, ypatingos svarbos infrastruktūros apsauga ir tiekimo grandinių vientisumo užtikrinimas taip pat sudaro sąlygas ES laikytis JT normų, taisyklių ir atsakingo valstybių elgesio principų[33].

1. ATSPARUMAS, TECHNOLOGINIS SUVERENUMAS IR LYDERYSTĖ

ES ypatingos svarbos infrastruktūros objektai ir esminės paslaugos tampa vis labiau tarpusavyje susiję ir skaitmeninami. Visi prie interneto prijungti daiktai ES, nesvarbu, ar tai būtų automatizuoti automobiliai, pramonės kontrolės sistemos ar buitinė technika, ir visos tiekimo grandinės, kuriomis jie pristatomi, turi būti saugaus dizaino, atsparūs kibernetiniams incidentams ir greitai pataisomi nustačius pažeidžiamumus. Tai labai svarbu siekiant ES privačiajam ir viešajam sektoriams suteikti galimybę rinktis iš saugiausių infrastruktūrų ir paslaugų. Ateinantis dešimtmetis – tai galimybė ES pirmauti kuriant saugias technologijas visoje tiekimo grandinėje. Siekiant užtikrinti atsparumą ir didesnius pramonės ir technologinius pajėgumus kibernetinio saugumo srityje, turėtų būti sutelktos visos būtinos reguliavimo, investavimo ir politikos priemonės. Projektavimo metu užtikrinus pramoninių procesų, operacijų ir prietaisų kibernetinį saugumą galima sušvelninti riziką, potencialiai sumažinti įmonių ir plačiosios visuomenės išlaidas ir taip padidinti atsparumą.

[32] Investicijos į visą skaitmeninių technologijų tiekimo grandinę, kuriomis prisidedama prie skaitmeninės pertvarkos arba su tuo susijusių problemų sprendimo, turėtų sudaryti bent 20 proc. – t. y. 134,5 mlrd. EUR – iš 672,5 mlrd. EUR vertės ekonomikos gaivinimo ir atsparumo didinimo priemonės, kurią sudaro dotacijos ir paskolos. ES finansavimas, kuris 2021–2027 m. daugiametėje finansinėje programoje yra numatytas kibernetiniam saugumui pagal Skaitmeninės Europos programą ir kibernetinio saugumo moksliniams tyrimams pagal programą „Europos horizontas“, ypatingą dėmesį skiriant paramai MVĮ, galėtų iš viso siekti 2 mlrd. EUR, prie kurių taip pat reikėtų pridėti valstybių narių ir pramonės sektoriaus investicijas.

[33] https://undocs.org/A/70/174.

1.1. Atspari infrastruktūra ir ypatingos svarbos paslaugos

ES **tinklų ir informacinių sistemų (TIS) saugumo taisyklės** yra bendrosios kibernetinio saugumo rinkos pagrindas. Komisija siūlo pertvarkyti šias taisykles pagal peržiūrėtą TIS direktyvą, kad būtų padidintas **visų susijusių viešojo ir privačiojo sektorių, kurie ekonomikoje ir visuomenėje atlieka svarbią funkciją, kibernetinio atsparumo** lygis[34]. Peržiūra yra būtina, kad būtų sumažinti neatitikimai vidaus rinkoje suderinant taikymo sritį, saugumo ir pranešimo apie incidentus reikalavimus, nacionalinę priežiūrą ir vykdymo užtikrinimą bei kompetentingų institucijų gebėjimus.

Pertvarkyta TIS direktyva bus grindžiamos konkretesnės taisyklės, kurios taip pat yra reikalingos strategiškai svarbiems sektoriams, įskaitant energetikos, transporto ir sveikatos sektorius. Siekiant užtikrinti nuoseklų požiūrį, kaip skelbiama 2020–2025 m. saugumo sąjungos strategijoje, kartu su pertvarkyta direktyva siūloma persvarstyti teisės aktus dėl ypatingos svarbos infrastruktūros objektų atsparumo[35]. Energetikos technologijos, apimančios skaitmeninius elementus, ir susijusių tiekimo grandinių saugumas yra svarbūs esminių paslaugų tęstinumui ir ypatingos svarbos energetikos infrastruktūros strateginei kontrolei. Todėl Komisija pasiūlys priemonių, įskaitant iki 2022 m. pabaigos priimsimą tinklo kodeksą, kuriame bus nustatytos tarpvalstybinių elektros energijos srautų kibernetinio saugumo taisyklės. Finansų sektorius taip pat turi stiprinti skaitmeninės veiklos atsparumą ir užtikrinti gebėjimą atlaikyti visų rūšių su IRT susijusius sutrikimus ir grėsmes, kaip pasiūlė Komisija[36]. Transporto srityje Komisija į ES teisės aktus dėl aviacijos saugumo įtraukė nuostatas dėl kibernetinio saugumo[37] ir toliau stengsis didinti visų rūšių transporto kibernetinį atsparumą. **Demokratinių procesų ir institucijų** kibernetinio atsparumo stiprinimas yra pagrindinis Europos demokratijos veiksmų plano, kuriuo siekiama apsaugoti ir skatinti laisvus rinkimus, demokratinį diskursą ir žiniasklaidos pliuralizmą, elementas[38]. Galiausiai, siekdama užtikrinti infrastruktūros ir paslaugų saugumą pagal būsimą Kosmoso programą, Komisija toliau stiprins naujos kartos pasaulinės palydovinės navigacijos sistemos paslaugų GALILEO kibernetinio saugumo strategiją ir kitus naujus Kosmoso programos elementus[39].

1.2. Europos kibernetinio skydo kūrimas

Plečiantis junglumui ir sudėtingėjant kibernetiniams išpuoliams, keitimosi informacija ir jos analizės centrai (ISAC) atlieka naudingą funkciją, įskaitant sektorių lygmeniu, sudarydami sąlygas įvairioms suinteresuotosioms šalims keistis informacija apie kibernetines grėsmes[40]. Be to, tinklus ir kompiuterines sistemas reikia nuolat stebėti ir analizuoti, kad būtų galima tikruoju laiku nustatyti įsibrovimo atvejus ir neįprastą veiklą. Todėl daugelis privačių įmonių,

---

[34] [*įrašyti TIS pasiūlymo nuorodą*]

[35] [įrašyti *pasiūlymo* dėl ypatingos svarbos subjektų atsparumo direktyvos nuorodą]

[36] Pasiūlymas dėl Reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 ir (ES) Nr. 909/2014, COM(2020) 595 *final*.

[37] Komisijos įgyvendinimo reglamentas (ES) 2019/1583.

[38] Komunikatas dėl Europos demokratijos veiksmų plano, COM(2020) 790. Pagal šį planą Europos bendradarbiavimo rinkimų klausimais tinklas, valstybių narių rinkimų tinklai rems bendrų ekspertų grupių, kurios kovoja su rinkimų procesams kylančiomis grėsmėmis, įskaitant kibernetines grėsmes, siuntimą; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en.

[39] Tai apima naują vyriausybinio palydovinio ryšio iniciatyvą (GOVSATCOM) ir kosmines šiukšles (SST).

[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

viešųjų organizacijų ir nacionalinių institucijų yra įsteigusios reagavimo į kompiuterių saugumo incidentus tarnybas (CSIRT) ir saugumo operacijų centrus (SOC).

Saugumo operacijų centrai yra gyvybiškai svarbūs kaupiant žurnalų duomenis[41] ir izoliuojant įtartinus įvykius jų stebimuose ryšių tinkluose. Jie tai atlieka nustatydami signalus ir modelius ir išgaudami informaciją apie grėsmę iš didelio duomenų kiekio, kurį reikia įvertinti. Šie centrai padeda aptikti piktavališkų vykdymo programų veiklą ir taip suvaldyti kibernetinius išpuolius. Šiuose centruose darbas reikalauja daug pastangų ir vyksta labai greitai, todėl dirbtinis intelektas ir ypač mašinų mokymosi metodai gali suteikti specialistams neįkainojamą pagalbą[42].

Komisija siūlo sukurti **saugumo operacijų centrų tinklą visoje ES[43]**, remti esamų centrų tobulinimą ir naujų centrų steigimą. Ji taip pat rems šiuos centrus valdančių darbuotojų mokymą ir įgūdžių tobulinimą. Remdamasi poreikių analize, atlikta su atitinkamomis suinteresuotosiomis šalimis ir remiama ES kibernetinio saugumo agentūros (ENISA), Komisija galėtų įsipareigoti skirti daugiau kaip 300 mln. EUR viešojo ir privačiojo sektorių ir tarpvalstybiniam bendradarbiavimui kuriant nacionalinius ir sektorių tinklus, taip pat įtraukiant ir MVĮ, remiantis atitinkamomis valdymo, dalijimosi duomenimis ir saugumo nuostatomis.

Valstybės narės raginamos bendrai investuoti į šį projektą. Tokiu atveju centrai galėtų veiksmingiau dalytis nustatytais signalais ir juos susieti, taip pat rengti kokybišką žvalgybos informaciją apie grėsmes, kuria būtų dalijamasi su ISAC ir nacionalinėmis institucijomis, taip sudarant sąlygas geriau informuoti apie padėtį. Taip būtų siekiama per keletą etapų sujungti kuo daugiau centrų visoje ES, kad būtų kaupiamos kolektyvinės žinios ir dalijamasi geriausia praktika. Šiems centrams bus teikiama parama incidentų aptikimo, analizės ir reagavimo spartai gerinti naudojantis pažangiausiais dirbtinio intelekto ir mašinų mokymosi pajėgumais, kurią papildytų Europos našiosios kompiuterijos bendrosios įmonės ES sukurta superkompiuterių infrastruktūra[44].

Nuolat bendradarbiaudamas šis tinklas laiku pateiks įspėjimus apie kibernetinio saugumo incidentus institucijoms ir visoms suinteresuotosioms šalims, įskaitant bendrą kibernetinio saugumo padalinį (žr. 2.1 skirsnį). **Šis tinklas,** kurį sudarys patikima sargybos bokštų, galinčių aptikti potencialias grėsmes anksčiau nei jos sukels didelio masto žalą, sistema, **veiks kaip tikras ES kibernetinio saugumo skydas**.

1.3. Itin saugi ryšių infrastruktūra

Europos Sąjungos vyriausybiniai palydoviniai ryšiai[45], kurie yra kosmoso programos dalis, suteiks saugius ir ekonomiškai efektyvius ryšių pajėgumus kosmose ir padės užtikrinti saugumo ir saugos požiūriu itin svarbias misijas ir operacijas, kurias valdys ES ir jos valstybės narės, įskaitant nacionalinio saugumo subjektus ir ES institucijas bei agentūras.

---

[41] Taip, kad teisėsaugos institucijos ir teismai galėtų jų rezultatus naudoti kaip įrodymus.

[42] Šaltinis: „Ponemon Institute Research“ apklausa „SOC veiksmingumo gerinimas 2019 m.“ (angl. *Improving the Effectiveness of the SOC*, 2019); apie dirbtinio intelekto naudojimą saugumo operacijų centruose galima, pavyzdžiui, pasiskaityti A. Khraisat, I. Gondal, P. Vamplew ir kt. *Survey of intrusion detection systems: techniques, datasets and challenges*, *Cybersecur*, 2**,** 20 (2019 m.).

[43] Bus parengta išsamesnė šių centrų valdymo, veiklos principų ir finansavimo tvarka ir informacija apie tai, kaip jie papildys dabartines struktūras, pavyzdžiui, skaitmeninių inovacijų centrus.

[44] https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking.

[45] GOVSATCOM yra Sąjungos kosmoso programos sudedamoji dalis.

Valstybės narės įsipareigojo bendradarbiauti su Komisija, kad būtų įdiegta saugi Europos kvantinė ryšių infrastruktūra (QCI)[46]. Siekiant apsisaugoti nuo kibernetinių išpuolių, kvantinė ryšių infrastruktūra pasiūlys valdžios institucijoms visiškai naują konfidencialios informacijos perdavimo būdą, pagal kurį naudojama itin saugi Europos sukurtomis technologijomis grindžiama šifravimo forma. Kvantinę ryšių infrastruktūrą sudarys dvi pagrindinės dalys: turimi antžeminiai šviesolaidinio ryšio tinklai, jungiantys strategines vietas nacionaliniu ir tarpvalstybiniu lygmenimis, ir susieti kosmoso palydovai, apimantys visą ES, įskaitant jos užjūrio teritorijas[47]. Ši iniciatyva kurti ir diegti naujas saugesnes šifravimo formas ir ieškoti naujų ypatingos svarbos ryšių ir duomenų išteklių apsaugos būdų gali padėti apsaugoti neskelbtiną informaciją ir kartu užtikrinti ypatingos svarbos infrastruktūros objektų saugumą.

Atsižvelgdama į tai ir žvelgdama į ateitį, Komisija išnagrinės galimybę įdiegti daugiažiedę saugią junglumo sistemą. Ši sistema naudotųsi GOVSATCOM ir kvantine ryšių infrastruktūra, į ją būtų integruotos pažangiausios technologijos („Quantum“, 5G, dirbtinis intelektas, tinklo paribio kompiuterija), laikantis griežčiausios kibernetinio saugumo sistemos, kad būtų palaikomos saugaus dizaino paslaugos, pavyzdžiui, patikimas, saugus ir ekonomiškai efektyvus ryšys ir šifruotas ryšys ypatingos svarbos vyriausybės veiklai.

1.4. Naujos kartos plačiajuosčio judriojo ryšio tinklų užtikrinimas

ES piliečiai ir įmonės, naudojantys pažangias ir novatoriškas prietaikas, kurių veikimo pagrindas yra **5G ir būsimų kartų tinklai**, turėtų gauti naudos dėl taikomų aukščiausių saugumo standartų. Valstybės narės drauge su Komisija ir padedant ENISA 2020 m. sausio mėn. ES 5G priemonių rinkiniu[48] nustatė visapusišką ir objektyvų rizika grindžiamą požiūrį į 5G kibernetinį saugumą, grindžiamą galimų rizikos švelninimo planų vertinimu ir veiksmingiausių priemonių nustatymu. Be to, ES stiprina savo pajėgumus 5G ir būsimos kartos tinklų sektoriuose, kad išvengtų priklausomybės ir skatintų tvarią diversifikuotą tiekimo grandinę.

2020 m. gruodžio mėn. Komisija paskelbė 2019 m. kovo 26 d. rekomendacijos dėl 5G tinklų kibernetinio saugumo poveikio ataskaitą[49]. Iš ataskaitos matyti, kad nuo tada, kai buvo susitarta dėl priemonių rinkinio, padaryta didelė pažanga ir kad dauguma valstybių narių pagal planą artimiausioje ateityje užbaigs įgyvendinti didelę priemonių rinkinio dalį, nors

[46] „EuroQCI“ deklaraciją pasirašė dauguma valstybių narių, o plėtra ir infrastruktūros diegimas turi būti vykdomi 2021–2027 m. ir finansuojami pagal programas „Europos horizontas“ ir „Skaitmeninė Europa“, taip pat iš Europos kosmoso agentūros biudžeto, taikant tinkamas valdymo priemones; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

[47] Kosmoso elemento kūrimas yra būtinas norint užtikrinti tolimojo susisiekimo tiesiogines jungtis (> 1 000 km), kurių antžeminė infrastruktūra negali palaikyti. Grindžiama kvantinės mechanikos savybėmis kvantinė ryšių infrastruktūra iš pradžių šalims suteiks galimybę saugiai dalytis atsitiktiniais slaptaisiais raktais, kurie bus naudojami pranešimams užšifruoti ir iššifruoti. Ji taip pat apims bandymų ir atitikties infrastruktūros diegimą, reikalingą siekiant įvertinti Europos kvantinių ryšių prietaisų ir sistemų atitiktį kvantinei ryšių infrastruktūrai ir jų sertifikavimą bei patvirtinimą prieš juos integruojant į kvantinę ryšių infrastruktūrą. Ji bus sukurta taip, kad galėtų palaikyti papildomas taikomąsias programas, kai jos pasiekia reikiamą technologinės brandos lygį. Dabartinis bandomasis projektas „OpenQKD“ (https://openqkd.eu/) yra šios bandymų ir atitikties infrastruktūros pirmtakas.

[48] Komunikatas „Saugaus 5G ryšio diegimas ES. ES priemonių rinkinio įgyvendinimas“, COM(2020) 50.

[49] Komisijos ataskaita dėl 2019 m. kovo 26 d. Komisijos rekomendacijos dėl 5G tinklų kibernetinio saugumo poveikio, 2020 m. gruodžio 15 d.

esama tam tikrų skirtumų ir spragų, nurodytų dar 2020 m. liepos mėn. paskelbtoje pažangos ataskaitoje[50].

2020 m. spalio mėn. Europos Vadovų Taryba paragino ES ir valstybes nares „visapusiškai pasinaudoti 5G kibernetinio saugumo priemonių rinkiniu“ ir „taikyti atitinkamus apribojimus pagrindinių objektų, kurie ES suderintuose rizikos vertinimuose apibrėžiami kaip ypatingos svarbos ir didesnės rizikos objektai, didelės rizikos tiekėjams <...>, remiantis bendrais objektyviais kriterijais“[51].

Žvelgiant į ateitį, ES ir jos valstybės narės turėtų užtikrinti, kad nustatyta rizika būtų tinkamai ir koordinuotai sumažinta, visų pirma kiek tai susiję su tikslu kuo labiau sumažinti didelės rizikos tiekėjų keliamą riziką ir išvengti priklausomybės nuo šių tiekėjų nacionaliniu ir Sąjungos lygmenimis, ir kad būtų atsižvelgta į visus naujus reikšmingus pokyčius ar riziką. Valstybės narės raginamos visapusiškai naudotis priemonių rinkiniu, kai investuoja į skaitmeninius pajėgumus ir ryšį.

Remdamasi 2019 m. rekomendacijos poveikio ataskaita, Komisija ragina valstybes nares paspartinti darbą ir užbaigti įgyvendinti pagrindines priemonių rinkinio priemones iki 2021 m. antrojo ketvirčio. Ji taip pat ragina valstybes nares toliau kartu stebėti daromą pažangą ir užtikrinti, kad požiūriai ir toliau būtų derinami. Siekiant remti šį procesą, ES lygmeniu bus siekiama trijų pagrindinių tikslų: užtikrinti tolesnę rizikos mažinimo metodų konvergenciją visoje ES, remti nuolatinį keitimąsi žiniomis ir gebėjimų stiprinimą, ir skatinti tiekimo grandinių atsparumą ir kitus ES strateginius saugumo tikslus. Konkretūs veiksmai, susiję su šiais pagrindiniais tikslais, išdėstyti šio komunikato specialiame priede.

Komisija, padedama ENISA, toliau glaudžiai bendradarbiaus su valstybėmis narėmis, kad šie tikslai ir veiksmai būtų įgyvendinti (žr. priedą).

Be to, ES 5G priemonių rinkinio požiūris sudomino ES nepriklausančias šalis, kurios šiuo metu kuria savo ryšių tinklų apsaugos metodus. Komisijos tarnybos kartu su Europos išorės veiksmų tarnyba ir ES delegacijų tinklu yra pasirengusios paprašius pateikti viso pasaulio institucijoms papildomos informacijos apie visapusišką, objektyvų ir rizika grindžiamą požiūrį.

1.5. Saugių daiktų internetas

Kiekvienam susietajam daiktui būdingi pažeidžiamai, kuriais gali būti pasinaudota, o pasekmės gali būti plataus masto. Vidaus rinkos taisyklėse numatytos apsaugos nuo nesaugių produktų ir paslaugų priemonės. Komisija jau dirba siekdama **pagal Kibernetinio saugumo aktą** užtikrinti **skaidrius saugumo sprendimus ir sertifikavimą**, taip pat skatinti teikti saugius produktus ir paslaugas nepakenkiant jų veiksmingumui[52]. Per pirmąjį 2021 m.

[50] 2020 m. liepos 24 d. TIS bendradarbiavimo grupės ataskaita dėl priemonių rinkinio įgyvendinimo.
[51] EUCO 13/20, specialiojo Europos Vadovų Tarybos susitikimo (2020 m. spalio 1 ir 2 d.) išvados.
[52] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas). Kibernetinio saugumo aktu skatinamas IRT sertifikavimas ES lygmeniu ir nustatoma Europos kibernetinio saugumo sertifikavimo sistema, skirta savanoriškoms Europos kibernetinio saugumo sertifikavimo schemoms kurti siekiant užtikrinti tinkamą IRT produktų, paslaugų ir procesų kibernetinio saugumo lygį Sąjungoje ir sumažinti vidaus rinkos susiskaidymą, susijusį su kibernetinio saugumo sertifikavimo schemomis Sąjungoje. Be to, kibernetinio saugumo reitingų įmonės paprastai yra įsisteigusios už ES ribų, o jų skaidrumas ir priežiūra yra riboti; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings.

ketvirtį ji priims pirmąją tęstinę Sąjungos darbo programą (kuri turi būti atnaujinama bent kartą per trejus metus), kad sektoriaus atstovai, nacionalinės institucijos ir standartizacijos įstaigos galėtų iš anksto pasirengti būsimoms Europos kibernetinio saugumo sertifikavimo schemoms[53]. Kadangi daiktų internetas sparčiai plečiasi, reikia griežtinti taisykles, kurių laikymąsi įmanoma užtikrinti, ir taip užtikrinti bendrą atsparumą bei padidinti kibernetinį saugumą.

Komisija apsvarstys galimybę taikyti visapusišką požiūrį, įskaitant galimas **naujas horizontaliąsias taisykles, kuriomis siekiama padidinti visų vidaus rinkai pateiktų susietųjų produktų ir susijusių paslaugų kibernetinį saugumą**[54]. Tokiose taisyklėse galėtų būti numatyta **nauja rūpestingumo pareiga, taikoma susietųjų įrenginių gamintojams**, šalinti programinės įrangos pažeidžiamumus, įskaitant tolesnį programinės įrangos ir saugumo naujinių tiekimą, taip pat užtikrinti, kad gyvavimo ciklo pabaigoje būtų ištrinti asmens ir kiti neskelbtini duomenys. Šios taisyklės padėtų sustiprinti Žiedinės ekonomikos veiksmų plane pristatytą „teisės taisyti pasenusią programinę įrangą“ iniciatyvą ir papildytų priemones, susijusias su tam tikrų rūšių produktais, pavyzdžiui, pasiūlysimus privalomus reikalavimus, susijusius su galimybe pateikti rinkai tam tikrų rūšių belaidžius produktus (priimant deleguotąjį aktą pagal Radijo įrangos direktyvą[55]), bei tikslą nuo 2022 m. liepos mėn. taikyti motorinių transporto priemonių kibernetinio saugumo taisykles visų naujų rūšių transporto priemonėms[56]. Be to, šios taisyklės būtų grindžiamos siūlomomis peržiūrėti bendros produktų saugos taisyklėmis, kuriomis kibernetinio saugumo aspektai tiesiogiai nereguliuojami[57].

1.6. Didesnis pasaulinio interneto saugumas

Interneto veikimą ir vientisumą visame pasaulyje padeda užtikrinti pagrindinių protokolų rinkinys ir pagalbinė infrastruktūra[58]. Šis rinkinys apima DNS ir jos hierarchinę bei deleguotą zonų sistemą, pradedant hierarchijos viršuje esančia šaknine zona ir trylika DNS šakninių serverių[59], nuo kurių priklauso žiniatinklis. Komisija ketina parengti **ES lėšomis remiamą nenumatytų atvejų planą, pagal kurį būtų imamasi veiksmų susiklosčius ekstremalių sąlygų scenarijams, darantiems poveikį pasaulinės DNS šakninės sistemos vientisumui ir prieinamumui**. Vertindama šių operatorių vaidmenį užtikrinant tolesnį interneto prieinamumą visame pasaulyje visomis aplinkybėmis Komisija bendradarbiaus su ENISA,

[53] Reikalaujama pagal Kibernetinio saugumo akto 47 straipsnio 5 dalį.
[54] Tarybos išvadose raginama imtis horizontaliųjų priemonių dėl susietųjų įrenginių kibernetinio saugumo; 13629/20, 2020 m. gruodžio 2 d.
[55] Direktyva 2014/53/ES.
[56] Remiantis 2020 m. birželio mėn. priimta JT taisykle; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.
[57] Dabartinių bendros produktų saugos taisyklių (Direktyva 2001/95/EB) peržiūra; taip pat planuojamas pasiūlymas pritaikyti gamintojų atsakomybės taisykles atsižvelgiant į skaitmeninį kontekstą pagal ES atsakomybės reguliavimo sistemą.
[58] „Atvirojo interneto viešasis pagrindas, kitaip tariant – interneto pagrindiniai protokolai ir infrastruktūra, kurie yra pasaulinės viešosios gėrybės, užtikrina esmines viso interneto funkcines galimybes ir nuo jų priklauso jo įprastas veikimas. ENISA turėtų remti atvirojo interneto viešojo pagrindo funkcionavimo saugumą ir stabilumą, įskaitant pagrindinius protokolus (visų pirma DNS, BGP ir IPv6), domenų vardų sistemos veikimą (kaip antai visų aukščiausio lygio domenų vardų veikimą) ir šakninės zonos veikimą, bet ne tik tai“; Kibernetinio saugumo akto 23 konstatuojamoji dalis.
[59] https://www.iana.org/domains/root/servers.

valstybėmis narėmis, dviem ES DNS šakninių serverių operatoriais[60] ir įvairių suinteresuotųjų šalių bendruomene.

Kad klientas galėtų naudotis tam tikrą domeno vardą turinčiu interneto ištekliumi, jo užklausa (paprastai dėl universaliojo ištekliaus adreso, URL) turi būti išversta į IP adresą arba pakeista IP adresu, pateikiant nuorodą į DNS vardų serverius. Tačiau ES gyventojai ir organizacijos yra vis labiau priklausomi nuo kelių viešų DNS keitiklių, kuriuos valdo ne ES subjektai. Dėl to, kad DNS keitimas sutelktas kelių įmonių rankose[61], pats keitimo procesas tampa pažeidžiamas, jeigu vieną pagrindinį paslaugų teikėją paveikia reikšmingi įvykiai, o ES institucijoms tampa sunkiau kovoti su galimais piktavališkais kibernetiniais išpuoliais ir dideliais geopolitiniais bei techniniais incidentais[62].

Siekdama sumažinti saugumo problemas, susijusias su rinkos koncentracija, Komisija skatins atitinkamas suinteresuotąsias šalis, įskaitant ES įmones, interneto paslaugų teikėjus ir naršyklių pardavėjus, priimti DNS keitimo įvairinimo strategiją. Komisija taip pat ketina prisidėti prie saugaus interneto ryšio užtikrinimo remdama viešojo **Europos DNS keitiklio** kūrimą. Ši iniciatyva „DNS4EU“ suteiks alternatyvią Europos prieigos prie pasaulinio interneto paslaugą. „DNS4EU“ bus skaidri, atitiks naujausius saugumo, duomenų apsaugos ir integruotosios privatumo apsaugos ir standartizuotosios privatumo apsaugos standartus bei taisykles ir bus Europos pramonės duomenų ir debesijos aljanso dalis[63].

Komisija, bendradarbiaudama su valstybėmis narėmis ir sektoriaus atstovais, taip pat **paspartins pagrindinių interneto standartų, įskaitant IPv6**[64] **ir nusistovėjusius interneto saugumo standartus, ir gerosios praktikos, susijusios su DNS, maršrutizavimu ir e. pašto saugumu, taikymą**[65], neatmetant reguliavimo priemonių, pavyzdžiui, Europos IPv4 laikino galiojimo sąlygos, kad rinka būtų nukreipta reikiama linkme, jeigu siekiant priimti šiuos standartus bus daroma nepakankama pažanga. ES turėtų skatinti (pavyzdžiui, pagal ES ir Afrikos strategiją[66]) įgyvendinti šiuos standartus šalyse partnerėse, kad būtų remiamas pasaulinio atvirojo interneto plėtojimas ir kovojama su uždarais ir kontroliuojamais interneto modeliais. Galiausiai Komisija apsvarstys, ar reikia sukurti mechanizmą, skirtą sistemingesnei stebėsenai ir suvestinių interneto srauto duomenų rinkimui, ir konsultuotis galimų sutrikimų klausimais[67].

---

[60] Švedijoje organizacijos „Netnod“ naudojami „i.root-servers“ („i“ šakniniai serveriai) ir Nyderlandų organizacijos RIPE NCC naudojami „k.root-servers“ („k“ šakniniai serveriai).

[61] *Consolidation in the DNS resolver market – how much, how fast how dangerous?* (), *Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services* ().

[62] Taip pat yra įrodymų, kad DNS duomenys gali būti naudojami profiliavimo tikslais, o tai turi įtakos privatumo ir duomenų apsaugos teisėms.

[63] Bendra deklaracija „Naujos kartos debesijos, skirtos ES įmonėms ir viešajam sektoriui, kūrimas“; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[64] IPv6 diegimas dabar jau pasistūmėjo, nes labai sumažėjo IPv4 adresų pasiūla ir padidėjo jų kaina. Tačiau IPv6 diegimas ES yra netolygus.

[65] Tokie standartai apima DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE ir maršrutizavimo normas bei gerąją praktiką, pvz., abipusiškai sutartas maršrutizavimo saugumo normas (MANRS).

[66] 2020 m. kovo 9 d. bendras komunikatas „Visapusiškos strategijos su Afrika kūrimas“, JOIN(2020) 4 *final*.

[67] Toks interneto stebėsenos centras galėtų būti įtrauktas į Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro veiklos sritį; Pasiūlymas dėl Reglamento, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas, COM(2018) 630 *final*.

1.7. Aktyvesnis dalyvavimas technologijų tiekimo grandinėje

2021–2027 m. daugiametėje finansinėje programoje numačiusi teikti finansinę paramą kibernetinei saugiai skaitmeninei transformacijai, ES turi unikalią galimybę sutelkti išteklius, kad, atsižvelgdama į savo vertybes ir prioritetus, skatintų savos pramonės strategiją[68] ir lyderystę skaitmeninių technologijų ir kibernetinio saugumo srityse visoje skaitmeninėje tiekimo grandinėje (įskaitant duomenis ir debesiją, naujos kartos procesorių technologijas, itin saugų ryšį ir 6G tinklus). Viešojo sektoriaus intervencija turėtų būti grindžiama ES viešųjų pirkimų reglamentavimo sistemos ir bendriems Europos interesams svarbių projektų teikiamomis priemonėmis. Be to, šia intervencija gali būti skatinamos privačios investicijos per viešojo ir privačiojo sektorių partnerystes (be kita ko, remiantis patirtimi, įgyta plėtojant ir įgyvendinant sutartimi pagrįstą viešojo ir privačiojo sektorių partnerystę kibernetinio saugumo srityje padedant Europos kibernetinio saugumo organizacijai), rizikos kapitalas, kuriuo remiamos MVĮ ar pramonės aljansai, ir technologijų pajėgumų strategijų įgyvendinimas.

Ypatingas dėmesys taip pat bus skiriamas techninės paramos priemonei[69] ir geriausiam MVĮ, ypač tų, kurios nepatenka į peržiūrėtos TIS direktyvos taikymo sritį, naudojimuisi naujausiomis kibernetinio saugumo priemonėmis, be kita ko, vykdant tikslinę veiklą skaitmeninių inovacijų centruose pagal Skaitmeninės Europos programą. Tikslas – pritraukti valstybių narių investicijas atitinkančią sumą iš pramonės sektoriaus pagal partnerystę, valdomą kartu su valstybėmis narėmis, į siūlomus įsteigti **Kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą ir Koordinavimo centrų tinklą (CCCN).** Kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Koordinavimo centrų tinklas, padedant pramonės sektoriui ir akademinėms bendruomenėms, turėtų atlikti pagrindinį vaidmenį plėtojant ES technologinį suverenumą kibernetinio saugumo srityje, stiprinant gebėjimus apsaugoti jautrią infrastruktūrą, pavyzdžiui, 5G tinklus, ir mažinant svarbiausių technologijų priklausomybę nuo kitų pasaulio šalių.

Komisija, galbūt per Kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą ir Koordinavimo centrų tinklą, ketina remti specialios kibernetinio saugumo magistrantūros programos rengimą ir prisidėti prie bendro Europos kibernetinio saugumo mokslinių tyrimų ir inovacijų veiksmų po 2020 m. plano. Investicijos, skirstomos per Kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą ir Koordinavimo centrų tinklą, taip pat būtų grindžiamos bendradarbiavimu mokslinių tyrimų ir technologinės plėtros srityje, kurioje veikia kibernetinio saugumo kompetencijos centrų tinklai, taip suvienijant geriausių Europos mokslinių tyrimų grupių ir pramonės atstovų pastangas parengti ir įgyvendinti bendrus mokslinių tyrimų planus laikantis Europos kibernetinio saugumo organizacijos veiksmų gairių[70]. Komisija toliau kliausis ENISA ir Europolo moksliniu tiriamuoju darbu ir pagal programą „Europos horizontas“ toliau rems pavienius interneto novatorius, kuriančius privatumo didinimo ir saugiojo ryšio technologijas, grindžiamas atvirojo kodo programine ir aparatine įranga, kaip šiuo metu vykdoma pagal Naujos kartos interneto iniciatyvą.

[68] Komunikatas dėl naujos Europos pramonės strategijos, COM(2020) 102 *final*.
[69] https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM:2020:0409:FIN.
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies.

1.8. Kibernetinių įgūdžių turintys ES darbuotojai

Apskritai, ES pastangos kelti darbuotojų kvalifikaciją, ugdyti, pritraukti ir išlaikyti geriausius kibernetinio saugumo srities talentus ir investuoti į pasaulinio lygio mokslinius tyrimus ir inovacijas yra svarbus apsaugos nuo kibernetinių grėsmių elementas. Šioje srityje yra daug potencialo. Taigi ypatingą dėmesį reikia skirti didesnio skaičiaus įvairių talentų ugdymui, pritraukimui ir išlaikymui. Peržiūrėtas Skaitmeninio švietimo veiksmų planas padės didinti asmenų, ypač vaikų ir jaunimo, ir organizacijų, visų pirma MVĮ, kibernetinį sąmoningumą[71]. Be to, šis planas paskatins moteris studijuoti mokslo, technologijų, inžinerijos ir matematikos (STEM) dalykus, kelti savo kvalifikaciją ir persikvalifikuoti, kad tokius įgūdžius įgytų ir galėtų dirbti su IRT susijusį darbą. Komisija su Europolo ES intelektinės nuosavybės tarnyba, ENISA, valstybėmis narėmis ir privačiuoju sektoriumi taip pat parengs informuotumo didinimo priemones ir gaires, kad padidintų ES įmonių atsparumą **kibernetinėms intelektinės nuosavybės vagystėms**[72].

Švietimas, įskaitant profesinį rengimą ir mokymą (PRM), informuotumą ir pratybas, taip pat turėtų dar labiau padidinti kibernetinio saugumo ir kibernetinės gynybos įgūdžius ES lygmeniu. Šiuo tikslu atitinkami ES subjektai, pavyzdžiui, ENISA, Europos gynybos agentūra (EGA) ir Europos saugumo ir gynybos koledžas (ESGK)[73], turėtų siekti savo atitinkamos veiklos sąveikos.

Strateginės iniciatyvos

ES turėtų užtikrinti:

- peržiūrėtos TIS direktyvos priėmimą;
- reguliavimo priemones, susijusias su saugių daiktų internetu;
- kad investicijos į kibernetinį saugumą, skirstomos per Kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą ir Koordinavimo centrų tinklą, (visų pirma pagal Skaitmeninės Europos programą, programą „Europos horizontas“ ir ekonomikos gaivinimo priemonę) 2021–2027 m. pasiektų iki 4,5 mlrd. EUR viešųjų ir privačiųjų investicijų;
- dirbtiniu intelektu grindžiamų saugumo operacijų centrų ES tinklą ir itin saugaus ryšio infrastruktūrą, kurioje būtų naudojamos kvantinės technologijos;
- kibernetinio saugumo technologijų diegimą plačiu mastu panaudojant specialią paramą MVĮ, teikiamą per skaitmeninių inovacijų centrus;
- ES DNS keitiklio, kaip saugios ir atviros interneto prieigos alternatyvos ES piliečiams, įmonėms ir viešojo administravimo institucijoms, plėtojimą ir
- 5G priemonių rinkinio įgyvendinimo užbaigimą iki 2021 m. antrojo ketvirčio (žr. priedą).

[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_lt.
[72] https://ec.europa.eu/commission/presscorner/detail/lt/IP_20_2187.
[73] Per Švietimo, mokymo, pratybų ir vertinimo kibernetinėje srityje platformą (ETEE).

2. VEIKLOS PAJĖGUMŲ, SUSIJUSIŲ SU PREVENCIJA, ATGRASYMU IR REAGAVIMU, STIPRINIMAS

Kibernetiniai incidentai – atsitiktiniai arba tyčia vykdomi nusikaltėlių, valstybinių ir kitų nevalstybinių subjektų, – gali padaryti didžiulę žalą. Atsižvelgiant į kibernetinių incidentų mastą bei sudėtingumą ir tai, kad juos vykdant dažnai naudojamos trečiųjų šalių paslaugos, aparatinė įranga ir programinė įranga, kuriais siekiama pakenkti galutiniam taikiniui, ES kolektyvinėje grėsmių aplinkoje sudėtinga jiems pasipriešinti be sistemingo ir visapusiško keitimosi informacija ir bendradarbiavimo bendro reagavimo srityje. **Visapusiškai įgyvendindama reguliavimo priemones, telkdama išteklius ir bendradarbiaudama** ES siekia teikti paramą valstybėms narėms, ginančioms savo piliečius ir savo ekonominius bei nacionalinio saugumo interesus, visais atžvilgiais laikantis pagrindinių teisių ir laisvių bei teisinės valstybės principų. Kelios bendruomenės, kurias sudaro tinklai, ES institucijos, įstaigos ir agentūros, taip pat valstybių narių institucijos, naudodamosi atitinkamomis savo priemonėmis ir iniciatyvomis, atsako už kibernetinių grėsmių prevenciją, trukdymą joms, atgrasymą nuo jų ir reagavimą į jas[74]. Šioms bendruomenėms priklauso: i) TIS institucijos, pavyzdžiui, CSIRT, ir reagavimo į ekstremaliąsias situacijas komandos; ii) teisėsaugos ir teisminės institucijos; iii) kibernetinės diplomatijos bendruomenės ir iv) kibernetinės gynybos bendruomenės.

2.1. Bendras kibernetinio saugumo padalinys

Bendras kibernetinio saugumo padalinys veiktų kaip virtuali ir fizinė įvairių ES kibernetinio saugumo bendruomenių bendradarbiavimo platforma, kurioje daugiausia dėmesio būtų skiriama operatyviniam ir techniniam koordinavimui kovoje su dideliais tarpvalstybiniais kibernetiniais incidentais ir grėsmėmis.

Bendras kibernetinio saugumo padalinys būtų svarbus žingsnis siekiant užbaigti kurti **Europos kibernetinio saugumo krizių valdymo sistemą**. Kaip nurodyta Komisijos pirmininkės politinėse gairėse[75], padalinys turėtų sudaryti sąlygas valstybėms narėms ir ES institucijoms, įstaigoms ir agentūroms visapusiškai pasinaudoti turimomis struktūromis, ištekliais bei pajėgumais ir skatinti **poreikiu dalytis** principu grindžiamą mąstyseną. Tai padėtų įtvirtinti iki šiol padarytą pažangą įgyvendinant 2017 m. Rekomendaciją dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (toliau – planas)[76]. Be to, tai suteiktų galimybę toliau stiprinti bendradarbiavimą, susijusį su plano struktūra, ir pasinaudoti pažangos, padarytos visų pirma TIS Bendradarbiavimo grupėje ir CyCLONe tinkle, rezultatais.

---

[74] Įskaitant Europos Sąjungos kibernetinio saugumo agentūros (ENISA) paramą operatyviniam bendradarbiavimui ir krizių valdymui; CSIRT tinklą; Ryšių palaikymo dėl kibernetinių krizių organizacinis tinklą (CyCLONe, ateityje bus pervadintas į EU-CyCLONe, kaip pasiūlyta peržiūrėtoje TIS direktyvoje); TIS bendradarbiavimo grupę; rezervą „rescEU“; Europos kovos su elektroniniu nusikalstamumu centrą, Europolo bendrą kovos su kibernetiniais nusikaltimais veiksmų darbo grupę ir Teisėsaugos institucijų reagavimo į ekstremalias situacijas protokolą; ES žvalgybos ir situacijų centrą (EU INTCEN) ir Kibernetinio saugumo diplomatijos priemonių rinkinį); Bendrą žvalgybinės informacijos analizės centrą (SIAC); kibernetinius projektus pagal nuolatinį struktūrizuotą bendradarbiavimą (PESCO), visų pirma greitojo reagavimo į kibernetinius incidentus komandas ir savitarpio pagalbą kibernetinio saugumo srityje (CRRT).

[75] „Daugiau siekianti Sąjunga. Mano Europos darbotvarkė“, 2019–2024 m. kadencijos Europos Komisijos politinės gairės, kurias pateikė kandidatė į Europos Komisijos pirmininko pareigas Ursula von der Leyen.

[76] 2017 m. rugsėjo 13 d. Rekomendacijos dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes planas, C(2017) 6100 *final*.

Taip būtų galima pašalinti dvi **pagrindines spragas**, dėl kurių dabar daugėja pažeidžiamumų ir atsiranda reagavimo į tarpvalstybines grėsmes ir incidentus, darančius poveikį Sąjungai, trūkumų. Pirma, pilietinės, diplomatinės, teisėsaugos ir gynybos kibernetinio saugumo **bendruomenės** dar neturi bendros erdvės, kurioje galėtų puoselėti struktūrizuotą bendradarbiavimą ir palengvinti operatyvinį ir techninį bendradarbiavimą. Antra, atitinkamos kibernetinio saugumo suinteresuotosios šalys dar negalėjo išnaudoti viso operatyvinio bendradarbiavimo ir savitarpio pagalbos esamuose tinkluose ir bendruomenėse **potencialo**. Be to, nėra platformos, kurioje būtų galima operatyviai bendradarbiauti su privačiuoju sektoriumi. Padalinys turėtų pagerinti ir paspartinti koordinavimą ir sudaryti sąlygas ES pasirengti didelio masto kibernetiniams incidentams bei krizėms ir į juos reaguoti.

Bendras kibernetinio saugumo padalinys nebūtų papildoma savarankiška įstaiga ir nedarytų poveikio nacionalinių kibernetinio saugumo institucijų ar ES dalyvių kompetencijai ir įgaliojimams. Padalinys veikiau veiktų kaip stabilizuojantis apsaugos mechanizmas, kuriame dalyviai galėtų naudotis vieni kitų parama ir žiniomis, ypač tuo atveju, kai įvairios kibernetinės bendruomenės turi glaudžiai bendradarbiauti. Kartu pastarojo meto įvykiai parodė, kad ES privalo plėsti savo tikslų mastą ir būti pasirengusi susidurti su kibernetinių grėsmių situacijomis ir realybe. Todėl ES subjektai (Komisija ir ES agentūros bei įstaigos), dalyvaudami bendro kibernetinio saugumo padalinio veikloje, bus pasirengę reikšmingai padidinti savo išteklius ir pajėgumus, kad suvienodintų savo parengtį ir atsparumą.

Bendras kibernetinio saugumo padalinys turėtų siekti trijų pagrindinių tikslų. Pirma, jis užtikrintų visų kibernetinio saugumo bendruomenių **parengtį**; antra, sudarydamas sąlygas dalytis informacija jis užtikrintų nuolatinį bendrą **informuotumą** apie padėtį; trečia, jis sustiprintų koordinuotą **reagavimą** ir veiklos atkūrimą. Kad pasiektų šiuos tikslus, padalinys turėtų grįsti savo veiklą aiškiai apibrėžtomis **sudedamosiomis dalimis ir tikslais**, pavyzdžiui, užtikrinti **saugų ir greitą dalijimąsi informacija**, gerinti dalyvių **bendradarbiavimą**, įskaitant valstybių narių ir atitinkamų ES subjektų sąveiką, užmegzti struktūrizuotas **partnerystes su patikima sektoriaus** baze ir sudaryti palankesnes sąlygas suderintam požiūriui į **bendradarbiavimą su išorės partneriais**. Šiuo tikslu, remdamasis turimų pajėgumų nacionaliniu ir ES lygmenimis inventoriumi, padalinys galėtų padėti plėtoti bendradarbiavimo sistemą.

Kad bendras kibernetinio saugumo padalinys taptų ES operatyvinio kibernetinio saugumo bendradarbiavimo ašimi, Komisija, visapusiškai atsižvelgdama į visų susijusių subjektų kompetenciją ir įgaliojimus, dirbs išvien su valstybėmis narėmis ir atitinkamomis ES institucijomis, įstaigomis ir agentūromis, įskaitant ENISA, CERT-EU ir Europolą, siekdama skatinti **laipsnišką ir įtraukų požiūrį**. Laikydamasis šio požiūrio, padalinys galėtų papildomai plėtoti konkrečios kibernetinės bendruomenės dalyvių bendradarbiavimą, kai, tų dalyvių manymu, tai yra būtina.

Kuriant bendrą kibernetinio saugumo padalinį siūloma imtis keturių pagrindinių veiksmų:

- *nustatyti* –turimų pajėgumų nacionaliniu ir ES lygmenimis inventorizavimas;
- *parengti* – nustatyti struktūrizuoto bendradarbiavimo ir pagalbos sistemą;
- *dislokuoti* – įgyvendinti sistemą pasinaudojant dalyvių suteiktais ištekliais, kad bendras kibernetinio saugumo padalinys pradėtų veikti;
- *plėstis* – stiprinti koordinuoto reagavimo pajėgumus padedant sektoriui ir partneriams.

Remdamasi konsultacijų su valstybėmis narėmis, ES institucijomis, įstaigomis ir agentūromis[77] rezultatais, Komisija, dalyvaujant vyriausiajam įgaliotiniui, savo kompetencijos ribose iki 2021 m. vasario mėn. pristatys **bendro kibernetinio saugumo padalinio nustatymo, parengimo, dislokavimo ir plėtros** procesą, etapus ir tvarkaraštį.

2.2. Kova su kibernetiniais nusikaltimais

Mūsų priklausomybė nuo internetinių priemonių proporcingai padidino kibernetinių nusikaltėlių išpuolių perimetrą ir lėmė tai, kad beveik visų rūšių nusikaltimų tyrimas turi skaitmeninį aspektą. Be to, pagrindinėms mūsų visuomenės grupėms grėsmę kelia kibernetiniai subjektai ir tie, kurie naudoja kibernetines priemones savo neteisėtiems veiksmams planuoti ir vykdyti. Todėl esama glaudžių sąsajų su bendra ES saugumo politika, kaip matyti iš ES 2020 m. saugumo sąjungos strategijos kibernetinių elementų ir ES kovos su terorizmu darbotvarkės[78].

Veiksminga kova su kibernetiniais nusikaltimais yra pagrindinis kibernetinio saugumo užtikrinimo veiksnys: atgrasymo negalima pasiekti užtikrinant tik atsparumą, tam taip pat reikia išaiškinti nusikaltėlius ir imtis jų baudžiamojo persekiojimo. Todėl labai svarbu skatinti kibernetinio saugumo subjektų ir teisėsaugos bendradarbiavimą ir mainus. Todėl ES lygmeniu Europolas ir ENISA jau ėmėsi tvirtai bendradarbiauti rengdami bendras konferencijas ir praktinius seminarus ir teikdami Komisijai, valstybėms narėms ir kitoms suinteresuotosioms šalims bendras ataskaitas kibernetinio saugumo grėsmių ir technologinių problemų klausimais. Komisija toliau rems šį integruotą požiūrį siekdama užtikrinti nuoseklų ir veiksmingą atsaką, pagrįstą išsamia informacija apie padėtį.

ES ir nacionalinės institucijos kaip svarbų to atsako elementą turi plėsti ir gerinti teisėsaugos pajėgumus tirti kibernetinius nusikaltimus, visapusiškai gerbiant pagrindines teises ir siekiant užtikrinti būtiną įvairių teisių ir interesų pusiausvyrą. ES turėtų turėti galimybę kovoti su kibernetiniais nusikaltimais visapusiškai įgyvendindama paskirtį atitinkančius teisės aktus, ypatingą dėmesį skirdama kovai su seksualine prievarta prieš vaikus internete ir skaitmeniniams tyrimams, kurių objektas, be kita ko, yra nusikaltimai tamsiajame tinkle. Teisėsaugos institucijos privalo būti visapusiškai pasirengusios skaitmeniniams tyrimams. Todėl Komisija pateiks veiksmų planą, kad pagerintų teisėsaugos institucijų skaitmeninius pajėgumus šiuo tikslu suteikdama joms būtinus įgūdžius ir priemonių. Be to, Europolas toliau plėtos savo, kaip kompetencijos centro, vaidmenį, kad padėtų nacionalinėms teisėsaugos institucijoms kovoti su nusikaltimais pasinaudojant kibernetine erdve ir išimtinai kibernetiniais nusikaltimais ir kartu prisidėtų prie bendrų kriminalistikos standartų (per Europolo inovacijų laboratoriją ir centrą) parengimo. Visoje šioje veikloje turi tinkamai dalyvauti valstybės narės, – jos skatinamos naudotis Vidaus saugumo fondo nacionalinėmis programomis ir siūlyti projektus atsiliepiant į kvietimus teikti pasiūlymus pagal teminę priemonę.

Komisija naudosis visomis tinkamomis priemonėmis, įskaitant pažeidimo nagrinėjimo procedūras, siekdama užtikrinti, kad 2013 m. Direktyva dėl atakų prieš informacines

[77] 2020 m. liepos – lapkričio mėn. vykusios konsultacijos su valstybėmis narėmis (įskaitant „Blue OLEx20“ pratybas, kuriose dalyvavo nacionalinių kibernetinio saugumo institucijų vadovai), ES institucijomis, įstaigomis ir agentūromis.

[78] Komunikatas „ES kovos su terorizmu darbotvarkė: numatyti, užkirsti kelią, apsaugoti, reaguoti“, 2020 12 9, COM(2020) 795 *final*.

sistemas[79] būtų visiškai perkelta į nacionalinę teisę ir įgyvendinta, įskaitant valstybių narių teikiamus statistinius duomenis. Tai padės geriau užkirsti kelią piktnaudžiavimui domenų vardais, be kita ko, kai tinkama, neteisėto turinio platinimui, ir siekti, kad būtų prieinami tikslūs registracijos duomenys, toliau bendradarbiaujant su Interneto vardų ir numerių paskyrimo korporacija (ICANN) ir kitomis interneto valdymo sistemos suinteresuotosiomis šalimis, visų pirma per ICANN Vyriausybinio patariamojo komiteto Visuomenės saugumo darbo grupe. Peržiūrėtoje TIS direktyvoje atitinkamai numatyta išlaikyti tikslias ir išsamias domenų vardų ir registracijos duomenų arba WHOIS duomenų bazes ir suteikti teisėtą prieigą prie tokių duomenų, kurie yra būtini siekiant užtikrinti DNS saugumą, stabilumą ir atsparumą.

Komisija taip pat toliau dirbs, kad užtikrintų tinkamus kanalus ir paaiškintų taisykles, kad būtų galima gauti tarpvalstybinę prieigą prie elektroninių įrodymų atliekant nusikalstamų veikų tyrimus (kurių reikia 85 proc. tyrimų, o 65 proc. visų prašymų pateikiama kitoje jurisdikcijoje esantiems paslaugų teikėjams), palengvindama „e. įrodymų rinkinio“ ir praktinių priemonių priėmimą ir paskesnį įgyvendinimą[80]. Siekiant suteikti specialistams veiksmingą priemonę, labai svarbu, kad Europos Parlamentas ir Taryba greitai priimtų pasiūlymus dėl e. įrodymų. Elektroninius įrodymus turi būti įmanoma perskaityti, todėl Komisija toliau dirbs remdama teisėsaugos gebėjimus skaitmeninių tyrimų srityje, be kita ko, spręs šifravimo, su kuriuo susiduriama atliekant nusikaltimų tyrimus, klausimus, ir kartu toliau besąlygiškai vykdys savo funkciją apsaugoti pagrindines teises ir užtikrinti kibernetinį saugumą.

2.3. ES kibernetinio saugumo diplomatijos priemonių rinkinys

ES naudojasi savo **Kibernetinio saugumo diplomatijos priemonių rinkiniu**[81], kad užkirstų kelią kibernetinei kenkimo veiklai, sutrukdytų jai, atgrasytų nuo jos ir į ją reaguotų. 2019 m. gegužės mėn. nustačius tikslinių ribojamųjų priemonių prieš kibernetinius išpuolius teisinę sistemą[82], ES 2020 m. liepos mėn. laikydamasi nustatytos tvarkos į sąrašą įtraukė šešis asmenis ir tris subjektus, atsakingus už kibernetinius išpuolius, darančius poveikį ES ir jos valstybėms narėms, arba dalyvavusius juos darant[83]. Dar du asmenys ir viena įstaiga buvo

[79] Direktyva 2013/40/ES dėl atakų prieš informacines sistemas.

[80] COM(2018) 225 ir 226; C(2020) 2779 *final*. Visų pirma, projektui SIRIUS neseniai buvo skirtas papildomas finansavimas pagal partnerystės priemonę, siekiant pagerinti kanalus, kuriais būtų galima gauti teisėtą tarpvalstybinę prieigą prie elektroninių įrodymų nusikalstamų veikų tyrimams atlikti (kurių reikia 85 proc. sunkių nusikaltimų tyrimų, o 65 proc. visų prašymų pateikiama kitoje jurisdikcijoje esantiems paslaugų teikėjams)), ir nustatyti tarptautinio lygmens suderintas taisykles.

[81] https://www.consilium.europa.eu/lt/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

[82] 2019 m. gegužės 17 d. Tarybos sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais (OL L 129I, 2019 5 17, p. 13) ir 2019 m. gegužės 17 d. Tarybos reglamentas (ES) 2019/796
dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais (OL L 129I, 2019 5 17, p. 1).

[83] 2020 m. liepos 30 d. Tarybos sprendimas (BUSP) 2020/1127, iš dalies keičiantis Sprendimą (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais (ST/9564/2020/INIT) (OL L 246, 2020 7 30, p. 12–17) ir 2020 m. liepos 30 d. Tarybos įgyvendinimo reglamentas (ES) 2020/1125, kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms (ST/9568/2020/INIT) (OL L 246, 2020 7 30, p. 4–9).

įtraukti į sąrašą 2020 m. spalio mėn.[84]. Kibernetinė kenkimo veikla, įskaitant ilgalaikes pasekmes sukeliančią veiklą, turėtų būti stabdoma veiksmingu ir visapusišku bendru ES diplomatiniu atsaku, pasitelkus pačias įvairiausias ES lygmens priemones.

Greitam ir veiksmingam bendram ES diplomatiniam atsakui reikalingas patikimas bendras informuotumas apie padėtį ir gebėjimas greitai parengti bendrą ES poziciją. Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai skatins ir sudarys palankesnes sąlygas įsteigti **valstybių narių ES kibernetinės žvalgybos darbo grupę**, veikiančią ES žvalgybos ir situacijų centre (INTCEN), kad būtų plėtojamas strateginės žvalgybos bendradarbiavimas kibernetinių grėsmių ir veiklos srityje. Šiuo darbu bus toliau remiamas ES informuotumas apie padėtį ir sprendimų dėl bendro diplomatinio atsako priėmimas. Darbo grupė turi naudotis turimomis struktūromis[85], prireikus įskaitant struktūras, kurios apima platesnę hibridinio ir užsienio kišimosi grėsmę, rinkti informaciją ir vertinti informuotumą apie padėtį.

Siekdamas stiprinti savo gebėjimą užkirsti kelią piktavališkam elgesiui kibernetinėje erdvėje, jam sutrukdyti, atgrasyti nuo jo ir į jį reaguoti, vyriausiasis įgaliotinis, bendradarbiaudamas su Komisija pagal jos kompetenciją, pateiks pasiūlymą ES, kuriuo bus siekiama išsamiau apibrėžti ES **kibernetines atgrasymo priemones**. Remiantis iki šiol atliktu darbu naudojant Kibernetinio saugumo diplomatijos priemonių rinkinį, šia pozicija turėtų būti prisidedama prie atsakingo valstybių elgesio ir bendradarbiavimo kibernetinėje erdvėje ir nurodoma konkreti kryptis kovoje su tais kibernetiniais išpuoliais, kurie turi didžiausią poveikį, visų pirma tais, kurie daro poveikį mūsų ypatingos svarbos infrastruktūros objektams, demokratinėms institucijoms ir procesams[86], taip pat išpuoliais prieš tiekimo grandinę ir intelektinės nuosavybės vagystėmis pasinaudojant kibernetine erdve. Pozicijoje turėtų būti išdėstyta, kaip ES ir valstybės narės galėtų pasinaudoti savo politinėmis, ekonominėmis, diplomatinėmis, teisinėmis ir strateginėmis komunikacijos priemonėmis kovodamos su kibernetine kenkimo veikla, ir nagrinėjama, kaip ES ir valstybės narės galėtų didinti savo gebėjimą išaiškinti kibernetinės kenkimo veiklos vykdytojus. Vyriausiasis įgaliotinis, bendradarbiaudamas su Taryba ir Komisija, taip pat ketina svarstyti **papildomas Kibernetinio saugumo diplomatijos priemonių rinkinio priemones**, įskaitant galimybę taikyti papildomas ribojamąsias priemones, taip pat nagrinėja galimybes **kvalifikuota balsų dauguma sudaryti sąrašus pagal horizontaliųjų sankcijų už kibernetinius išpuolius režimą**. Be to, ES turėtų toliau dėti pastangas siekdama **stiprinti bendradarbiavimą su tarptautiniais partneriais**, įskaitant NATO, kad būtų didinamas bendras supratimas apie grėsmių padėtį, plėtojami bendradarbiavimo mechanizmai ir nustatomi bendri diplomatinio atsako veiksmai.

Bendradarbiaudamas su Komisija vyriausiasis įgaliotinis taip pat pasiūlys atnaujinti **Kibernetinio saugumo diplomatijos priemonių rinkinio įgyvendinimo gaires[87]**, be kita

[84] 2020 m. spalio 22 d. Tarybos sprendimas (BUSP) 2020/1537, iš dalies keičiantis Sprendimą (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais (OL L 351I, 2020 10 22, p. 5–7) ir 2020 m. spalio 22 d. Tarybos įgyvendinimo reglamentas (ES) 2020/1536, kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms (OL L 351I, 2020 10 22, p. 1–4).

[85] Pavyzdžiui, ES bendru žvalgybinės informacijos analizės centru (SIAC) ir prireikus pagal PESCO nustatytais atitinkamais projektais, taip pat 2018 m. Skubaus informavimo sistema (RAS), sukurta siekiant remti bendrą ES požiūrį į kovą su dezinformacija.

[86] Visų pirma siekiant sąveikos su iniciatyvomis pagal Europos demokratijos veiksmų planą.

[87] 13007/17

ko, siekiant padidinti sprendimų priėmimo proceso veiksmingumą, ir toliau reguliariai rengs pratybas bei vertinimus, susijusius su Kibernetinio saugumo diplomatijos priemonių rinkiniu. Be to, ES turėtų toliau **integruoti Kibernetinio saugumo diplomatijos priemonių rinkinį į ES krizių valdymo mechanizmus**, siekti sąveikos su kovos su hibridinėmis grėsmėmis, dezinformacija ir užsienio subjektų kišimusi veiksmais pagal Bendrą kovos su mišriomis grėsmėmis sistemą[88] ir Europos demokratijos veiksmų planą. Šiomis aplinkybėmis ES turėtų apsvarstyti Kibernetinio saugumo diplomatijos priemonių rinkinio ir galimo ES sutarties 42 straipsnio 7 dalies ir SESV 222 straipsnio taikymo sąveiką[89].

2.4. Kibernetinės gynybos pajėgumų didinimas

ES ir valstybės narės turi didinti savo gebėjimą užkirsti kelią kibernetinėms grėsmėms ir į jas reaguoti laikydamosi 2016 m. Visuotinėje ES strategijoje nustatyto ES tikslų masto[90]. Šiuo tikslu vyriausiasis įgaliotinis, bendradarbiaudamas su Komisija, pateiks **peržiūrėtus ES kibernetinės gynybos politikos metmenis (CDPF)**, kad būtų dar labiau sustiprintas ES subjektų[91] veiklos koordinavimas ir bendradarbiavimas, taip pat veiklos koordinavimas ir bendradarbiavimas su valstybėmis narėmis ir tarp jų, įskaitant kiek tai susiję su bendros saugumo ir gynybos politikos (BSGP) misijomis ir operacijomis. Remiantis ES kibernetinės gynybos politikos metmenimis bus rengiamas strateginis kelrodis[92] užtikrinant, kad kibernetinis saugumas ir kibernetinė gynyba būtų toliau integruojami į platesnę saugumo ir gynybos darbotvarkę.

2018 m. ES nustatė, kad kibernetinės erdvė yra operacijų sritis[93]. Būsimoje ES karinio komiteto **karinėje vizijoje ir strategijoje dėl kibernetinės erdvės kaip operacijų srities** turėtų būti išsamiau apibrėžta, kaip kibernetinėje erdvėje, kaip operacijų srityje, įgyjama teisė vykdyti ES BSGP karines misija ir operacijas. Europos gynybos agentūros kuriamas **karinis CERT tinklas**[94] dar labiau padės reikšmingai padidinti valstybių narių bendradarbiavimą. Be to, siekiant užtikrinti ypatingos svarbos kosmoso infrastruktūros objektų, valdomų pagal Kosmoso programą, kibernetinį saugumą, bus sustiprinta Europos kosmoso programos agentūra, visų pirma GALILEO saugumo stebėsenos centras, o į jos įgaliojimus bus įtrauktas kitas ypatingos svarbos Kosmoso programos turtas.

ES ir valstybės narės turėtų toliau skatinti **plėtoti pažangiausius kibernetinės gynybos pajėgumus**, pasitelkdamos įvairias ES politikos kryptis ir priemones, visų pirma ES kibernetinės gynybos politikos metmenis, ir prireikus remdamosi EGA darbu. Šiuo tikslu daug dėmesio reikia skirti pagrindinių technologijų, tokių kaip dirbtinis intelektas, šifravimas ir kvantinė kompiuterija, kūrimui ir naudojimui. Atsižvelgdama į 2018 m. ES pajėgumų plėtojimo prioritetus[95] ir remdamasi pirmosios visapusiškos suderintos metinės peržiūros

[88] https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52016JC0018&from=LT.
[89] Atitinkamai tarpusavio gynybos sąlyga ir solidarumo sąlyga.
[90] Tarybos išvados (14149/16) dėl Visuotinės ES strategijos įgyvendinimo saugumo ir gynybos srityje.
[91] Visų pirma EIVT, įskaitant ES karinį štabą (EUMS), Europos saugumo ir gynybos koledžą (ESGK), Komisiją ir ES agentūras, pirmiausia Europos gynybos agentūrą (EGA).
[92] 2020 m. birželio 17 d. Tarybos išvados dėl saugumo ir gynybos (8910/20)
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/lt/pdf.
[94] ES karinio CERT tinklo sukūrimas atitinka 2018 m. kibernetinės gynybos politikos programoje nustatytą tikslą ir juo siekiama skatinti aktyvų ES valstybių narių karinių CERT bendradarbiavimą ir keitimąsi informacija.
[95] 2018 m. birželio mėn. valstybės narės EGA valdančiojoje taryboje susitarė teikti gaires bendradarbiavimui gynybos srityje ES lygmeniu.

gynybos srityje (CARD) ataskaitos išvadomis[96], ES turėtų toliau puoselėti valstybių narių bendradarbiavimą **kibernetinės gynybos mokslinių tyrimų, inovacijų ir pajėgumų plėtojimo** srityse, ragindama valstybes nares visapusiškai pasinaudoti **nuolatinio struktūrizuoto bendradarbiavimo (PESCO)[97]** ir **EGF[98]** teikiamomis galimybėmis.

Į būsimą **Komisijos civilinės, gynybos ir kosmoso pramonės sinergijos veiksmų planą**, pateiksimą 2021 m. pirmąjį ketvirtį, bus įtraukti veiksmai, kuriais bus toliau remiama sinergija programų, technologijų, inovacijų ir startuolių lygmeniu, laikantis atitinkamų programų valdymo reikalavimų[99].

Be to, siekiant remti dalijimąsi informacija ir savitarpio paramą turėtų būti plėtojama atitinkama kibernetinės gynybos iniciatyvų, įgyvendinamų pagal kitas sistemas, įskaitant su kibernetine erdve susijusius valstybių narių bendradarbiavimo projektus[100] pagal PESCO, ir kartu su ES kibernetinio saugumo struktūromis, sinergija ir sąsajos.

Strateginės iniciatyvos

ES turėtų:

- baigti kurti Europos kibernetinio saugumo krizių valdymo sistemą ir nustatyti bendro kibernetinio saugumo padalinio įsteigimo procesą, etapus ir tvarkaraštį;
- toliau įgyvendinti kovos su elektroniniais nusikaltimais darbotvarkę pagal Saugumo sąjungos strategiją;
- skatinti ir palengvinti valstybių narių kibernetinės žvalgybos darbo grupės, veikiančios EU INTCEN, įsteigimą;
- tobulinti ES kibernetinio atgrasymo poziciją siekiant užkirsti kelią ir sutrukdyti kibernetinei kenkimo veiklai, atgrasyti nuo jos ir į ją reaguoti;
- persvarstyti kibernetinės gynybos politikos sistemą;
- palengvinti BSGP karinėms misijoms ir operacijoms skirtų ES karinės vizijos ir strategijos kibernetinėje erdvėje, kaip operacijų srityje, plėtojimą;
- remti civilinės, gynybos ir kosmoso pramonės šakų sinergiją ir
- stiprinti ypatingos svarbos kosmoso infrastruktūros objektų kibernetinį saugumą pagal Kosmoso programą.

[96] 2020 m. lapkričio mėn. patvirtinta gynybos ministrų EGA valdančiojoje taryboje. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card).

[97] Dabar vykdoma keletas su kibernetine erdve susijusių PESCO projektų, visų pirma Dalijimosi informacija apie reagavimą į kibernetines grėsmes ir incidentus platforma, Greitojo reagavimo į kibernetinius incidentus komandos ir savitarpio pagalba kibernetinio saugumo srityje, ES kibernetinės mokslinės kompetencijos ir inovacijų centras ir Kibernetinių ir informacijos sričių koordinavimo centras (CIDCC).

[98] Pagal EGF Komisija jau nustatė galimybes, susijusias su potencialiais bendradarbiavimu grindžiamais kibernetinės gynybos mokslinių tyrimų ir technologinės plėtros veiksmais, kuriais siekiama stiprinti bendradarbiavimą, inovacinius pajėgumus ir gynybos pramonės konkurencingumą.

[99] Pavyzdžiui, programos „Europos horizontas“, Skaitmeninės Europos ir EGF.

[100] https://pesco.europa.eu/.

3. PASAULINĖS ATVIROS KIBERNETINĖS ERDVĖS KŪRIMAS

ES turėtų toliau bendradarbiauti su tarptautiniais partneriais, kad skatintų kibernetinės erdvės politinį modelį ir viziją, grindžiamus teisinės valstybės principu, žmogaus teisėmis, pagrindinėmis laisvėmis ir demokratinėmis vertybėmis, kuriomis visame pasaulyje užtikrinamas socialinis, ekonominis ir politinis vystymasis ir prisidedama prie saugumo sąjungos kūrimo. Tarptautinis bendradarbiavimas yra labai svarbus siekiant užtikrinti kibernetinės erdvės visuotinumą, atvirumą, stabilumą ir saugumą. Šiuo tikslu ES turėtų toliau bendradarbiauti su trečiosiomis valstybėmis, tarptautinėmis organizacijomis ir įvairių suinteresuotųjų šalių bendruomene, kad būtų plėtojama ir įgyvendinama nuosekli ir holistinė tarptautinė kibernetinė politika, atsižvelgiant į gausėjančias naujųjų technologijų, vidaus saugumo ir užsienio saugumo ir gynybos politikos ekonominių aspektų sąsajas. ES, kaip tvirtas ekonomikos ir prekybos blokas, pagrįstas pagrindinėmis demokratinėmis vertybėmis, pagarba teisinei valstybei ir pagrindinėms teisėms, taip pat turi unikalią galimybę vadovauti nustatant ir skatinant tarptautines normas ir standartus.

3.1. ES lyderystė kibernetinės erdvės standartų, normų ir sistemų srityje

Žengiant tarptautinės standartizacijos link

Siekdama skatinti ir ginti savo kibernetinės erdvės viziją tarptautiniu lygmeniu, ES privalo **aktyviau dalyvauti tarptautiniuose standartizacijos procesuose ir jiems vadovauti, taip pat stiprinti atstovavimą tarptautinėse ir Europos standartizacijos institucijose ir kitose standartus rengiančiose organizacijose**[101]. Kadangi skaitmeninės technologijos kuriamos sparčiai, tarptautiniai standartai tampa vis didesne paspirtimi tradicinėms reguliavimo pastangoms tokiose srityse kaip dirbtinis intelektas, debesija, kvantinė kompiuterija ir kvantinė komunikacija. Siekdamos įgyvendinti savo politinę ir ideologinę darbotvarkę, kuri dažnai neatitinka ES vertybių, trečiosios valstybės vis dažniau naudojasi tarptautiniais standartais. Be to, auga konkuruojančių tarptautinių standartų sistemų rizika, lemianti susiskaidymą.

Siekiant užtikrinti, kad internetas išliktų visuotinis ir atviras, kad technologijos būtų orientuotos į žmogų ir jo privatumą ir kad jų naudojimas būtų teisėtas, saugus ir etiškas, labai svarbu rengti ES vertybes atitinkančius tarptautinius standartus, taikytinus tokioms sritims kaip besiformuojančios technologijos ir pagrindinė interneto architektūra. Būsimoje standartizacijos strategijoje ES turėtų apibrėžti savo **tarptautinės standartizacijos tikslus** ir vykdyti aktyvią ir koordinuotą informavimo veiklą, kad šie tikslai būtų skatinami tarptautiniu lygmeniu. Reikėtų siekti glaudžiau bendradarbiauti ir dalytis našta su panašiai mąstančiais partneriais ir Europos suinteresuotosiomis šalimis.

Atsakingo valstybių elgesio kibernetinėje erdvėje skatinimas

ES toliau bendradarbiauja su tarptautiniais partneriais, siekdama pastūmėti kurti ir skatinti pasaulinę, atvirą, stabilią ir saugią kibernetinę erdvę, kurioje **gerbiama tarptautinė teisė, visų pirma Jungtinių Tautų (JT) chartija**[102], ir laikomasi **savanoriškų neprivalomų**

[101] Pavyzdžiui, Tarptautinė standartizacijos organizacija (ISO), Tarptautinė elektrotechnikos komisija (IEC), Tarptautinė telekomunikacijų sąjunga (ITU), Europos standartizacijos komitetas (CEN), Europos elektrotechnikos standartizacijos komitetas (CENELEC), Europos telekomunikacijų standartų institutas (ETSI), Interneto inžinerijos grupė (IETF), 3-iosios kartos partnerystės projektas (3GPP) ir Elektros ir elektronikos inžinierių institutas (IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/.

atsakingo valstybių elgesio normų, taisyklių ir principų[103]. Pakrikus veiksmingoms daugiašalėms diskusijoms dėl tarptautinio saugumo kibernetinėje erdvėje, akivaizdu, kad ES ir valstybėms narėms reikia laikytis aktyvesnės pozicijos JT ir kituose atitinkamuose tarptautiniuose forumuose vykstančiose diskusijose. ES turi geriausias galimybes **paskubinti, koordinuoti ir konsoliduoti valstybių narių pozicijas tarptautiniuose forumuose** ir turėtų **parengti ES poziciją dėl tarptautinės teisės taikymo kibernetinėje erdvėje**. Vyriausiasis įgaliotinis kartu su valstybėmis narėmis taip pat siekia pateikti įtraukų ir bendru sutarimu grindžiamą pasiūlymą dėl politinio įsipareigojimo dėl JT **veiksmų programos, kuria siekiama skatinti atsakingą valstybių elgesį kibernetinėje erdvėje**[104]. Esama *acquis*, patvirtinta JT Generalinės Asamblėjos[105], grindžiama veiksmų programa nustatoma bendradarbiavimo ir keitimosi geriausios praktikos pavyzdžiais JT platforma ir siūloma sukurti mechanizmą, kuriuo būtų praktiškai įgyvendinamos atsakingo valstybių elgesio normos ir skatinamas pajėgumų stiprinimas. Be to, vyriausiasis įgaliotinis siekia stiprinti ir skatinti valstybių **tarpusavio pasitikėjimo stiprinimo priemonių** įgyvendinimą, įskaitant dalijimąsi geriausios praktikos pavyzdžiais regioniniu ir daugiašaliu lygmenimis ir prisidedant prie įvairių regionų bendradarbiavimo.

Didesnis visuotinis junglumas neturėtų lemti cenzūros, masinio sekimo, duomenų privatumo pažeidimų ir represijų prieš pilietinę visuomenę, akademinę bendruomenę ir piliečius. ES turėtų toliau vadovauti **žmogaus teisių ir pagrindinių laisvių** apsaugai ir skatinimui internete. Šiuo tikslu ES turėtų skatinti toliau laikytis tarptautinės žmogaus teisių teisės ir standartų[106], vykdyti savo 2020–2024 m. veiksmų planą žmogaus teisių ir demokratijos srityje[107] ir toliau įgyvendinti ES žmogaus teisių gaires dėl saviraiškos laisvės internete ir realiame gyvenime[108], **suteikdama naują postūmį praktiniam ES priemonių taikymui**. ES turėtų nuolat stengtis **apsaugoti žmogaus teisių gynėjus, pilietinę visuomenę ir akademinę bendruomenę, dirbančius tokios srityse kaip kibernetinis saugumas, duomenų privatumas, sekimas ir cenzūra internete**. Šiuo tikslu ES turėtų teikti tolesnes praktines gaires, skatinti geriausią praktiką ir dėti daugiau pastangų, kad būtų užkirstas kelias piktnaudžiavimui besiformuojančiomis technologijomis, visų pirma prireikus taikant diplomatines priemones ir vykdant tokių technologijų eksporto kontrolę. ES taip pat turėtų toliau kovoti už pažeidžiamiausių visuomenės narių apsaugą internete, siūlydama teisės aktus, kuriais siekiama geriau apsaugoti vaikus nuo seksualinės prievartos ir išnaudojimo, ir Vaiko teisių strategiją.

Budapešto konvencija dėl elektroninių nusikaltimų

ES toliau remia trečiąsias valstybes, kurios nori prisijungti prie **Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų**, ir siekia užbaigti rengti **Budapešto konvencijos antrąjį papildomą protokolą**, į kurį įtrauktos priemonės ir apsaugos priemonės

[103] Kaip nurodyta atitinkamose Jungtinių Tautų Generalinės Asamblėjos (JT GA) patvirtintose Vyriausybių ekspertų grupių dėl atsakingo valstybių elgesio kibernetinėje erdvėje gerinimo tarptautinio saugumo kontekste (UNGGE) ataskaitose, visų pirma 2015, 2013 ir 2010 m. ataskaitose.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] Kaip nurodyta atitinkamose JT GA patvirtintose Vyriausybių ekspertų grupių dėl atsakingo valstybių elgesio kibernetinėje erdvėje gerinimo tarptautinio saugumo kontekste (UNGGE) ataskaitose, visų pirma 2015, 2013 ir 2010 m. ataskaitose.

[106] Visų pirma, JT Chartijos ir Visuotinės žmogaus teisių deklaracijos.

[107] https://www.consilium.europa.eu/lt/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

tarptautiniam teisėsaugos ir teisminių institucijų bendradarbiavimui, taip pat jų bendradarbiavimui su paslaugų teikėjais kitose šalyse, dėl kurio Komisija dalyvauja derybose ES vardu, gerinti[109]. Dabartinė JT lygmens iniciatyva dėl naujos teisinės priemonės kovai su kibernetiniais nusikaltimais gali padidinti susiskaidymą ir sulėtinti labai reikalingas nacionalines reformas bei susijusias gebėjimų stiprinimo pastangas, o tai gali trukdyti veiksmingam tarptautiniam bendradarbiavimui kovoje su kibernetiniais nusikaltimais: ES nemano, kad JT lygmeniu reikalingos naujos teisinės priemonės kovai su kibernetiniais nusikaltimais. ES toliau dalyvauja **daugiašaliuose informacijos mainuose kibernetinių nusikaltimų klausimais**, kad užtikrintų pagarbą žmogaus teisėms ir pagrindinėms laisvėms, pasitelkdama įtraukumą, skaidrumą ir atsižvelgdama į turimas ekspertines žinias, kad pridėtinė vertė būtų užtikrinta visiems.

3.2. Bendradarbiavimas su partneriais ir įvairių suinteresuotųjų šalių bendruomene

ES turėtų **stiprinti ir plėtoti savo dialogus kibernetikos klausimais su trečiosiomis valstybėmis**, kad skatintų savo kibernetinės erdvės vertybes ir viziją, keistųsi geriausios praktikos pavyzdžiais ir siektų veiksmingiau bendradarbiauti. ES taip pat turėtų pradėti **struktūrinius mainus su regioninėmis organizacijomis**, pavyzdžiui, Afrikos Sąjunga, ASEAN regioniniu forumu, Amerikos valstybių organizacija ir Europos saugumo ir bendradarbiavimo organizacija. Kartu, kai įmanoma ir tikslinga, ES turėtų stengtis rasti bendrą sutarimą su kitais partneriais, remdamasi bendro intereso klausimais. Bendradarbiaudama su ES delegacijomis ir atitinkamais atvejais valstybių narių ambasadomis visame pasaulyje, ES turėtų suformuoti neformalų **ES kibernetinio saugumo diplomatijos tinklą**, siekdama skatinti ES kibernetinės erdvės viziją, keistis informacija ir nuolat koordinuoti pokyčius kibernetinėje erdvėje[110].

Remdamasi 2016 m. liepos 8 d.[111] ir 2018 m. liepos 10 d.[112] bendromis deklaracijomis, ES toliau turėtų skatinti **ES ir NATO bendradarbiavimą**, visų pirma kibernetinės gynybos sąveikumo reikalavimų srityje. Šiomis aplinkybėmis ES turėtų toliau siekti, kad atitinkamos BSGP struktūros būtų susietos su NATO federalinių misijų tinklu, kad prireikus būtų užtikrintas tinklo sąveikumas su NATO ir partneriais. Be to, turėtų būti toliau nagrinėjamas ES ir NATO bendradarbiavimas švietimo, mokymo ir pratybų srityse, be kita ko, siekiant Europos saugumo ir gynybos koledžo ir NATO bendradarbiaujamosios kibernetinės gynybos kompetencijos centro sinergijos.

Vadovaudamasi savo vertybėmis, ES tvirtai remia ir skatina **interneto valdymo modelį, grindžiamą įvairių suinteresuotųjų šalių bendradarbiavimu**. Kontroliuoti interneto neturėtų siekti joks pavienis subjektas, vyriausybė ar tarptautinė organizacija. ES turėtų toliau dalyvauti forumuose[113], kad stiprintų bendradarbiavimą ir užtikrintų pagrindinių teisių ir laisvių, visų pirma teisės į orumą ir privatumą, saviraiškos bei informacijos laisvės, apsaugą. Siekiant skatinti įvairių suinteresuotųjų šalių bendradarbiavimą kibernetinio saugumo klausimais, Komisija ir vyriausiasis įgaliotinis savo kompetencijos ribose siekia stiprinti **nuolatinius ir struktūrizuotus mainus su suinteresuotosiomis šalimis**, įskaitant privatųjį

[109] 2019 m. birželio mėn. Tarybos sprendimas (Nr. 9116/19).
[110] Prireikus ji taip pat galėtų pasinaudoti neoficialaus ES kibernetinės diplomatijos tinklo, kuriame dalyvauja valstybių narių užsienio reikalų ministerijos, veikla.
[111] https://www.consilium.europa.eu/lt/press/press-releases/2016/07/08/eu-nato-joint-declaration/.
[112] https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Pavyzdžiui, Interneto vardų ir numerių paskyrimo korporacijoje (ICANN) ir Interneto valdymo forume (IGF).

sektorių, akademinę bendruomenę ir pilietinę visuomenę, pabrėždami, kad dėl tarpusavyje susijusio kibernetinės erdvės pobūdžio visos suinteresuotosios šalys turi keistis informacija ir prisiimti konkrečią atsakomybę, kad kibernetinė erdvė išliktų pasaulinė, atvira, stabili ir saugi. Šios pastangos bus vertingas indėlis imantis galimų svarbių veiksmų ES lygmeniu.

3.3. Visuotinių pajėgumų didinti pasaulinį atsparumą stiprinimas

Siekdama užtikrinti, kad visos šalys galėtų pasinaudoti socialine, ekonomine ir politine interneto ir technologijų naudojimo teikiama nauda, ES toliau padeda savo partneriams didinti savo kibernetinį atsparumą ir stiprinti pajėgumus tirti kibernetinius nusikaltimus, patraukti už juos baudžiamojon atsakomybėn ir kovoti su kibernetinėmis grėsmėmis. Siekdama užtikrinti bendrą nuoseklumą, ES turėtų parengti **ES išorės kibernetinių pajėgumų stiprinimo planą**, kad šios pastangos būtų dedamos vadovaujantis jos išorės kibernetinių pajėgumų stiprinimo gairėmis[114] ir Darnaus vystymosi darbotvarke iki 2030 m.[115] Darbotvarkėje turėtų būti pasinaudota valstybių narių ir atitinkamų ES institucijų, įstaigų bei agentūrų ekspertinėmis žiniomis ir iniciatyvomis, įskaitant ES kibernetinių pajėgumų stiprinimo tinklą[116] laikantis jų atitinkamų įgaliojimų. Turi būti sukurta **ES kibernetinių pajėgumų stiprinimo valdyba**, kurioje dalyvautų atitinkamos ES institucinės suinteresuotosios šalys ir kuri stebėtų pažangą, taip pat nustatytų tolesnę sinergiją ir galimas spragas. Be to, ji gali remti glaudesnį bendradarbiavimą su valstybėmis narėmis, taip pat su viešojo ir privačiojo sektorių partneriais ir kitomis atitinkamomis tarptautinėmis organizacijomis, kad būtų užtikrintas pastangų koordinavimas ir išvengta dubliavimosi.

ES kibernetinių pajėgumų stiprinimas toliau turėtų būti sutelktas į Vakarų Balkanus ir ES kaimynines šalis, taip pat į šalis partneres, kuriose vyksta spartus skaitmeninis vystymasis. ES pastangomis turėtų būti remiamas šalių partnerių teisės aktų ir politikos rengimas laikantis atitinkamos ES kibernetinės diplomatijos politikos ir standartų. Šiomis aplinkybėmis ES pajėgumų stiprinimo pastangos skaitmeninimo srityje turėtų apimti kibernetinį saugumą kaip įprastą aspektą. Šiuo tikslu ES turėtų parengti mokymo programą, skirtą ES darbuotojams, atsakingiems už ES skaitmeninių ir kibernetinių išorės pajėgumų stiprinimo pastangų įgyvendinimą. ES taip pat turėtų padėti šioms šalims spręsti augančią kibernetinės kenkimo veiklos, kuri daro žalą jų visuomenių vystymuisi ir **demokratinių sistemų vientisumui bei saugumui**, problemą, atsižvelgiant į pastangas pagal Europos demokratijos veiksmų planą. Šiuo atžvilgiu galėtų būti ypač naudingas ES valstybių narių, taip pat atitinkamų ES agentūrų ir trečiųjų valstybių tarpusavio mokymasis.

Galiausiai, atsižvelgiant į 2018 m. susitarimą dėl civilinių BSGP pajėgumų[117], civilinės BSGP misijos taip pat gali prisidėti prie platesnio ES atsako sprendžiant kibernetinio saugumo problemas, visų pirma įtvirtinant teisinės valstybės principą šalyse partnerėse, taip pat jų teisėsaugos ir civilinių administracijų pajėgumus.

Strateginės iniciatyvos

ES turėtų:

- apibrėžti tarptautinių standartizacijos procesų tikslus ir skatinti jų laikytis tarptautiniu

[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf.
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm.
[116] https://www.eucybernet.eu/.
[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/lt/pdf.

lygmeniu;

- didinti tarptautinį saugumą ir stabilumą kibernetinėje erdvėje, visų pirma Jungtinėse Tautose pateikdama ES ir jos valstybių narių pasiūlymą dėl veiksmų programos, kuria siekiama skatinti atsakingą valstybių elgesį kibernetinėje erdvėje;
- teikti praktines gaires dėl žmogaus teisių ir pagrindinių laisvių taikymo kibernetinėje erdvėje;
- geriau apsaugoti vaikus nuo seksualinės prievartos ir išnaudojimo, taip pat parengti Vaiko teisių strategiją;
- stiprinti Budapešto konvenciją dėl elektroninių nusikaltimų ir skatinti jos laikytis, be kita ko, rengiant Budapešto konvencijos antrąjį papildomą protokolą;
- plėsti ES dialogą kibernetikos klausimais su trečiosiomis valstybėmis, regioninėmis ir tarptautinėmis organizacijomis, be kita ko, pasitelkiant neoficialų ES kibernetinės diplomatijos tinklą;
- stiprinti informacijos mainus su įvairių suinteresuotųjų šalių bendruomene, visų pirma nuolat ir struktūrizuotai keičiantis informacija su privačiuoju sektoriumi, akademine bendruomene ir pilietine visuomene, ir
- pasiūlyti ES išorės kibernetinių pajėgumų stiprinimo planą ir ES kibernetinių pajėgumų stiprinimo valdybą.

III. KIBERNETINIS SAUGUMAS ES INSTITUCIJOSE, ĮSTAIGOSE IR AGENTŪROSE

Dėl didelio politinio matomumo, labai svarbių užduočių koordinuojant itin opius klausimus ir vaidmens valdant dideles viešųjų lėšų sumas **ES institucijos, įstaigos ir agentūros yra nuolatiniai kibernetinių išpuolių**, visų pirma kibernetinio šnipinėjimo, **taikiniai**. Tačiau šių subjektų kibernetinio atsparumo lygis ir gebėjimų aptikti kibernetinę kenkimo veiklą ir į ją reaguoti branda labai skiriasi. Todėl būtina pagerinti bendrą kibernetinio saugumo lygį taikant nuoseklias ir vienodas taisykles.

Informacijos saugumo srityje padaryta pažanga užtikrinant didesnį **ES įslaptintos informacijos ir neskelbtinos neįslaptintos informacijos apsaugos taisyklių** nuoseklumą. Tačiau įslaptintos informacijos sistemų sąveikumas išlieka ribotas, o tai trukdo sklandžiai perduoti informaciją tarp įvairių subjektų. Reikėtų toliau daryti pažangą, kad būtų galima taikyti tarpinstitucinį požiūrį į ES įslaptintos informacijos ir neskelbtinos neįslaptintos informacijos tvarkymą, kuris taip pat galėtų tapti valstybių narių sąveikumo modeliu. Taip pat reikėtų nustatyti atskaitos scenarijų, kuriuo remiantis būtų supaprastintos ryšių su valstybėmis narėmis procedūros. ES taip pat turėtų toliau plėtoti savo gebėjimus palaikyti saugius ryšius su atitinkamais partneriais, kuo platesniu mastu taikydama esamus susitarimus ir procedūras.

Todėl, kaip paskelbta Saugumo sąjungos strategijoje, Komisija **2021 m.** pateiks pasiūlymus dėl **bendrų privalomų informacijos saugumo taisyklių ir bendrų privalomų kibernetinio**

saugumo taisyklių, taikytinų visoms ES institucijoms, įstaigoms ir agentūroms, pagrįstus vykstančiomis ES tarpinstitucinėmis diskusijomis dėl kibernetinio saugumo[118].

Atsižvelgiant į dabartines ir būsimas nuotolinio darbo tendencijas, taip pat reikės toliau investuoti į saugią įrangą, infrastruktūrą ir įrankius, leisiančius dirbti su neskelbtinomis ir įslaptintomis rinkmenomis nuotoliniu būdu.

Be to, vis priešiškesnė kibernetinio saugumo padėtis ir augantis sudėtingesnių kibernetinių išpuolių, darančių poveikį ES institucijoms, įstaigoms ir agentūroms, skaičius lemia poreikį didinti investicijas, reikalingas aukštam kibernetinės brandos lygiui pasiekti. Siekiant didinti visų ES institucijų, įstaigų ir agentūrų informuotumą, kibernetinę higieną ir remti bendrą kibernetinio saugumo kultūrą, kuriama kibernetinio sąmoningumo programa.

Būtina **stiprinti CERT-EU patobulinant finansavimo mechanizmą**, kad būtų padidintas šios tarnybos gebėjimas padėti ES institucijoms, įstaigoms ir agentūroms taikyti naujas kibernetinio saugumo taisykles ir didinti jų kibernetinį atsparumą. Taip pat būtina sustiprinti CERT-EU įgaliojimus, kad ji turėtų stabilių priemonių šiems tikslams pasiekti.

Strateginės iniciatyvos

1. Reglamentas dėl informacijos saugumo ES institucijose, įstaigose ir agentūrose
2. Reglamentas dėl ES institucijų, įstaigų ir agentūrų bendrų kibernetinio saugumo taisyklių
3. Naujas CERT-EU teisinis pagrindas siekiant sustiprinti jos įgaliojimus ir finansavimą.

IV. IŠVADOS

Suderintas šios strategijos įgyvendinimas padės užtikrinti ES skaitmeninio dešimtmečio kibernetinį saugumą, sukurti saugumo sąjungą ir stiprinti ES poziciją pasaulyje.

ES turėtų nutiesti kelią pasaulinio lygio sprendimų standartams bei normoms ir kibernetinio saugumo standartams, skirtiems svarbiausioms paslaugoms ir ypatingos svarbos infrastruktūros objektams, taip pat naujų technologijų kūrimui ir taikymui. Kiekviena internetu besinaudojanti organizacija ir asmuo yra sprendimo, kuriuo užtikrinama saugi kibernetinė skaitmeninė transformacija, dalis.

Komisija ir vyriausiasis įgaliotinis, atsižvelgdami į atitinkamas savo kompetencijos sritis, stebės šios strategijos įgyvendinimo pažangą ir parengs vertinimo kriterijus. Šią stebėseną turėtų padėti vykdyti ENISA ataskaitos ir reguliarios Komisijos saugumo sąjungos ataskaitos. Rezultatai padės siekti artimiausio skaitmeninio dešimtmečio tikslų[119]. Pagal savo atitinkamą kompetenciją Komisija ir vyriausiasis įgaliotinis toliau palaikys ryšius su valstybėmis narėmis, kad nustatytų praktines priemones, skirtas keturioms ES kibernetinio saugumo bendruomenėms ypatingos svarbos infrastruktūros objektų ir vidaus rinkos atsparumo, teisingumo ir teisėsaugos, kibernetinės diplomatijos ir kibernetinės gynybos srityse sujungti. Be to, Komisija ir vyriausiasis įgaliotinis toliau bendradarbiaus su įvairių suinteresuotųjų šalių bendruomene, pabrėždami, kad visi internetu besinaudojantys asmenys privalo atlikti

[118] Reguliarios ES tarpinstitucinės diskusijos dėl kibernetinio saugumo yra platesnių ES institucijų informacijos apie skaitmeninės transformacijos galimybes ir iššūkius mainų dalis.
[119] Kaip paskelbta 2021 m. Komisijos darbo programoje.

savo vaidmenį užtikrinant pasaulinę, atvirą, stabilią ir saugią kibernetinę erdvę, kurioje kiekvienas galėtų saugiai gyventi savo skaitmeninį gyvenimą.

Priedas. Tolesni veiksmai, susiję su 5G tinklų kibernetiniu saugumu

Remiantis Komisijos rekomendacijos dėl 5G tinklų kibernetinio saugumo peržiūros rezultatais[120], kituose koordinuoto darbo ES lygmeniu etapuose daugiausia dėmesio reikėtų skirti toliau pateiktoje lentelėje nurodytiems trims pagrindiniams tikslams ir svarbiausiems trumpalaikiams ir vidutinės trukmės laikotarpio veiksmams, kuriuos turi įgyvendinti valstybių narių institucijos, Komisija ir ENISA.

Pirmasis kito etapo prioritetas – **užbaigti priemonių rinkinio įgyvendinimą nacionaliniu lygmeniu ir spręsti 2020 m. liepos mėn. pažangos ataskaitoje nustatytas problemas**. Šiomis aplinkybėmis kai kurioms priemonių rinkinio strateginėms priemonėms būtų naudingas **intensyvesnis koordinavimo darbas arba keitimasis informacija** pagal TIS darbo procesą, kaip jau nurodyta pažangos ataskaitoje, o tai galėtų padėti plėtoti **geriausią praktiką ar gaires**. Kalbant apie technines priemones, ENISA galėtų teikti tolesnę paramą, remdamasi jau atliktu darbu ir išsamesne tam tikrų dalykų analize, taip pat **parengti išsamią visų atitinkamų gairių dėl 5G kibernetinio saugumo reikalavimų judriojo ryšio tinklų operatoriams apžvalgą**.

Antra, valstybės narės pabrėžė, kad svarbu neatsilikti nuo pokyčių **nuolat stebint technologijų, 5G architektūros, grėsmių ir 5G naudojimo atvejų bei taikomųjų programų raidą, taip pat išorės veiksnius**, kad būtų galima **nustatyti ir šalinti naują ar atsirandančią riziką**. Be to, turėtų būti toliau nagrinėjami keli pradinės rizikos analizės aspektai, visų pirma siekiant užtikrinti, kad ji apimtų visą 5G ekosistemą, įskaitant visas atitinkamas tinklo infrastruktūros ir 5G tiekimo grandinės dalis. Nors priemonių rinkinys parengtas kaip lanksti ir pritaikoma priemonė, prireikus vidutinės trukmės laikotarpiu būtų galima jį papildyti arba iš dalies pakeisti, siekiant užtikrinti, kad jis išliktų išsamus ir aktualus.

Trečia, turėtų būti toliau imamasi **ES lygmens veiksmų** siekiant remti ir papildyti priemonių rinkinio tikslus ir juos visapusiškai integruoti į atitinkamas Sąjungos ir Komisijos politikos kryptis, visų pirma imantis tolesnių veiksmų, susijusių su 2020 m. sausio 29 d. Komisijos komunikate dėl priemonių rinkinio[121] paskelbtais veiksmais įvairiausiose srityse (pvz., ES finansavimas saugiems 5G tinklams, investicijos į 5G ir vėlesnės kartos technologijas, prekybos apsaugos priemonės ir konkurencija siekiant išvengti 5G tiekimo rinkos iškraipymų ir pan.).

Prireikus 2021 m. pradžioje pagrindiniai subjektai turėtų susitarti dėl išsamios toliau nurodytų pagrindinių veiksmų tvarkos ir etapų.

1 pagrindinis tikslas. Užtikrinti suderintus nacionalinius veiksmingo rizikos mažinimo metodus visoje ES		
Sritys	**Pagrindiniai trumpalaikiai ir vidutinės trukmės veiksmai**	**Pagrindiniai subjektai**
Priemonių rinkinio	Iki 2021 m. antrojo ketvirčio užbaigti priemonių rinkinio	Valstybių narių

[120] Komisijos ataskaita dėl 2019 m. kovo 26 d. Komisijos rekomendacijos 2019/534 dėl 5G tinklų kibernetinio saugumo poveikio.

[121] 2020 m. sausio 29 d. Komisijos komunikatas „Saugaus 5G ryšio diegimas ES. ES priemonių rinkinio įgyvendinimas“, COM(2020) 50.

įgyvendinimas valstybėse narėse	išvadose rekomenduojamų priemonių įgyvendinimą, periodiškai įvertinant padėtį pagal TIS darbo procesą.	institucijos
Keitimasis informacija ir geriausios praktikos pavyzdžiais, susijusiais su tiekėjams skirtomis strateginėmis priemonėmis	Intensyviau keistis informacija ir apsvarstyti galimus geriausios praktikos pavyzdžius, visų pirma susijusius su: - didelės rizikos tiekėjams taikomais apribojimais (SM03) ir priemonėmis, susijusiomis su valdomų paslaugų teikimu (SM04); - tiekimo grandinės saugumu ir atsparumu, visų pirma atsižvelgiant į BEREC atliktą apklausą apie SM05-SM06.	Valstybių narių institucijos, Komisija
Gebėjimų stiprinimas ir techninių priemonių gairės	Vykdyti išsamias technines analizes ir rengti bendras gaires bei priemones, įskaitant: - išsamią ir dinamišką saugumo kontrolės ir geriausios praktikos 5G saugumo srityje matricą; rekomendacijas, kuriomis remiamas atrinktų priemonių rinkinio techninių priemonių įgyvendinimas.	ENISA, valstybių narių institucijos
2 pagrindinis tikslas. Remti nuolatinį keitimąsi žiniomis ir gebėjimų stiprinimą		
Sritys	**Pagrindiniai trumpalaikiai ir vidutinės trukmės veiksmai**	**Pagrindiniai subjektai**
Nuolatinis žinių kaupimas	Organizuoti žinių apie technologijas ir susijusius uždavinius (atviroji architektūra, 5G savybės, pvz., virtualizavimas, konteinerizavimas, padalijimas ir pan.), grėsmių padėties pokyčius, realius incidentus ir pan. kaupimo veiklą.	ENISA, valstybių narių institucijos, kitos suinteresuotosios šalys
Rizikos vertinimai	Atnaujinti informaciją apie atnaujintus nacionalinius rizikos vertinimus ir ja keistis.	Valstybių narių institucijos, Komisija, ENISA
Bendri ES finansuojami projektai, kuriais remiamas priemonių rinkinio įgyvendinimas	Naudojant ES lėšas teikti finansinę paramą projektams, kuriais remiamas priemonių rinkinio įgyvendinimas, visų pirma pagal Skaitmeninės Europos programą (pvz., nacionalinių institucijų gebėjimų stiprinimo projektai, bandymo stendai ar kiti pažangūs pajėgumai ir pan.).	Valstybių narių institucijos, Komisija
Suinteresuotųjų šalių bendradarbiavimas	Skatinti 5G kibernetinį saugumą užtikrinančių nacionalinių institucijų (pvz., TIS bendradarbiavimo grupės, kibernetinio saugumo institucijų, telekomunikacijų reguliavimo institucijų) ir privačių suinteresuotųjų šalių bendradarbiavimą.	Valstybių narių institucijos, Komisija, ENISA
3 pagrindinis tikslas. Skatinti tiekimo grandinės atsparumą ir kitus ES strateginius saugumo tikslus		
Sritys	**Pagrindiniai trumpalaikiai ir vidutinės trukmės veiksmai**	**Pagrindiniai subjektai**
Standartizavimas	Nustatyti ir įgyvendinti konkretų ES atstovavimo standartų nustatymo institucijose stiprinimo veiksmų planą, kuris būtų TIS pogrupio standartizacijos klausimais tolesnių veiksmų dalis, kad būtų pasiekti konkretūs saugumo tikslai, įskaitant sąveikių sąsajų skatinimą, ir sudarytos palankesnės sąlygos įvairinti tiekėjus.	Valstybių narių institucijos

Tiekimo grandinės atsparumas	– Atlikti išsamią 5G ekosistemos ir tiekimo grandinės analizę, kad būtų galima geriau nustatyti ir stebėti pagrindinius išteklius ir galimą kritinę priklausomybę. – Užtikrinti, kad 5G rinkos ir tiekimo grandinės veiktų pagal ES prekybos ir konkurencijos taisykles ir tikslus, nustatytus sausio 29 d. Komisijos komunikate, ir kad TUI tikrinimas būtų taikomas įvykus investavimo pokyčiams, galintiems daryti poveikį 5G vertės grandinei, atsižvelgiant į priemonių rinkinio tikslus. – Stebėti esamas ir numatomas rinkos tendencijas ir įvertinti riziką bei galimybes atvirojo radijo prieigos tinklo (RAN) srityje, visų pirma atliekant nepriklausomą tyrimą.	Valstybių narių institucijos, Komisija
Sertifikavimas	Pradėti rengti atitinkamą (-as) kandidatų sertifikavimo schemą (-as), skirtą (-as) pagrindiniams 5G komponentams ir tiekėjų procesams, siekiant padėti šalinti tam tikrą riziką, susijusią su techninėmis spragomis, kaip apibrėžta priemonių rinkinio rizikos mažinimo planuose.	Komisija, ENISA, nacionalinės institucijos, kitos suinteresuotosios šalys
ES pajėgumai ir saugus tinklų plėtojimas	– Investuoti į mokslinius tyrimus ir pajėgumus, visų pirma patvirtinant pažangių tinklų ir paslaugų partnerystę. – Įgyvendinti atitinkamas ES finansavimo programų ir finansinių priemonių (vidaus ir išorės) saugumo sąlygas, kaip paskelbta sausio 29 d. Komisijos komunikate.	Valstybių narių institucijos, Komisija, 5G pramonės suinteresuotosios šalys
Išorės aspektai	Tenkinti trečiųjų valstybių, kurios norėtų suprasti ir galbūt taikyti ES sukurtą priemonių rinkinio metodą, prašymus.	Valstybių narių institucijos, Komisija, EIVT, ES delegacijos.