EUROPOS
KOMISIJA

Strasbūras, 2022 10 18
COM(2022) 551 final

2022/0338 (NLE)

Pasiūlymas

TARYBOS REKOMENDACIJA

dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros objektų atsparumo didinimą

(Tekstas svarbus EEE)

AIŠKINAMASIS MEMORANDUMAS

1. PASIŪLYMO APLINKYBĖS

• Pasiūlymo pagrindimas ir tikslai

Saugumas yra esminis Europos Sąjungos tikslas. Nors didžiausia atsakomybė už piliečių apsaugą tenka valstybėms narėms, Sąjungos lygmeniu visos ES saugumui didelės svarbos turi bendri veiksmai. Koordinuoti veiksmai didina atsparumą, gerina budrumą ir stiprina mūsų bendrą reagavimą. Stiprinant ES saugumo sąjungą imtasi svarbių veiksmų siekiant gerinti daugelio grėsmių saugumui prevencijos, nustatymo ir greito reagavimo į jas gebėjimus ir pajėgumus ir bendromis pastangomis vienyti viešojo ir privačiojo sektorių dalyvius.

Siekiant suteikti ES priemonių, kurios padėtų reaguoti į nuolat besikeičiančią grėsmių padėtį, reikia nuolat išlikti budriems ir sugebėti prisitaikyti. Rusijos agresijos karas prieš Ukrainą sukėlė naujų pavojų, kurie dažnai tapdavo hibridine grėsme. Vienas iš jų – rizika, kad gali būti sutrikdytas ypatingos svarbos infrastruktūros objektus Europoje eksploatuojančių subjektų esminių paslaugų teikimas. Tai tapo dar akivaizdžiau po neabejotino „Nord Stream“ dujotiekių sabotažo ir kitų pastarojo laikotarpio incidentų. Tiek fizinės, tiek skaitmeninės infrastruktūros svarba visuomenei yra didelė, o esminių paslaugų teikimo nutraukimas, nesvarbu, ar tai būtų įprastiniai fiziniai išpuoliai, ar kibernetiniai išpuoliai, ar ir viena, ir kita, gali turėti sunkių pasekmių piliečių gerovei, mūsų ekonomikai ir pasitikėjimui mūsų demokratinėmis sistemomis.

Sklandaus vidaus rinkos veikimo užtikrinimas – tai dar vienas svarbus ES tikslas, be kita ko, susijęs su ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų teikiamomis esminėmis paslaugomis. Todėl ES jau ėmėsi įvairių priemonių, kad sumažintų ypatingos svarbos subjektų pažeidžiamumą ir padidintų jų atsparumą kibernetinės ir nekibernetinės rizikos atžvilgiu.

Reikia skubiai imtis veiksmų siekiant padidinti ES pajėgumą pasipriešinti galimiems išpuoliams prieš ypatingos svarbos infrastruktūros objektus, visų pirma pačioje ES, o prireikus ir kaimyninėse valstybėse.

Siūloma Tarybos rekomendacija siekiama sustiprinti ES paramą ypatingos svarbos infrastruktūros objektų atsparumo didinimui ir užtikrinti parengties ir reagavimo veiksmų koordinavimą ES lygmeniu. Ja siekiama kuo labiau padidinti ir paspartinti pastangas, kuriomis siekiama apsaugoti ekonomikos veikimui užtikrinti būtiną turtą, infrastruktūrą ir sistemas, suteikti vidaus rinkoje piliečiams reikalingas esmines paslaugas, taip pat sušvelninti bet kokio išpuolio poveikį užtikrinant kuo spartesnį atsigavimą. Nors reikėtų apsaugoti visą tokią infrastruktūrą, šiuo metu energetikos, skaitmeninės infrastruktūros, transporto ir kosmoso sektoriai yra svarbiausias prioritetas dėl savo ypatingo horizontalumo ir svarbos visuomenei bei ekonomikai, taip pat dėl dabartinio rizikos vertinimo.

ES turi imtis ypatingo vaidmens, kai kalbama apie infrastruktūros, išsidėsčiusios abipus sausumos ar jūrų sienos ir turinčios poveikio kelių valstybių narių interesams, arba naudojamos esminėms tarpvalstybinėms paslaugoms teikti, atsparumo užtikrinimą. Kelioms valstybėms narėms svarbūs ypatingos svarbos infrastruktūros objektai vis dėl to gali būti vienoje valstybėje narėje arba net už valstybės narės teritorijos ribų, pavyzdžiui, jei tai jūriniai kabeliai ar vamzdynai. Aiškus ypatingos svarbos infrastruktūros objektų ir juos eksploatuojančių subjektų, taip pat jiems kylančios rizikos identifikavimas ir bendras įsipareigojimas juos apsaugoti atitinka visų valstybių narių ir visos ES interesus.

Europos Parlamentas ir Taryba jau pasiekė politinį susitarimą stiprinti ES teisės aktų sistemą, kuri padidintų ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų

atsparumą. 2022 m. vasarą buvo susitarta dėl Direktyvos dėl ypatingos svarbos subjektų atsparumo (CER direktyva)[1] ir peržiūrėtos Kibernetinio saugumo direktyvos (TIS 2 direktyva)[2]. Palyginti su esama teisės aktų sistema, t. y. 2008 m. gruodžio 8 d. Direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo (EPI direktyva)[3] ir Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva)[4], šie pajėgumai gerokai sustiprės. Tikimasi, kad nauji teisės aktai įsigalios 2022 m. pabaigoje arba 2023 m. pradžioje, o valstybės narės turėtų imtis perkėlimo į nacionalinę teisę ir taikymo priemonių pagal Sąjungos teisę prioriteto tvarka.

Šiomis aplinkybėmis, atsižvelgiant į potencialiai skubią būtinybę pašalinti grėsmes, kurias kelia Rusijos agresijos karas prieš Ukrainą, naujaisiais teisės aktais numatytos priemonės, kai įmanoma ir tinkama, turėtų būti pradėtos taikyti jau šiandien. Jeigu tarpusavio bendradarbiavimas būtų sustiprintas jau dabar, tai taip pat suteiktų postūmį veiksmingam įgyvendinimui, kai naujieji teisės aktai visiškai įsigalios.

Tokiu būdu būtų išplėstas tiek dabartinės sistemos veiksmų mastas, tiek reglamentuojamų sektorių aprėptis. Naująja CER direktyva nustatyta nauja valstybių narių ir ypatingos svarbos subjektų bendradarbiavimo sistema ir įpareigojimai, kuriais siekiama stiprinti tų vidaus rinkoje esmines paslaugas teikiančių subjektų fizinį nekibernetinį atsparumą natūralioms ir žmogaus sukeltoms grėsmėms vienuolikoje sektorių[5]. TIS 2 direktyva bus nustatyta plati sektorinė kibernetinio saugumo srities įpareigojimų aprėptis. Joje taip pat bus nustatytas naujas reikalavimas valstybėms narėms į savo kibernetinio saugumo strategijas, jei taikytina, įtraukti nuostatas dėl jūrinių kabelių.

Teisės aktais reikalaujama, kad Komisija imtųsi svarbaus koordinatorės vaidmens. Pagal CER direktyvą Komisija atlieka paramos ir palankesnių sąlygų sudarymo užduotis, kurias ji atliks remiama ta direktyva įsteigtos Ypatingos svarbos subjektų atsparumo klausimų grupės (CERG) ir jai dalyvaujant, ir turėtų papildyti valstybių narių veiklą parengdama geriausią praktiką, gaires ir metodikas. Kalbant apie kibernetinį saugumą, Taryba jau savo 2022 m. vasarą priimtose išvadose dėl ES kibernetinio saugumo būklės ragino Komisiją, vyriausiąjį įgaliotinį ir TIS bendradarbiavimo grupę rengti kibernetinio saugumo rizikos vertinimus ir scenarijus. Toks koordinavimas gali paskatinti parengti kitiems ypatingos svarbos infrastruktūros objektams taikytiną požiūrį.

2022 m. spalio 5 d. Pirmininkė U. von der Leyen pristatė 5 punktų planą, kuriame išdėstytas suderintas požiūris į darbą, kurį reikės atlikti. Pagrindiniai plano tikslai: stiprinti parengtį, bendradarbiauti su valstybėmis narėmis siekiant atlikti jų ypatingos svarbos infrastruktūros testavimą nepalankiausiomis sąlygomis – iš pradžių energetikos sektoriaus, vėliau – kitų didelės rizikos sektorių, didinti reagavimo pajėgumus, visų pirma pasitelkiant Sąjungos civilinės saugos mechanizmą, gerai išnaudoti palydovų pajėgumą galimoms grėsmėms nustatyti ir stiprinti bendradarbiavimą su NATO ir pagrindiniais partneriais ypatingos svarbos infrastruktūros atsparumo srityje. 5 punktų plane pabrėžta, kaip svarbu pasirengti taikyti teisės aktus, dėl kurių jau pasiektas politinis susitarimas.

---

1 COM(2020) 829 *final*
2 COM(2020) 823 *final*
3 OL L 345, 2008 12 23
4 OL L 194, 2016 7 19
5 Energetika, transportas, skaitmeninė infrastruktūra, bankininkystė, finansų rinkos infrastruktūra, sveikata, geriamasis vanduo, nuotekos, viešasis administravimas, kosmosas ir maistas.

Toks požiūris palankiai vertinamas šioje siūlomoje Tarybos rekomendacijoje siekiant struktūrizuoti paramą valstybėms narėms ir koordinuoti jų pastangas didinti informuotumą apie riziką ir stiprinti parengtį bei reagavimą į dabartines grėsmes. Atsižvelgiant į tai, rengiantis CER direktyvos įsigaliojimui ir CERG įsteigimui šia direktyva, rengiami ekspertų susitikimai siekiant aptarti ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumą.

Bus labai svarbu sustiprinti bendradarbiavimą su pagrindiniais partneriais ir kaimyninėmis bei kitomis susijusiomis trečiosiomis šalimis ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumo klausimais, visų pirma plėtojant ES ir NATO struktūrinį dialogą atsparumo klausimais.

Šioje rekomendacijoje daugiausia dėmesio skiriama tam, kad būtų sustiprinti Sąjungos pajėgumai numatyti naujas grėsmes, kylančias dėl Rusijos agresijos karo prieš Ukrainą, užkirsti joms kelią ir į jas reaguoti. Todėl siūlomose rekomendacijose daugiausia dėmesio skiriama su saugumu susijusios rizikos ir grėsmių ypatingos svarbos infrastruktūros objektams šalinimui. Vis dėlto reikėtų pažymėti, kad pastarieji įvykiai taip pat parodė, kad reikia nedelsiant skirti daugiau dėmesio klimato kaitos poveikiui ypatingos svarbos infrastruktūrai ir paslaugoms, kaip antai sezoninėms ir nenuspėjamoms atominėms elektrinėms vėsinti, hidroenergijai ir vidaus vandenų laivybai reikalingo vandens tiekimo triktims arba materialinės žalos transporto infrastruktūrai rizikos, nes tai gali gerokai sutrikdyti esminių paslaugų teikimą. Šie susirūpinimą keliantys klausimai ir toliau bus sprendžiami priimant atitinkamus teisės aktus ir koordinuojant veiksmus.

- **Suderinamumas su toje pačioje politikos srityje galiojančiomis nuostatomis**

Šis Tarybos rekomendacijos pasiūlymas visiškai atitinka dabartinę ir būsimą ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumo srityje nustatytą teisės sistemą, atitinkamai EPI direktyvą ir CER direktyvą, nes ja, *inter alia,* siekiama palengvinti valstybių narių bendradarbiavimą šioje srityje ir remti konkrečias priemones, kuriomis siekiama didinti ypatingos svarbos infrastruktūros objektus ES eksploatuojančių subjektų atsparumą dabartinėms neišvengiamoms grėsmėms.

Be to, juo CER direktyva papildoma ir pasirengiama jos taikymui, raginant valstybes nares prioriteto tvarka laiku užtikrinti direktyvos perkėlimą į nacionalinę teisę, pasitelkiant bendradarbiavimo tikslais ekspertus, kurių susitikimai būtų rengiami pagal Komisijos skelbiamą 5 punktų planą, ir siekiant koordinuoti bendro požiūrio į ypatingos svarbos infrastruktūros objektų testavimą nepalankiausiomis sąlygomis ES įgyvendinimą.

Pasiūlymas taip pat atitinka TIS direktyvą ir būsimą TIS 2 direktyvą, kuria TIS direktyva bus panaikinta, raginant kuo greičiau pradėti įgyvendinimo ir perkėlimo į nacionalinę teisę veiksmus. Jis taip pat atspindi 2022 m. kovo mėn. Nevere paskelbtą bendrą raginimą ir 2022 m. gegužės mėn. Tarybos išvadas dėl ES kibernetinio saugumo būklės, atsižvelgiant į valstybių narių prašymą Komisijai parengti rizikos vertinimą ir scenarijus.

Pasiūlymas taip pat atitinka ES civilinės saugos politiką, kurios laikantis didelio masto ypatingos svarbos infrastruktūros objektų (subjektų) veiklos sutrikimo atveju valstybės narės ir trečiosios šalys pagal Sąjungos civilinės saugos mechanizmą (SCSM) gali kreiptis pagalbos į Reagavimo į nelaimes koordinavimo centrą (RNKC). SCSM aktyvavimo atveju RNKC gali koordinuoti ir bendrai finansuoti valstybių narių (iš dalies Europos civilinės saugos rezerve) ir rezerve „rescEU“ turimos būtinosios įrangos, medžiagų ir ekspertinių žinių dislokavimą nukentėjusioje šalyje. Paprašius gali būti teikiama įvairi pagalba, įskaitant, pavyzdžiui, degalus, generatorius, elektros infrastruktūrą, pastogės suteikimą, vandens valymo pajėgumus ir greitosios medicinos pagalbos pajėgumus.

Pasiūlymas taip pat atitinka energijos tiekimo saugumo srities ES *acquis*.

Į siūlomą Tarybos rekomendaciją konkrečiai neįtrauktas branduolinės energetikos sektorius, išskyrus, pavyzdžiui, susijusią infrastruktūrą, tokią kaip atominių elektrinių perdavimo linijos, kuri gali turėti įtakos tiekimo saugumui. Pagal Euratomo sutartį ir (arba) nacionalinės teisės aktus konkretiems branduoliniams elementams taikomi atitinkami branduolinės energetikos teisės aktai[6]. Įvertinus per Fukušimos avariją įgytą patirtį, buvo sugriežtinti Europos branduolinės saugos teisės aktai, taigi nacionalinės valdžios institucijos turi reguliariai atlikti kiekvieno įrenginio saugumo patikras, kad būtų nuolat užtikrinama atitiktis aukščiausiems saugos reikalavimams ir būtų nustatyti tolesni saugos patobulinimai, taip pat kas šešerius metus atliekami ES lygmens teminiai ekspertiniai vertinimai.

ES jūrų saugumo strategijoje[7] ir jos veiksmų plane[8] pabrėžiamas kintantis grėsmių jūrų srityje pobūdis ir raginama atnaujinti įsipareigojimą apsaugoti ypatingos svarbos jūrų infrastruktūrą, įskaitant povandeninę infrastruktūrą, visų pirma jūrų transporto, energetikos ir ryšių infrastruktūrą, *inter alia*, pasitelkus sąveikumo gerinimo ir keitimosi informacija supaprastinimo priemones, didinant informuotumą apie padėtį jūroje.

Pasiūlymas taip pat atitinka kitus susijusius sektorių teisės aktus. Todėl šios rekomendacijos įgyvendinimas turėtų atitikti konkrečias priemones, reguliuojančias arba galinčias ateityje reguliuoti tam tikrus susijusiuose sektoriuose, kaip antai transporto, veikiančių subjektų atsparumo klausimus. Į ją įtrauktos kitos susijusios iniciatyvos, kaip antai transporto sektoriui skirtas nenumatytų atvejų planas[9] arba nenumatytų atvejų planas siekiant užtikrinti maisto tiekimą ir aprūpinimą maistu per krizes[10] ir susijęs Europos pasirengimo apsirūpinimo maistu krizėms ir reagavimo į jas mechanizmas. Apskritai rekomendacija akivaizdžiai turėtų būti įgyvendinama visapusiškai laikantis visų taikytinų ES teisės taisyklių, įskaitant EPI ir TIS direktyvose nustatytas taisykles.

Pasiūlymas taip pat atitinka Saugumo ir gynybos strateginį kelrodį, kuriame pabrėžta būtinybė iš esmės didinti atsparumą ir gebėjimą kovoti su hibridinėmis grėsmėmis ir kibernetiniais išpuoliais, taip pat būtinybė didinti šalių partnerių atsparumą ir bendradarbiauti su NATO. Jis taip pat atitinka pagrindą koordinuotam ES atsakui į hibridines grėsmes ir kampanijas, darančias poveikį ES, valstybėms narėms ir partneriams[11].

2. TEISINIS PAGRINDAS, SUBSIDIARUMO IR PROPORCINGUMO PRINCIPAI

• Teisinis pagrindas

Pasiūlymas grindžiamas Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsniu, kuriuo numatoma derinti teisės aktus siekiant geresnio vidaus rinkos veikimo, kartu su SESV 292 straipsniu. Tai pateisinama tuo, kad siūloma Tarybos rekomendacija iš esmės siekiama pasirengti priemonėms, nustatytoms naujomis CER ir TIS 2 direktyvomis, kurios abi taip pat grindžiamos SESV 114 straipsniu. Laikantis logikos, kuria grindžiamas rėmimasis tuo straipsniu kaip minėtų direktyvų teisiniu pagrindu, ES reikia imtis veiksmų, kad būtų užtikrintas sklandus vidaus rinkos veikimas, visų pirma atsižvelgiant į atitinkamų paslaugų

6 Tarybos direktyvos 2008/114/EB (EPI direktyva) 9 konstatuojamoji dalis.
7 11205/14
8 10494/18
9 COM(2022) 211
10 COM(2021) 689
11 Europos Sąjungos Taryba, 10016/22, 2022 m. birželio 21 d.

tarpvalstybinį pobūdį bei apimtį ir galimas pasekmes sutrikimų atveju, taip pat į esamas ir naujas nacionalines priemones, kuriomis siekiama didinti ypatingos svarbos infrastruktūros objektų, naudojamų esminėms paslaugoms vidaus rinkoje teikti, atsparumą.

- **Subsidiarumo principas (neišimtinės kompetencijos atveju)**

Atsižvelgiant į ypatingos svarbos infrastruktūros veiklos ir teikiamų esminių paslaugų tarpusavio priklausomybę ir tarpvalstybinį pobūdį ir į tai, kad reikia bendresnio ir labiau koordinuoto Europos požiūrio, siekiant užtikrinti, kad susiję subjektai būtų pakankamai atsparūs dabartinėmis geopolitinėmis aplinkybėmis, pagrįsta imtis tolesnių veiksmų Europos lygmeniu, susijusių su ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumu. Kadangi daugelis bendrų problemų, pvz., akivaizdus „Nord Stream“ dujotiekių sabotažas, visų pirma sprendžiamos taikant nacionalines priemones arba jas sprendžia ypatingos svarbos infrastruktūros objektus eksploatuojantys subjektai, siekiant didinti atsparumą, gerinti budrumą ir stiprinti bendrą ES reagavimą, būtina užtikrinti ES, įskaitant, kai tinkama, atitinkamų agentūrų, paramą.

- **Proporcingumo principas**

Šis pasiūlymas atitinka Europos Sąjungos sutarties 5 straipsnio 4 dalyje nustatytą proporcingumo principą.

Nei šios siūlomos Tarybos rekomendacijos turinys, nei forma neviršija to, kas būtina jos tikslams pasiekti. Siūlomi veiksmai yra proporcingi siekiamiems tikslams, nes jais atsižvelgiama į valstybių narių teises ir pareigas pagal nacionalinę teisę.

Galiausiai pasiūlyme atsižvelgiama į potencialiai diferencijuotą požiūrį, atspindintį skirtingas valstybių narių vidaus aplinkybes, kai kalbama apie ypatingos svarbos infrastruktūros objektų parengtį ir reagavimą į fizines grėsmes.

- **Priemonės pasirinkimas**

SESV, visų pirma 292 straipsnyje, numatyta, kad, siekiant pirmiau nurodytų tikslų, Taryba, remdamasi Komisijos pasiūlymu, priima rekomendacijas. Šiuo atveju, o taip pat atsižvelgiant į pirmiau paaiškintas dabartines teisines aplinkybes, Tarybos rekomendacija yra tinkama priemonė. Tarybos rekomendacija, nors tai ir nėra privalomo pobūdžio teisės aktas, rodo valstybių narių įsipareigojimą imtis į ją įtrauktų priemonių ir suteikia tvirtą politinį pagrindą bendradarbiauti šiose srityse, kartu visapusiškai gerbiant valstybių narių įgaliojimus.

3. *EX POST* VERTINIMO, KONSULTACIJŲ SU SUINTERESUOTOSIOMIS ŠALIMIS IR POVEIKIO VERTINIMO REZULTATAI

- **Konsultacijos su suinteresuotosiomis šalimis**

Rengiant šį pasiūlymą buvo atsižvelgta į 2022 m. spalio 12 d. posėdyje valstybių narių ekspertų pareikštas nuomones. Pasirengiant tam tikroms CER direktyvos nuostatoms, kol ji dar oficialiai nepriimta, iš esmės buvo sutarta dėl to, kad geresnis su parengtimi ir reagavimu į dabartines grėsmes susijęs koordinavimas Sąjungos lygmeniu duotų naudos. Valstybės narės pareiškė esančios pasirengusios dalytis patirtimi ir geriausia praktika, susijusia su ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumo didinimo priemonėmis ir metodikomis. Be to, valstybės narės pareiškė esančios pasirengusios laikytis suderinto požiūrio į ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų testavimą nepalankiausiomis sąlygomis pagal savanoriškumo principą, laikantis bendrųjų principų. Valstybės narės nurodė, kad, taikant šią rekomendaciją, ypatingos svarbos infrastruktūros objektus eksploatuojantys energetikos, skaitmeninės infrastruktūros ir transporto sektorių

subjektai, visų pirma tie, kuriuos svarbiais laiko keletas valstybių narių, turėtų būti laikomi prioritetiniais. Valstybės narės taip pat palankiai įvertino Komisijos ketinimą artimiausiomis savaitėmis surengti papildomus valstybių narių ekspertų susitikimus.

- **Išsamus konkrečių pasiūlymo nuostatų paaiškinimas**

Tarybos rekomendacijos pasiūlymo:

– I skyriuje nustatomas pasiūlymo tikslas, taikymo sritis ir rekomenduojamų priemonių prioritetai;

– II skyriuje daugiausia dėmesio skiriama priemonėms, kurių reikėtų imtis siekiant sustiprinti parengtį tiek Sąjungos, tiek valstybių narių lygmenimis;

– III skyriuje aptariamas sustiprintas reagavimas tiek ES, tiek valstybių narių lygmenimis.

– IV skyriuje aptariamas tarptautinis bendradarbiavimas ir veiksmai, kurių reikėtų imtis siekiant didinti ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumą.

2022/0338 (NLE)

Pasiūlymas

TARYBOS REKOMENDACIJA

dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros objektų atsparumo didinimą

(Tekstas svarbus EEE)

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 114 ir 292 straipsnius,

atsižvelgdama į Europos Komisijos pasiūlymą,

kadangi:

(1) Sąjunga turi imtis ypatingo vaidmens, kai kalbama apie infrastruktūrą, išsidėsčiusią abipus sienos ir turinčią poveikio kelių valstybių narių interesams, arba kitaip naudojamą esminėms tarpvalstybinėms paslaugoms teikti. Taip kelioms valstybėms narėms teikiamos svarbios paslaugos ir su jomis susiję ypatingos svarbos infrastruktūros objektai vis dėl to gali būti vienoje valstybėje narėje arba net už valstybių narių teritorijų ribų, pavyzdžiui, jei tai jūriniai kabeliai ar vamzdynai. Aiškus tokių infrastruktūros objektų ir subjektų, taip pat jiems kylančių grėsmių identifikavimas ir bendras įsipareigojimas juos apsaugoti atitinka visų valstybių narių ir visos Sąjungos interesus;

(2) dviems sektoriams priklausančių ypatingos svarbos infrastruktūros objektų apsauga šiuo metu reglamentuojama Tarybos direktyvoje 2008/114/EB[12]. Siekiant prisidėti prie žmonių apsaugos, ta direktyva nustatoma Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems tvarka bei bendras požiūris į būtinybės gerinti tokių infrastruktūros objektų apsaugą vertinimą. Ji reglamentuoja energetikos ir transporto sektorius. Siekdamas padidinti ypatingos svarbos subjektų, jų teikiamų esminių paslaugų ir ypatingos svarbos infrastruktūros, kuria jie naudojasi, atsparumą, Sąjungos teisės aktų leidėjas šiuo metu rengiasi priimti naują direktyvą dėl ypatingos svarbos subjektų atsparumo[13] (CER direktyva), kuri pakeis Direktyvą 2008/114/EB ir apims daugiau sektorių, įskaitant skaitmeninę infrastruktūrą;

(3) be to, Europos Parlamento ir Tarybos direktyvoje (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti[14] dėmesys sutelktas į kibernetines grėsmes. Ta direktyva bus pakeista nauja Direktyva dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje

---

12 2008 m. gruodžio 8 d. Tarybos direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo (OL L 345, 2008 12 23, p. 75).

13 COM(2020) 829

14 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

Sąjungoje užtikrinti[15] (TIS 2 direktyva), kurią Sąjungos teisės aktų leidėjas šiuo metu taip pat rengiasi priimti;

(4) sparčiai kintant grėsmių padėčiai, visų pirma atsižvelgiant į akivaizdų „Nord Stream 1“ ir „Nord Stream 2“ dujų vamzdynų sabotažą, ypatingos svarbos infrastruktūros objektus eksploatuojantiems subjektams tenka susidurti su išskirtiniais iššūkiais, susijusiais su jų atsparumu priešiškiems veiksmams ir kitoms žmogaus sukeltoms grėsmėms, o didėjantys gamtos veiksnių ir klimato kaitos keliami iššūkiai gali papildyti priešiškus veiksmus. Todėl jie, remiami valstybių narių, turi imtis tinkamų atsparumo didinimo priemonių. Tų priemonių turėtų būti imtasi ir ta parama turėtų būti suteikta platesne apimtimi, nei nustatyta Direktyva 2008/114/EB ir Direktyva (ES) 2016/1148 ir netgi anksčiau nei bus priimtos, įsigalios ir į nacionalinę teisę bus perkeltos naujos CER ir TIS 2 direktyvos;

(5) kol tos naujos direktyvos bus priimtos, įsigalios ir bus perkeltos į nacionalinę teisę, Sąjunga ir valstybės narės, laikydamosi Sąjungos teisės, raginamos panaudoti visas turimas priemones pažangai pasiekti ir minėtų subjektų ir jų eksploatuojamų ypatingos svarbos infrastruktūros objektų, kuriuos naudodami vidaus rinkoje jie teikia esmines paslaugas (t. y. gyvybiškai svarbių visuomenės funkcijų, ekonominės veiklos, visuomenės sveikatos ir saugos arba aplinkos išsaugojimui itin reikalingas paslaugas), fiziniam ir kibernetiniam atsparumui sustiprinti. Šiuo atveju atsparumo sąvoka turėtų būti aiškinama kaip subjekto gebėjimas užkirsti kelią įvykiams, galintiems labai sutrikdyti atitinkamų esminių paslaugų teikimą arba jį trikdantiems, nuo jų apsisaugoti, reaguoti į juos, atsilaikyti prieš juos, juos švelninti, absorbuoti, prisitaikyti prie jų ir po jų atsigauti;

(6) siekiant užtikrinti, kad požiūris būtų tiek veiksmingas, tiek kuo labiau atitiktų naująją CER direktyvą, šioje rekomendacijoje pateiktos priemonės turėtų būti susijusios su infrastruktūra, kurios ypatingą svarbą pripažino valstybė narė, įskaitant tiek nacionalinę ypatingos svarbos infrastruktūrą, tiek europinę ypatingos svarbos infrastruktūrą, neatsižvelgiant į tai, ar pagal tą naują direktyvą ypatingos svarbos infrastruktūros objektą eksploatuojantis subjektas jau buvo pripažintas ypatingos svarbos subjektu. Šioje rekomendacijoje ypatingos svarbos infrastruktūros sąvoka turėtų būti aiškinama atitinkamai;

(7) atsižvelgiant į esamas grėsmes, pagrindiniuose energetikos, skaitmeninės infrastruktūros, transporto ir kosmoso sektoriuose atsparumo didinimo priemonių reikėtų imtis prioriteto tvarka ir tų priemonių svarbiausias tikslas turėtų būti ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumo žmogaus sukeltai rizikai didinimas. Kalbant apie nacionalinę ypatingos svarbos infrastruktūrą, jei kiltų reali rizika, atsižvelgiant į galimas pasekmes, prioritetas turėtų būti teikiamas tarpvalstybinės reikšmės infrastruktūrai;

(8) todėl šioje rekomendacijoje nustatytomis priemonėmis iš esmės siekiama papildyti naująsias CER ir TIS 2 direktyvas, grindžiamas Sutarties dėl Europos Sąjungos veikimo (SESV) 114 straipsniu, pasirengiant taikyti ir papildant priemones, kurios bus numatytos tose naujose direktyvose. Todėl, atsižvelgiant į atitinkamų esminių paslaugų ir ypatingos svarbos infrastruktūros objektų tarpvalstybinį pobūdį ir reikšmę, taip pat į esamus ir atsirandančius nacionalinės teisės aktų skirtumus, išsikreipiančius vidaus rinką, šią rekomendaciją taip pat tikslinga grįsti SESV 114 straipsniu kartu su SESV 292 straipsniu;

[15] COM(2020) 823

(9) šios rekomendacijos įgyvendinimas neturėtų būti suprantamas kaip darantis poveikį dabartiniams ir būsimiems Sąjungos teisės reikalavimams dėl tam tikrų atitinkamų subjektų atsparumo aspektų ir turėtų su jais derėti. Tokie reikalavimai nustatyti bendrosiose priemonėse, kaip antai Direktyvoje 2008/114/EB ir Direktyvoje (ES) 2016/1148 ir jas pakeičiančiose naujose CER ir TIS 2 direktyvose, taip pat tam tikrose konkretiems sektoriams skirtose priemonėse, pavyzdžiui, transporto sektoriuje, kuriame Komisija ėmėsi iniciatyvos dėl transporto sektoriui skirto nenumatytų atvejų plano[16]. Vadovaujantis lojalaus bendradarbiavimo principu, ši rekomendacija turėtų būti įgyvendinama laikantis abipusės pagarbos ir pagalbos principų;

(10) 2022 m. spalio 5 d. Komisija paskelbė penkių punktų planą, kuriame išdėstytas suderintas požiūris į tai, kaip spręsti būsimus iššūkius, ir į kurį įtraukti su parengtimi susiję darbai, atsižvelgiant į naujos CER direktyvos priėmimą ir įsigaliojimą ir tam rengiantis, bei nuostatos dėl bendradarbiavimo su valstybėmis narėmis siekiant atlikti ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų, pradedant energetikos sektoriumi, testavimą nepalankiausiomis sąlygomis, laikantis bendrųjų principų. Šia, minėtą planą įgyvendinti padėsiančia, rekomendacija siūlomam požiūriui pritariama ir nurodoma, kaip jis galėtų būti įgyvendintas;

(11) atsižvelgiant į sparčiai kintančią grėsmių padėtį ir dabartinę rizikos aplinką, kuriai būdinga žmogaus keliama rizika, visų pirma kiek tai susiję su tarpvalstybinės reikšmės turinčiais ypatingos svarbos infrastruktūros objektais, itin svarbu susidaryti tikslų, aktualų ir išsamų vaizdą apie svarbiausią riziką, kylančią ypatingos svarbos infrastruktūros objektus eksploatuojantiems subjektams. Todėl valstybės narės turėtų imtis tos rizikos vertinimui atlikti arba atnaujinti reikalingų priemonių. Nors šioje rekomendacijoje daugiausia dėmesio skiriama su saugumu susijusiai rizikai, turėtų ir toliau būti dedamos pastangos spręsti klimato kaitos ir aplinkos rizikos iššūkius, visų pirma tais atvejais, kai dėl gamtos reiškinių žmogaus keliama rizika gali dar labiau padidėti;

(12) atsižvelgiant į tą grėsmių padėtį, valstybės narės turėtų būti raginamos kuo greičiau imtis tinkamų ypatingos svarbos infrastruktūros objektų atsparumo didinimo priemonių, ne tik minėto rizikos vertinimo, kurių vėliau bus reikalaujama pagal naująją CER direktyvą;

(13) įgyvendinant Komisijos paskelbtą penkių punktų planą, būtina imtis koordinavimo veiklos suburiant nacionalinius ekspertus ir taip pasirengiant Ypatingos svarbos subjektų atsparumo klausimų grupės įsteigimui pagal naująją CER direktyvą, kad būtų sudarytos sąlygos valstybėms narėms bendradarbiauti ir keistis informacija apie ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumą. Kartu reikėtų įtraukti bendradarbiavimą ir keitimąsi informacija apie tokią veiklą, kaip ypatingos svarbos subjektų ir infrastruktūros objektų identifikavimas, bendrų testavimo nepalankiausiomis sąlygomis principų parengimas, plėtojimas bei taikymo skatinimas ir mokymasis iš bendros testavimo nepalankiausiomis sąlygomis patirties siekiant nustatyti pažeidžiamumą ir galimus gebėjimus. Šie procesai turėtų taip pat būti naudingi ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumui su klimatu ir aplinka susijusiai rizikai. Be to, vykdant šį darbą bus galima nustatyti bendrus testavimo nepalankiausiomis sąlygomis veiklos prioritetus, daugiausia dėmesio skiriant energetikos, skaitmeninės infrastruktūros, transporto ir kosmoso sektoriams. Komisija jau pradėjo kviesti minėtus ekspertus į susitikimus,

[16] COM(2022)211

ėmėsi pastangų palengvinti jų darbą ir ketina toliau tai tęsti. Įsigaliojus naujai CER direktyvai ir įsteigus Ypatingos svarbos subjektų atsparumo klausimų grupę, ši grupė turėtų tęsti minėtą parengiamąją veiklą, vykdydama pagal CER direktyvą nustatytas užduotis;

(14) testavimas nepalankiausiomis sąlygomis turėtų būti papildytas ypatingos svarbos infrastruktūros incidentų ir krizių valdymo planu, kuriame aprašomi ir nustatomi valstybių narių ir ES institucijų, įstaigų, tarnybų ir agentūrų bendradarbiavimo reaguojant į incidentus, susijusius su ypatingos svarbos infrastruktūros objektais, tikslai ir būdai, visų pirma tais atvejais, kai dėl incidentų kyla didelių esminių paslaugų teikimo vidaus rinkai sutrikimų. Šis planas turėtų būti grindžiamas dabartiniu reagavimui koordinuoti skirtu integruotu politinio atsako į krizes (IPCR) mechanizmu, turėtų tarpusavyje derėti su didelio masto kibernetinių incidentų valdymo planu ir vienas kitą papildyti ir turėtų numatyti, kad bus susitarta dėl pagrindinių viešosios komunikacijos pranešimų, atsižvelgiant į komunikacijos krizės metu svarbą siekiant sumažinti neigiamą ypatingos svarbos infrastruktūros incidentų ir krizių poveikį;

(15) siekdama užtikrinti koordinuotą ir veiksmingą reagavimą į dabartines ir numatomas grėsmes, Komisija teiks valstybėms narėms papildomą paramą siekdama didinti atsparumą tų grėsmių akivaizdoje, visų pirma teikdama atitinkamą informaciją informacinių pranešimų, vadovų ir gairių forma, skatindama naudotis Sąjungos finansuojamų mokslinių tyrimų ir inovacijų projektų rezultatais, imdamasi būtinų parengiamųjų veiksmų ir optimizuodama Sąjungos stebėjimo išteklių naudojimą. Grėsmių vertinimą turėtų atlikti EIVT, visų pirma padedama ES žvalgybos ir situacijų centro;

(16) tam tikriems sektoriams priklausančios Sąjungos agentūros ir kitos susijusios įstaigos taip pat turėtų teikti paramą su atsparumu susijusiais klausimais pagal savo atitinkamus įgaliojimus, kaip nustatyta atitinkamose Sąjungos teisės priemonėse. Visų pirma Europos kibernetinio saugumo agentūra (ENISA) galėtų padėti kibernetinio saugumo srityje, Europos jūrų saugumo agentūra (EMSA) valstybėms narėms galėtų padėti jūrų saugumo ir saugos srityje teikdama jūrų stebėjimo paslaugas, Europos Sąjungos teisėsaugos bendradarbiavimo agentūra (Europolas) galėtų padėti, kai renkama informacija ir vykdomi tyrimai, susiję su tarpvalstybiniais teisėsaugos veiksmais, o Europos Sąjungos kosmoso programos agentūra (EUSPA) ir ES palydovų centras (SATCEN) gali padėti vykdydami operacijas pagal Sąjungos kosmoso programą;

(17) nors pagrindinė atsakomybė už ypatingos svarbos infrastruktūros objektų ir atitinkamų subjektų saugumo užtikrinimą tenka valstybėms narėms, reikalingas geresnis koordinavimas Sąjungos lygmeniu, ypač atsižvelgiant į grėsmes, kurios vienu metu gali daryti poveikį kelioms valstybėms narėms, kaip antai Rusijos agresijos karas prieš Ukrainą, arba daryti poveikį Sąjungos ekonomikos, bendrosios rinkos ir visuomenės atsparumui ir tinkamam funkcionavimui;

(18) ši rekomendacija neapima informacijos, kurios atskleidimas prieštarauja esminiams valstybių narių nacionalinio saugumo, visuomenės saugumo ar gynybos interesams, teikimo;

(19) didėjant fizinės ir skaitmeninės infrastruktūros tarpusavio priklausomybei, kibernetinė kenkimo veikla ypatingos svarbos srityse gali sutrikdyti fizinę infrastruktūrą arba jai pakenkti, o dėl fizinės infrastruktūros sabotažo gali būti neįmanoma naudotis skaitmeninėmis paslaugomis. Atsižvelgdamos į padidėjusią sudėtingų hibridinių išpuolių keliamą grėsmę, valstybės narės taip pat turėtų atsižvelgti į šiuos aspektus

imdamosi priemonių šiai rekomendacijai įgyvendinti. Atsižvelgiant į operatorių kibernetinio saugumo ir fizinio saugumo sąsajas, svarbu, kad pasirengimas naujos TIS 2 direktyvos perkėlimui į nacionalinę teisę ir taikymui būtų pradėtas kuo greičiau ir su naująja CER direktyva susijusi tokia veikla taip pat vyktų lygiagrečiai;

(20) be parengties stiprinimo, taip pat svarbu stiprinti pajėgumus greitai ir veiksmingai reaguoti tuo atveju, jei pasitvirtintų rizika, turinti įtakos ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų esminių paslaugų teikimui. Todėl šioje rekomendacijoje turėtų būti nurodytos priemonės, kurių turėtų būti imamasi tiek valstybių narių, tiek Sąjungos lygmeniu, įskaitant tvirtesnį bendradarbiavimą bei keitimąsi informacija pagal Sąjungos civilinės saugos mechanizmą ir atitinkamų Sąjungos kosmoso programos išteklių naudojimą;

(21) reaguodami į Tarybos prašymą, pateiktą išvadose dėl ES kibernetinio saugumo būklės[17], Komisija, Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai (toliau – vyriausiasis įgaliotinis) ir pagal Direktyvą (ES) 2016/1148 įsteigta Bendradarbiavimo grupė (toliau – TIS bendradarbiavimo grupė), koordinuodami veiksmus su atitinkamomis civilinėmis ir karinėmis įstaigomis bei agentūromis ir sukurtais tinklais, įskaitant EU-CyCLONe, atlieka kibernetinio saugumo rizikos vertinimą ir rengia jos scenarijus esant grėsmei ar galimam išpuoliui prieš valstybes nares ar šalis partneres. Daugiausia dėmesio skiriama ypatingos svarbos sektoriams, įskaitant energetikos, skaitmeninės infrastruktūros, transporto ir kosmoso sektorius;

(22) Nevere paskelbtame bendrame ministrų raginime[18] ir Tarybos išvadose dėl ES kibernetinio saugumo būklės taip pat paraginta didinti Sąjungos ryšių infrastruktūros ir tinklų atsparumą teikiant rekomendacijas valstybėms narėms ir Komisijai, remiantis rizikos vertinimu. Šį rizikos vertinimą šiuo metu atlieka TIS bendradarbiavimo grupė, padedama Komisijos ir ENISA ir bendradarbiaudama su Europos elektroninių ryšių reguliuotojų institucija (BEREC). Atliekant rizikos vertinimą ir spragų analizę nagrinėjama kibernetinių išpuolių rizika įvairiems ryšių infrastruktūros pasektoriams, įskaitant fiksuotojo ir judriojo ryšio infrastruktūrą, palydovus, jūrinius kabelius, interneto maršruto parinkimą ir t. t., taip suteikiant pagrindą darbui pagal šią rekomendaciją. Šiuo rizikos vertinimu bus teikiama informacija vykdomam tarpsektoriniam kibernetinės rizikos vertinimui ir scenarijams, kurių Taryba paprašė 2022 m. gegužės 23 d. Tarybos išvadose;

(23) šios dvejos pratybos bus nuoseklios ir koordinuojamos su scenarijų pratybomis, kuriomis daugiausia dėmesio skiriama civilinei saugai, atsižvelgiant į įvairias stichines ir žmogaus sukeltas nelaimes, įskaitant kibernetinio saugumo įvykius ir jų realų poveikį, ir kurias šiuo metu įgyvendina Komisija ir valstybės narės pagal Europos Parlamento ir Tarybos sprendimą Nr. 1313/2013/ES[19]. Siekiant veiksmingumo, efektyvumo ir nuoseklumo, ši rekomendacija turėtų būti įgyvendinama atsižvelgiant į tų pratybų rezultatus;

(24) ES 5G kibernetinio saugumo priemonių rinkinyje[20] nustatytos atitinkamos priemonės ir rizikos mažinimo planai, kuriais siekiama sustiprinti 5G tinklų saugumą.

---

17 Kibernetinio saugumo būklė. Taryba patvirtino išvadas, Europos Sąjungos Taryba (europa.eu)

18 https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

19 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

Atsižvelgiant į daugelio esminių paslaugų priklausomybę nuo 5G tinklų ir skaitmeninių ekosistemų tarpusavio sąsajų, labai svarbu, kad visos valstybės narės skubiai įgyvendintų priemonių rinkinyje rekomenduojamas priemones ir visų pirma taikytų atitinkamus apribojimus pagrindinių objektų, kurie ES koordinuotame rizikos vertinime apibrėžiami kaip ypatingos svarbos ir didesnės rizikos objektai, didelės rizikos tiekėjams;

(25) siekdama nedelsiant sustiprinti parengtį ir pajėgumus reaguoti į didelius kibernetinius incidentus, Komisija parengė trumpalaikę paramos valstybėms narėms programą, skirdama papildomą finansavimą ENISA. Finansuojamos paslaugos apims pasirengimo veiksmus, pavyzdžiui, ypatingos svarbos subjektų skverbimosi testavimą, siekiant nustatyti pažeidžiamumą. Ji taip pat padidins galimybes padėti valstybėms narėms didelių incidentų, darančių poveikį ypatingos svarbos subjektams, atveju. Tai pirmas žingsnis pagal Tarybos išvadas dėl kibernetinio saugumo būklės, kuriose Komisijos prašoma pateikti Reagavimo į kibernetinio saugumo krizes fondo pasiūlymą. Valstybės narės turėtų visapusiškai pasinaudoti tomis galimybėmis pagal taikomus reikalavimus;

(26) pasaulinis jūrinių duomenų ir elektroninių ryšių kabelių tinklas yra labai svarbus pasauliniam ir ES vidaus junglumui. Dėl didelio šių kabelių ilgio ir jų įrengimo jūros dugne daugumos kabelių ruožų povandeninis vizualinis stebėjimas yra itin sudėtingas. Bendra jurisdikcija ir kiti su šiais kabeliais susiję jurisdikcijos klausimai yra ypač svarbūs Europos ir tarptautiniam bendradarbiavimui infrastruktūros apsaugos ir atkūrimo srityje. Todėl šiuo metu vykdomus ir planuojamus rizikos vertinimus, susijusius su skaitmenine ir fizine infrastruktūra, kuria grindžiamos skaitmeninės paslaugos, būtina papildyti konkrečiais rizikos vertinimais ir galimybėmis imtis rizikos mažinimo priemonių, susijusių su jūriniais kabeliais. Todėl Komisija šiuo tikslu atlieka tyrimus ir dalijasi savo išvadomis su valstybėmis narėmis;

(27) su skaitmenine infrastruktūra susijusi rizika taip pat gali daryti poveikį šioje rekomendacijoje nustatytiems prioritetiniams energetikos ir transporto sektoriams. Toks poveikis gali būti daromas, pavyzdžiui, energetikos technologijoms, kuriomis integruojami skaitmeniniai komponentai. Susijusių tiekimo grandinių saugumas yra svarbus esminių paslaugų teikimo tęstinumui ir energetikos sektoriaus subjektų eksploatuojamų ypatingos svarbos infrastruktūros objektų strateginei kontrolei. Į tas aplinkybes turėtų būti atsižvelgta imantis priemonių ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumui didinti pagal šią rekomendaciją;

(28) didėjant kosmoso infrastruktūros ir kosmoso paslaugų svarbai su saugumu susijusiai veiklai, labai svarbu ne tik užtikrinti Sąjungos kosmoso priemonių ir paslaugų atsparumą ir apsaugą ES, bet ir įgyvendinant šią rekomendaciją užtikrinti, kad kosmoso sistemų ir kitų sektorių ypatingos svarbos infrastruktūros stebėjimo ir apsaugos programų teikiami kosmoso duomenys ir paslaugos būtų naudojami struktūriškiau. Būsimoje ES kosmoso strategijoje saugumo ir gynybos srityje bus pasiūlyti atitinkami šios srities veiksmai, į kuriuos reikėtų atsižvelgti įgyvendinant šią rekomendaciją;

(29) taip pat reikalingas bendradarbiavimas tarptautiniu lygmeniu, siekiant veiksmingai mažinti riziką ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumui Sąjungoje, atitinkamose trečiosiose šalyse arba tarptautiniuose vandenyse. Todėl valstybių narių turėtų būti paprašyta bendradarbiauti su Komisija ir vyriausiuoju įgaliotiniu, kad būtų imtasi tam tikrų veiksmų šiuo tikslu, susitariant, kad bet kokių

tokių veiksmų turi būti imamasi tik atsižvelgiant į jų atitinkamas užduotis ir pareigas pagal Sąjungos teisę, visų pirma ES sutarčių nuostatas dėl išorės santykių;

(30) kaip nustatyta Komunikate „Komisijos indėlis į Europos gynybą“[21], remdama planą „Saugumo ir gynybos strateginis kelrodis – Europos Sąjungai, kuri gina savo piliečius, vertybes bei interesus ir prisideda prie tarptautinės taikos ir saugumo“[22], Komisija, bendradarbiaudama su vyriausiuoju įgaliotiniu ir valstybėmis narėmis, įvertins sektorių atsparumo hibridinėms grėsmėms bazinius kriterijus, kad nustatytų spragas ir poreikius, taip pat jų šalinimo ar tenkinimo veiksmus iki 2023 m. Šia iniciatyva turėtų būti remiamasi vykdant veiklą pagal šią rekomendaciją, padedant stiprinti dalijimąsi informacija ir veiksmų koordinavimą, siekiant toliau stiprinti atsparumą, įskaitant ypatingos svarbos infrastruktūros objektų atsparumą;

(31) 2014 m. ES jūrų saugumo strategijoje ir jos veiksmų plane raginama didinti ypatingos svarbos jūrų infrastruktūros, įskaitant povandeninę infrastruktūrą, visų pirma jūrų transporto, energetikos ir ryšių infrastruktūros, objektų apsaugą, *inter alia*, didinant informuotumą apie padėtį jūroje pagerinus sąveikumą ir supaprastinus keitimąsi informacija (privalomą ir savanorišką). Strategija ir veiksmų planas šiuo metu atnaujinami ir į juos bus įtraukti aktyvesni veiksmai, kuriais siekiama apsaugoti ypatingos svarbos jūrų infrastruktūrą. Šie veiksmai turėtų būti grindžiami šia rekomendacija ir ją papildyti;

(32) valstybės narės turėtų atsižvelgti į visą Sąjungos saugumo mokslinių tyrimų programos potencialą, konkrečiai sutelkdamos dėmesį į jos konkretų ypatingos svarbos infrastruktūros prioritetą, visų pirma pagal Vidaus saugumo fondo finansuojamas programas, taip pat kitas galimas finansavimo galimybes Sąjungos lygmeniu, konkrečiai pasitelkdamos Europos regioninės plėtros fondą tiek, kiek konkrečios priemonės atitinka tinkamumo finansuoti reikalavimus. Atsparumo didinimas taip pat galėtų būti finansuojamas pagal planą „REPowerEU“. Visais atvejais Sąjungos finansavimo teikiamomis galimybėmis turi būti naudojamasi laikantis taikytinų teisinių reikalavimų,

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

I SKYRIUS. TIKSLAS, TAIKYMO SRITIS IR PRIORITETAI

(1) Šia rekomendacija valstybės narės raginamos imtis skubių ir veiksmingų priemonių ir lojaliai, veiksmingai, solidariai ir koordinuotai bendradarbiauti tarpusavyje, su Komisija ir kitomis atitinkamomis valdžios institucijomis, taip pat atitinkamais subjektais, kad esmines paslaugas vidaus rinkoje teikiantys ypatingos svarbos infrastruktūros objektai būtų atsparesni.

(2) Šioje rekomendacijoje nustatytos priemonės yra susijusios su infrastruktūra, kurią valstybė narė priskiria ypatingos svarbos infrastruktūros objektams, įskaitant Europos ypatingos svarbos infrastruktūros objektus.

(3) Įgyvendinant šią rekomendaciją pirmenybė turėtų būti teikiama subjektų, veikiančių energetikos, skaitmeninės infrastruktūros, transporto ir kosmoso sektoriuose, ir ypatingos svarbos infrastruktūros objektų, kuriuos tie subjektai eksploatuoja tarpvalstybiniu mastu, atsparumui žmogaus sukeltai rizikai didinti.

---

21 com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu)

22 Europos Sąjungos Taryba, 7371/22, 2022 m. kovo 21 d.

II SKYRIUS. GERESNĖ PARENGTIS

Valstybių narių lygmens veiksmai

(4) Valstybės narės raginamos atlikti arba atnaujinti Europos ypatingos svarbos infrastruktūros objektų, nustatytų transporto ir energetikos sektoriuose pagal Direktyvą 2008/114/EB, atsparumo rizikos vertinimus ir toliau tarpusavyje bendradarbiauti dėl tokių rizikos vertinimų ir dėl jų priimtų atsparumo didinimo priemonių, kai tinkama ir laikantis tos direktyvos.

(5) Be to, siekdamos užtikrinti aukštą ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumo lygį, valstybės narės turėtų paspartinti parengiamąjį darbą, kad naujoji CER direktyva būtų kuo greičiau perkelta į nacionalinę teisę ir pradėta taikyti:

(a) paspartinti nacionalinių strategijų, skirtų ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumui didinti siekiant reaguoti į dabartinę grėsmę, priėmimą arba atnaujinimą. Atitinkamos šios strategijos dalys turėtų būti pateiktos Komisijai;

(b) atlikti arba atnaujinti rizikos vertinimus atsižvelgiant į kintantį dabartinių grėsmių pobūdį, kiek tai susiję su subjektų, eksploatuojančių ypatingos svarbos infrastruktūros objektus atitinkamuose sektoriuose, ne tik energetikos, skaitmeninės infrastruktūros, transporto ir kosmoso sektorius, ir jei įmanoma tuose sektoriuose, kuriems taikoma naujoji CER direktyva (t. y. bankų, finansų rinkos infrastruktūros, skaitmeninės infrastruktūros, sveikatos, geriamojo vandens, nuotekų, viešojo administravimo, kosmoso ir maisto gamybos, perdirbimo ir paskirstymo), atsparumu, atsižvelgiant į galimą hibridinį atitinkamų grėsmių pobūdį, įskaitant grandininį poveikį ir klimato kaitos poveikį;

(c) informuoti Komisiją apie kiekvienam sektoriui ir pasektoriui nustatytos rizikos rūšis ir rizikos vertinimų rezultatus; tai galima atlikti naudojant bendrą ataskaitų teikimo šabloną, kurį Komisija parengė bendradarbiaudama su valstybėmis narėmis;

(d) paspartinti ypatingos svarbos subjektų nustatymo ir pripažinimo procesą, pirmenybę teikiant ypatingos svarbos subjektams, kurie:

(a) naudoja ypatingos svarbos infrastruktūrą, kuri yra fiziškai sujungta tarp dviejų ar daugiau valstybių narių;

(b) yra įmonių struktūrų, kurios yra sujungtos su ypatingos svarbos subjektais kitose valstybėse narėse arba susietos su jomis, dalis;

(c) yra nustatyti kaip tokie vienoje valstybėje narėje ir teikia esmines paslaugas šešiose ar daugiau valstybių narių ir todėl yra ypač svarbūs Europai, ir apie tai atitinkamai informuoja Komisiją;

(d) bendradarbiauja tarpusavyje, visų pirma ypatingos svarbos subjektų ir esminių paslaugų bei tarpvalstybinės reikšmės ypatingos svarbos infrastruktūros objektų klausimais, visų pirma dalyvaujant tarpusavio konsultacijose 5 punkto d papunkčio tikslais ir informuojant vienas kitą apie incidentą, kuris turi didelį arba potencialiai reikšmingą tarpvalstybinį trikdomąjį poveikį, kartu atitinkamai informuojant Komisiją;

(e) didinti paramą paskirtiems ypatingos svarbos subjektams, kad būtų padidintas jų atsparumas, kuri gali apimti rekomendacinės medžiagos ir metodikų teikimą, pratybų, skirtų jų atsparumui išbandyti, organizavimą ir jų darbuotojų konsultavimą

ir mokymą, taip pat sąlygų atlikti didesnės rizikos funkcijas atliekančių asmenų patikrinimus pagal Sąjungos ir nacionalinės teisės aktus, kurie yra ypatingos svarbos subjektų vykdomų darbuotojų saugumo valdymo priemonių dalis, sudarymą;

(f) paspartinti vieno bendrojo informacinio centro kompetentingoje institucijoje paskyrimą arba įsteigimą, kad būtų vykdoma ryšių palaikymo funkcija siekiant užtikrinti tarpvalstybinį bendradarbiavimą su kitų valstybių narių bendraisiais informaciniais punktais, susijusį su ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumu.

(6) Valstybės narės raginamos atlikti ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų testavimą nepalankiausiomis sąlygomis. Visų pirma valstybės narės raginamos didinti savo ir atitinkamų subjektų pasirengimą energetikos sektoriuje ir atlikti jame testavimą nepalankiausiomis sąlygomis, kai įmanoma, laikantis Sąjungos lygmeniu bendrai sutartų principų, kartu užtikrinant veiksmingus ryšius su atitinkamais subjektais. Prireikus vėliau būtų galima apsvarstyti galimybę atlikti testavimą nepalankiausiomis sąlygomis ir kituose prioritetiniuose sektoriuose, konkrečiai skaitmeninės infrastruktūros, transporto ir kosmoso sektoriuose, tinkamai atsižvelgiant į oro ir jūrų pasektoriuose pagal Sąjungos teisę atliekamus patikrinimus ir atsižvelgiant į atitinkamas sektorių teisės aktų nuostatas.

(7) Valstybės narės raginamos, kai tinkama ir laikantis Sąjungos teisės, bendradarbiauti su atitinkamomis trečiosiomis šalimis dėl tarpvalstybinės reikšmės ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumo.

(8) Valstybės narės raginamos, laikantis taikytinų reikalavimų, pasinaudoti potencialiomis Sąjungos ir nacionalinio lygmens finansavimo galimybėmis, kad Sąjungoje ypatingos svarbos infrastruktūros objektus eksploatuojantys subjektai, įskaitant, pavyzdžiui, transeuropinius tinklus, būtų atsparesni visoms didelėms grėsmėms, visų pirma pagal Vidaus saugumo fondo ir Europos regioninės plėtros fondo finansuojamas programas, su sąlyga, kad jie atitinka atitinkamus tinkamumo kriterijus, ir Europos infrastruktūros tinklų priemonę, įskaitant nuostatas dėl atsparumo klimato kaitai didinimo. Sąjungos civilinės saugos mechanizmo finansavimas taip pat gali būti naudojamas tuo tikslu, laikantis taikytinų reikalavimų, visų pirma projektams, susijusiems su rizikos vertinimais, investicijų planais ar tyrimais, gebėjimų stiprinimu arba žinių bazės gerinimu. Atsparumo didinimas taip pat galėtų būti finansuojamas pagal planą „REPowerEU“.

(9) Kalbant apie ryšių ir tinklų infrastruktūrą Sąjungoje, TIS bendradarbiavimo grupė, veikdama pagal Direktyvos (ES) 2016/1148 11 straipsnį, o vėliau – pagal TIS 2 direktyvos 14 straipsnį, turėtų paspartinti vykdomą darbą, susijusį su tiksliniu rizikos vertinimu, ir 2023 m. pradžioje turėtų pateikti pirmąsias rekomendacijas. Tas darbas turėtų būti atliekamas užtikrinant TIS bendradarbiavimo grupės darbo krypties informacinių ir ryšių technologijų tiekimo grandinės saugumo srityje ir kitų atitinkamų grupių, pavyzdžiui, Ypatingos svarbos subjektų atsparumo klausimų grupės, kuri turi būti įsteigta pagal naująją CER direktyvą, ir Priežiūros forumo, kuris turi būti įsteigtas pagal naująjį Skaitmeninės veiklos atsparumo aktą (SVAA)[23], darbo nuoseklumą ir papildomumą.

[23] COM(2020) 595 *final*

(10) TIS bendradarbiavimo grupės, kuri turi vykdyti savo užduotis pagal Direktyvos (ES) 2016/1148 11 straipsnį, o vėliau – pagal TIS 2 direktyvos 14 straipsnį, prašoma, padedant Komisijai ir ENISA, teikti pirmenybę darbui skaitmeninės infrastruktūros ir kosmoso sektorių saugumo srityje, be kita ko, rengiant politikos gaires ir kibernetinio saugumo rizikos valdymo metodikas bei priemones, grindžiamas visas pavojaus rūšis apimančiu požiūriu, kiek tai susiję su jūriniais ryšių kabeliais, rengiantis TIS 2 direktyvos įsigaliojimui, taip pat rengiant kosmoso sektoriaus veiklos vykdytojams skirtų kibernetinio saugumo rizikos valdymo priemonių gaires, siekiant padidinti antžeminės infrastruktūros, padedančios teikti kosmoso paslaugas, atsparumą.

(11) Valstybės narės turėtų visapusiškai naudotis Komisijos trumpalaikės paramos programos, įgyvendinamos kartu su ENISA, siūlomomis kibernetinio saugumo parengties paslaugomis, visų pirma skverbimosi testavimu siekiant nustatyti pažeidžiamumą, ir šiomis aplinkybėmis jos raginamos teikti pirmenybę ypatingos svarbos infrastruktūros objektus energetikos, skaitmeninės infrastruktūros ir transporto sektoriuose eksploatuojantiems subjektams.

(12) Valstybės narės turėtų nedelsdamos įgyvendinti ES 5G kibernetinio saugumo priemonių rinkinyje[24] rekomenduojamas priemones. Valstybės narės, kurios dar nėra nustačiusios apribojimų didelės rizikos tiekėjams, turėtų tai padaryti nedelsdamos, atsižvelgdamos į tai, kad dėl prarasto laiko gali padidėti tinklų pažeidžiamumas Sąjungoje. Jos taip pat turėtų sustiprinti fizinę ir nefizinę ypatingos svarbos ir didesnės rizikos 5G tinklų dalių apsaugą, be kita ko, taikydamos griežtą prieigos kontrolę. Be to, valstybės narės, bendradarbiaudamos su Komisija, turėtų įvertinti, ar reikia imtis papildomų veiksmų, įskaitant teisiškai privalomus reikalavimus Sąjungos lygmeniu, kad būtų užtikrintas nuoseklus 5G tinklų saugumo ir atsparumo lygis.

(13) Valstybės narės turėtų kuo greičiau įgyvendinti būsimą tinklo kodeksą, skirtą tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektams, remdamosi patirtimi, įgyta įgyvendinant TIS direktyvą, ir atitinkamomis TIS bendradarbiavimo grupės parengtomis gairėmis, visų pirma jos informaciniu dokumentu dėl esminių paslaugų operatoriams taikomų saugumo priemonių.

(14) Valstybės narės turėtų plėtoti GALILEO ir (arba) „Copernicus“ naudojimą stebėjimui ir dalytis atitinkama informacija su ekspertais, sušauktais pagal 15 punktą. Reikėtų tinkamai išnaudoti Sąjungos vyriausybinio palydovinio ryšio (GOVSATCOM) pagal Sąjungos kosmoso programą teikiamus pajėgumus ypatingos svarbos infrastruktūros objektų stebėsenai ir reagavimui į krizes remti.

Sąjungos lygmens veiksmai

(15) Komisija ketina stiprinti valstybių narių ekspertų bendradarbiavimą, kad padėtų didinti ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų fizinį nekibernetinį atsparumą, visų pirma:

(a) rengti bendras priemones, skirtas padėti valstybėms narėms didinti tokį atsparumą, įskaitant metodikas ir rizikos scenarijus, ir jas skatinti;

(b) remti bendrų principų, pagal kuriuos valstybės narės atlieka 6 punkte nurodytą testavimą nepalankiausiomis sąlygomis, rengimą, pradedant tokiais testavimais, daugiausia dėmesio skiriant žmogaus keliamai rizikai energetikos sektoriuje, o vėliau ir kituose pagrindiniuose sektoriuose, pavyzdžiui, skaitmeninės infrastruktūros,

[24] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

transporto ir kosmoso sektoriuose; šalinti kitą reikšmingą riziką ir pavojų; taip pat, kai aktualu, remti ir konsultuoti tokio testavimo nepalankiausiomis sąlygomis klausimais;

(c) sukurti saugią platformą, kurioje būtų kaupiama ir vertinama geriausia patirtis, nacionalinės patirties išvados ir kita informacija, susijusi su tokiu atsparumu, be kita ko, susijusi su to testavimo nepalankiausiomis sąlygomis atlikimu ir jo rezultatų įtraukimu į protokolus ir nenumatytų atvejų planus, ir būtų ja dalijamasi.

Tų ekspertų darbe ypatingas dėmesys turėtų būti skiriamas tarpsektorinei priklausomybei ir subjektams, eksploatuojantiems tarpvalstybinės reikšmės ypatingos svarbos infrastruktūros objektus, ir jį turėtų tęsti Ypatingos svarbos subjektų atsparumo klausimų grupė, kai ji bus įsteigta.

(16) Valstybės narės turėtų visapusiškai dalyvauti 15 punkte nurodytame tvirtesniame bendradarbiavime, be kita ko, paskirdamos atitinkamų ekspertinių žinių turinčius kontaktinius punktus ir dalydamosi patirtimi, susijusia su metodikomis, kaip atlikti testavimą nepalankiausiomis sąlygomis, ir tuo remiantis parengtais protokolais ir nenumatytų atvejų planais. Keičiantis informacija turėtų būti išsaugomas tos informacijos konfidencialumas ir ypatingos svarbos subjektų saugumo ir komerciniai interesai, kartu atsižvelgiant į valstybių narių saugumą. Tai nereiškia, kad bus teikiama informacija, kurios atskleidimas prieštarauja esminiams valstybių narių nacionalinio saugumo, visuomenės saugumo ar gynybos interesams.

(17) Komisija padės valstybėms narėms parengti vadovus ir gaires, pavyzdžiui, parengti Ypatingos svarbos infrastruktūros objektų ir viešųjų erdvių apsaugos nuo bepiločių orlaivių sistemų vadovą ir rizikos vertinimo priemones. EIVT, visų pirma per ES žvalgybos ir situacijų centrą ir jo hibridinių grėsmių analizės ir informavimo centrą, raginama rengti informacinius pranešimus apie grėsmes ypatingos svarbos infrastruktūrai ES, kad būtų pagerintas informuotumas apie padėtį.

(18) Komisija rems ypatingos svarbos infrastruktūros objektų atsparumo projektų, finansuojamų pagal Sąjungos mokslinių tyrimų ir inovacijų programas, rezultatų įsisavinimą. Komisija ketina padidinti tokių atsparumo didinimo priemonių finansavimą, neviršydama programai „Europos horizontas“ pagal 2021–2027 m. daugiametę finansinę programą skirto biudžeto. Tai turėtų sudaryti sąlygas spręsti dabartinius ir būsimus šios srities uždavinius, pavyzdžiui, ypatingos svarbos infrastruktūros objektų atsparumo klimato kaitai didinimą Sąjungoje, nepakenkiant kitų su civiliniu saugumu susijusių mokslinių tyrimų ir inovacijų finansavimui pagal programą „Europos horizontas“. Komisija taip pat dės daugiau pastangų, kad skleistų atitinkamų Sąjungos finansuojamų mokslinių tyrimų projektų rezultatus.

(19) TIS bendradarbiavimo grupės, bendradarbiaujant su Komisija ir vyriausiuoju įgaliotiniu, prašoma, atsižvelgiant į atitinkamas jų užduotis ir pareigas pagal Sąjungos teisę, intensyviau dirbti su atitinkamais tinklais ir civilinėmis bei karinėmis žinybomis atliekant rizikos vertinimą ir rengiant kibernetinio saugumo rizikos scenarijus, iš pradžių daugiausia dėmesio skiriant energetikos, ryšių, transporto ir kosmoso infrastruktūrai ir sektorių bei valstybių narių tarpusavio priklausomybei. Atliekant šį darbą reikėtų atsižvelgti į susijusią riziką fizinei infrastruktūrai, nuo kurios šie sektoriai priklauso. Rizikos vertinimai ir scenarijai turėtų būti rengiami reguliariai ir turėtų papildyti esamus arba planuojamus rizikos vertinimus šiuose sektoriuose, jais remtis ir jų nedubliuoti, taip pat jais turėtų būti remiamasi diskutuojant apie tai, kaip stiprinti bendrą ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumą ir spręsti pažeidžiamumo problemas.

(20) Komisija paspartins savo veiklą, kuria remiamas valstybių narių pasirengimas didelio masto kibernetinio saugumo incidentams ir reagavimas į juos, visų pirma:

(a) papildydama atitinkamus rizikos vertinimus, susijusius su tinklų ir informacijos saugumu, atliks išsamų tyrimą, kuriame būtų apžvelgta jūrinių kabelių infrastruktūra, jungianti valstybes nares ir Europą su visu pasauliu, įskaitant žemėlapį, jos pajėgumus ir dubliavimą, pažeidžiamumą, riziką paslaugų prieinamumui ir rizikos mažinimą. Išvadomis turėtų būti dalijamasi su valstybėmis narėmis;

(b) rems valstybių narių ir ES institucijų, įstaigų ir agentūrų pasirengimą didelio masto kibernetinio saugumo incidentams ir reagavimą į juos.

(21) Komisijos prašoma intensyviau dirbti rengiant į ateitį orientuotus išankstinius veiksmus, be kita ko, pagal SCSM, bendradarbiaujant su valstybėmis narėmis pagal Sprendimo 1313/2013/ES 6 ir 10 straipsnius ir planuojant nenumatytus atvejus, kad būtų remiamas Reagavimo į nelaimes koordinavimo centro operatyvinis pasirengimas.

Visų pirma Komisija imsis šių veiksmų:

(a) tęs darbą Reagavimo į nelaimes koordinavimo centre, susijusį su numatymu ir tarpsektoriniu prevencijos, parengties ir reagavimo planavimu, kad būtų galima numatyti ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų esminių paslaugų teikimo sutrikimus ir jiems pasirengti;

(b) didins investicijas į prevencinius metodus ir gyventojų pasirengimą tokių sutrikimų atveju, ypatingą dėmesį skiriant cheminėms, biologinėms, radiologinėms ir branduolinėms sprogstamosioms medžiagoms ar kitoms kylančioms žmogaus sukeltoms grėsmėms;

(c) stiprins keitimąsi atitinkamomis žiniomis ir geriausia praktika, taip pat geriau rengs ir vykdys pajėgumų stiprinimo veiklą, pavyzdžiui, mokymo kursus ir pratybas su ypatingos svarbos infrastruktūros objektus eksploatuojančiais subjektais, pasitelkdama esamas struktūras ir ekspertines žinias, pavyzdžiui, Sąjungos civilinės saugos žinių tinklą.

(22) Komisija skatins naudoti ES stebėjimo priemones („Copernicus“ ir GALILEO), kad padėtų valstybėms narėms stebėti ypatingos svarbos infrastruktūros objektus ir, kai aktualu, teritoriją prie pat jų, ir rems kitas Sąjungos kosmoso programoje numatytas stebėjimo galimybes.

(23) Kai aktualu ir laikydamosi savo atitinkamų įgaliojimų, Sąjungos agentūros ir kitos atitinkamos įstaigos raginamos teikti paramą klausimais, susijusiais su ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumu, visų pirma, pavyzdžiui:

(a) Europolas – informacijos rinkimo, nusikalstamų veikų analizės ir paramos tyrimams vykdant tarpvalstybinius teisėsaugos veiksmus;

(b) EMSA – klausimais, susijusiais su Sąjungos jūrų sektoriaus saugumu ir sauga, įskaitant jūrų stebėjimo paslaugas, susijusias su jūrų saugumu ir sauga;

(c) EUSPA – kiek tai susiję su veikla pagal Sąjungos kosmoso programą;

(d) ENISA – kiek tai susiję su veikla, susijusia su kibernetiniu saugumu.

III SKYRIUS. SUSTIPRINTAS REAGAVIMAS

Valstybių narių lygmens veiksmai

(24) Valstybės narės turėtų:

(a) koordinuoti reagavimą ir stebėti, kaip vyksta bendras tarpsektorinis reagavimas į didelius esminių paslaugų, kurias teikia ypatingos svarbos infrastruktūros objektus eksploatuojantys subjektai, sutrikimus pagal Tarybos atsako į krizes mechanizmą (IPCR) tarpvalstybinės reikšmės ypatingos svarbos infrastruktūros atveju, Didelės apimties kibernetinio saugumo incidentų ir krizių planą arba pagrindą koordinuotam ES atsakui į hibridines kampanijas hibridinės kampanijos atveju;

(b) aktyviau keistis informacija pagal Sąjungos civilinės saugos mechanizmą, kad būtų sustiprintas ankstyvasis perspėjimas ir koordinuojamas jų reagavimas pagal mechanizmą tokių didelių sutrikimų atveju, taip prireikus užtikrinant spartesnį Sąjungos tarpininkavimą;

(c) didinti savo pasirengimą pagal Sąjungos civilinės saugos mechanizmą reaguoti į tokius didelius sutrikimus, visų pirma tais atvejais, kai tikėtina, kad jie turės didelį tarpvalstybinį poveikį ar net visai Europai daromą poveikį, taip pat tarpsektorinį poveikį;

(d) bendradarbiauti su Komisija toliau plėtojant atitinkamus Europos civilinės saugos rezervo ir „rescEU“ reagavimo pajėgumus;

(e) raginti ypatingos svarbos infrastruktūros objektus eksploatuojančius subjektus ir atitinkamas nacionalines institucijas didinti tų subjektų pajėgumus greitai atkurti pagrindinį teikiamų esminių paslaugų veikimą;

(f) užtikrinti, kad tais atvejais, kai būtina atstatyti ypatingos svarbos infrastruktūros objektus, tokie atstatyti infrastruktūros objektai būtų atsparūs įvairiai didelei rizikai, kuri gali jiems kilti, įskaitant nepalankius klimato scenarijus.

(25) Valstybės narės raginamos paspartinti parengiamąjį darbą, susijusį su TIS 2 direktyvos perkėlimu į nacionalinę teisę ir taikymu, nedelsiant pradedant stiprinti nacionalinių reagavimo į kompiuterinius saugumo incidentus tarnybų (CSIRT) pajėgumus, atsižvelgiant į naujas CSIRT užduotis ir padidėjusį subjektų iš naujų sektorių skaičių, skubiai atnaujinant jų kibernetinio saugumo strategijas ir kuo greičiau priimant nacionalinius reagavimo į kibernetinio saugumo incidentus ir krizes planus.

Sąjungos lygmens veiksmai

(26) Valstybių narių ekspertai turėtų koordinuoti reagavimą į didelius esminių paslaugų, kurias teikia ypatingos svarbos infrastruktūros objektus eksploatuojantys subjektai, sutrikimus, kiek tai susiję su tų subjektų atsparumu ir reagavimu į tokius sutrikimus, kurie gali turėti įtakos Tarybos atsako į krizes mechanizmo (IPCR) veikimui.

(27) Komisija glaudžiai bendradarbiaus su valstybėmis narėmis siekdama toliau plėtoti dislokuojamus reagavimo į nelaimes pajėgumus, įskaitant ekspertus ir rezervo „rescEU“ atsargas pagal SCSM, kad būtų pagerintas operatyvinis pasirengimas reaguoti į tiesioginį ir netiesioginį didelių esminių paslaugų, kurias teikia ypatingos svarbos infrastruktūros objektus eksploatuojantys subjektai, sutrikimų poveikį.

(28) Atsižvelgdama į kintančią rizikos padėtį ir bendradarbiaudama su valstybėmis narėmis, Komisija pagal SCSM:

(a) nuolat analizuos ir tikrins esamų reagavimo pajėgumų tinkamumą ir operacinę parengtį;

(b) reguliariai peržiūrės galimą poreikį kurti naujus reagavimo pajėgumus ES lygmeniu naudojantis „rescEU“;

(c) toliau intensyvins tarpsektorinį bendradarbiavimą, kad būtų užtikrintas tinkamas reagavimas ES lygmeniu, ir rengs reguliarias pratybas šiam bendradarbiavimui išbandyti;

(d) toliau plėtos RNKC kaip tarpsektorinį krizių centrą ES lygmeniu, kad būtų koordinuojama parama nukentėjusioms valstybėms narėms.

(29) Komisija, bendradarbiaudama su vyriausiuoju įgaliotiniu ir glaudžiai konsultuodamasi su valstybėmis narėmis bei padedama atitinkamų Sąjungos agentūrų, parengs Ypatingos svarbos infrastruktūros objektų incidentų ir krizių valdymo planą, kuriame apibūdinami ir nustatomi valstybių narių ir ES institucijų, įstaigų, tarnybų ir agentūrų bendradarbiavimo reaguojant į ypatingos svarbos infrastruktūros objektų incidentus, visų pirma tais atvejais, kai dėl jų atsiranda didelių esminių paslaugų teikimo vidaus rinkai sutrikimų, tikslai ir būdai. Šiame plane turėtų būti pasinaudota esamomis integruoto politinio atsako į krizes (IPCR) priemonėmis, kuriomis koordinuojami reagavimo veiksmai.

(30) Komisija bendradarbiaus su suinteresuotaisiais subjektais ir ekspertais dėl galimų jūrinių kabelių infrastruktūros atkūrimo priemonių po susijusių incidentų, kurios bus pristatytos kartu su 20 punkto a papunktyje nurodytu padėties vertinimo tyrimu, taip pat toliau plėtos nenumatytų atvejų planavimą, rizikos scenarijus ir darbą, susijusį su Sąjungos atsparumu nelaimėms pagal Sąjungos civilinės saugos mechanizmą.

IV SKYRIUS. TARPTAUTINIS BENDRADARBIAVIMAS

(31) Komisija ir vyriausiasis įgaliotinis, kai tinkama ir atsižvelgiant į atitinkamas savo užduotis ir pareigas pagal Sąjungos teisę, rems šalis partneres, kad būtų didinamas jų teritorijoje ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumas.

(32) Komisija ir vyriausiasis įgaliotinis, vykdydami savo atitinkamas užduotis ir pareigas pagal Sąjungos teisę, stiprins ypatingos svarbos infrastruktūros objektų atsparumo koordinavimą su NATO per ES ir NATO struktūrinį dialogą atsparumo klausimais ir šiuo tikslu įsteigs darbo grupę.

(33) Valstybių narių prašoma, bendradarbiaujant su Komisija ir vyriausiuoju įgaliotiniu, prisidėti prie spartesnio ES hibridinių priemonių rinkinio ir įgyvendinimo gairių, nurodytų Tarybos išvadose dėl pagrindo koordinuotam ES atsakui į hibridines kampanijas[25], rengimo ir įgyvendinimo, ir vėliau jomis naudotis, kad būtų užtikrintas visapusiškas pagrindo koordinuotam ES atsakui į hibridines kampanijas veiksmingumas, visų pirma svarstant ir rengiant visapusišką ir koordinuotą ES atsaką į hibridines kampanijas ir hibridines grėsmes, be kita ko, nukreiptas prieš ypatingos svarbos infrastruktūros objektus eksploatuojančius subjektus.

(34) Komisija apsvarstys trečiųjų šalių atstovų dalyvavimą, kai aktualu ir tikslinga, valstybių narių ekspertams bendradarbiaujant ir keičiantis informacija ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumo srityje.

[25] Tarybos išvados dėl pagrindo koordinuotam ES atsakui į hibridines kampanijas, Europos Sąjungos Taryba (europa.eu)

[…]

Priimta Strasbūre

Tarybos vardu
Pirmininkas