Europos Sąjungos
Taryba

Briuselis, 2022 m. gruodžio 9 d.
(OR. en)

15623/22

Tarpinstitucinė byla:
2022/0338(NLE)

PROCIV 149	**ATO 102**
ENV 1248	**CSC 561**
JAI 1617	**ECOFIN 1279**
SAN 650	**CSCI 189**
COSI 315	**DATAPROTECT 346**
CHIMIE 100	**MI 912**
ENFOPOL 619	**CODEC 1916**
RECH 645	**COPS 581**
CT 220	**JAIEX 103**
DENLEG 93	**COPEN 430**
COTER 297	**IND 533**
RELEX 1657	**POLMIL 297**
ENER 654	**IPCR 116**
HYBRID 116	**DIGIT 231**
TRANS 768	**DISINFO 102**
CYBER 397	**CSDP/PSDC 848**
TELECOM 512	**MARE 71**
ESPACE 125	**POLMAR 78**

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	13713/22, 15454/22
Dalykas:	TARYBOS REKOMENDACIJA dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą

Delegacijoms priede pateikiama Tarybos rekomendacija dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą, kurią Taryba priėmė 2022 m. gruodžio 8 d įvykusiame 3920-ajame posėdyje.

PRIEDAS

TARYBOS REKOMENDACIJA (ES) 2022/…

... m. ... ... d.

dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą

(Tekstas svarbus EEE)

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 114 straipsnį ir 292 straipsnio pirmą ir antrą sakinius,

atsižvelgdama į Europos Komisijos pasiūlymą,

kadangi:

(1) siekiant užtikrinti vidaus rinkos veikimą, visos valstybės narės ir visa Sąjunga yra suinteresuotos, kad būtų aiškiai identifikuojama ir saugoma atitinkama ypatingos svarbos infrastruktūra, kuria toje rinkoje teikiamos esminės paslaugos, ypač pagrindiniuose sektoriuose, pavyzdžiui, energetikos, skaitmeninės infrastruktūros, transporto ir kosmoso, taip pat didelę tarpvalstybinę reikšmę turinti ypatingos svarbos infrastruktūra[1], kurios sutrikdymas darytų didelį poveikį kitoms valstybėms narėms;

[1] Valstybės narės turėtų įvertinti tą reikšmę laikydamosi savo nacionalinės praktikos ir gali tai padaryti remdamosi, be kitų veiksnių, rizikos vertinimu ir įvykio poveikiu bei pobūdžiu.

(2) šia rekomendacija, kuri yra neprivalomas aktas, demonstruojama valstybių narių politinė valia bendradarbiauti ir jų įsipareigojimas rekomenduoti priemones, akcentuojama Europos Komisijos pirmininkės paskelbtame penkių punktų plane, kartu visapusiškai gerbiant valstybių narių kompetenciją. Ši rekomendacija nedaro poveikio valstybių narių nacionalinio saugumo, visuomenės saugumo ar gynybos esminių interesų apsaugai ir neturėtų būti tikimasi, kad kuri nors valstybė narė dalysis informacija, jei tai galėtų pakenkti tiems interesams;

(3) nors pagrindinė atsakomybė už ypatingos svarbos infrastruktūros objektų saugumo ir jų teikiamų esminių paslaugų užtikrinimą tenka valstybėms narėms ir jų ypatingos svarbos infrastruktūros objektų operatoriams, tinkama vykdyti geresnį koordinavimą Sąjungos lygmeniu, ypač atsižvelgiant į kintančias grėsmes, kurios gali daryti poveikį vienu metu kelioms valstybėms narėms, pavyzdžiui, Rusijos agresijos karą prieš Ukrainą ir hibridines kampanijas prieš valstybes nares, arba daryti poveikį Sąjungos ekonomikos, vidaus rinkos ir visos visuomenės atsparumui ir tinkamam funkcionavimui. Ypatingas dėmesys turėtų būti skiriamas ypatingos svarbos infrastruktūrai už valstybių narių teritorijos ribų, pavyzdžiui, ypatingos svarbos povandeninei infrastruktūrai arba jūroje esančiai energetikos infrastruktūrai;

(4) 2022 m. spalio 20–21 d. išvadose Europos Vadovų Taryba griežtai pasmerkė sabotažo aktus prieš ypatingos svarbos infrastruktūrą, pavyzdžiui, įvykdytus prieš dujotiekius „Nord Stream“, nurodydama, kad Sąjunga yra pasirengusi vieningai ir ryžtingai atsakyti į bet kokį tyčinį ypatingos svarbos infrastruktūros trikdymą ar kitus hibridinius veiksmus;

(5) atsižvelgiant į sparčiai kintančią grėsmių panoramą, prioriteto tvarka svarbiausiuose sektoriuose (pavyzdžiui, energetikos, skaitmeninės infrastruktūros, transporto ir kosmoso) ir kituose valstybių narių nurodytuose atitinkamuose sektoriuose reikėtų imtis atsparumo didinimo priemonių. Tokiomis priemonėmis daugiausia dėmesio turėtų būti skiriama ypatingos svarbos infrastruktūros atsparumo didinimui atsižvelgiant į atitinkamą riziką, ypač grandininį poveikį, tiekimo grandinių sutrikimą, priklausomybę, klimato kaitos poveikį, nepatikimus pardavėjus bei partnerius ir hibridines grėsmes bei kampanijas, įskaitant užsienio manipuliavimą informacija ir kišimąsi. Kalbant apie nacionalinę ypatingos svarbos infrastruktūrą, atsižvelgiant į galimas pasekmes, pirmenybė turėtų būti teikiama didelę tarpvalstybinę reikšmę turinčiai ypatingos svarbos infrastruktūrai. Valstybės narės raginamos, kai tinkama, skubos tvarka numatyti tokias atsparumo didinimo priemones kartu toliau laikydamosi kintančioje teisinėje sistemoje nustatyto požiūrio;

(6) energetikos ir transporto sektorių Europos ypatingos svarbos infrastruktūros apsaugą šiuo metu reglamentuoja Tarybos direktyva 2008/114/EB[2], o tinklų ir informacinių sistemų saugumas, daugiausia dėmesio skiriant su kibernetine veikla susijusioms grėsmėms, visoje Sąjungoje užtikrinamas Europos Parlamento ir Tarybos direktyva (ES) 2016/1148[3]. Siekiant užtikrinti didesnį bendrą ypatingos svarbos infrastruktūros atsparumo ir apsaugos lygį, kibernetinį saugumą ir finansų rinkos apsaugą, esama teisinė sistema iš dalies keičiama ir papildoma priimant naujas ypatingos svarbos subjektams taikomas taisykles (Direktyva dėl ypatingos svarbos subjektų atsparumo), stiprinant taisykles, kuriomis visoje Sąjungoje užtikrinamas aukštas bendras kibernetinio saugumo lygis (TIS 2 direktyva), ir priimant naujas taisykles dėl skaitmeninės veiklos atsparumo finansų sektoriuje (SVAA);

(7) valstybės narės turėtų, laikydamosi Sąjungos ir nacionalinės teisės, naudotis visomis turimomis priemonėmis, kad darytų pažangą ir padėtų didinti fizinį ir kibernetinį atsparumą. Šiuo atžvilgiu ypatingos svarbos infrastruktūra turėtų būti suprantama kaip apimanti atitinkamą ypatingos svarbos infrastruktūrą, valstybės narės nustatytą nacionaliniu lygmeniu arba pagal Direktyvą 2008/114/EB priskirtą Europos ypatingos svarbos infrastruktūrai, taip pat ypatingos svarbos subjektus, kurie turi būti nustatyti pagal Direktyvą dėl ypatingos svarbos subjektų atsparumo arba, kai aktualu, subjektus, kuriems taikoma TIS 2 direktyva. Atsparumo sąvoka turėtų būti suprantama kaip nurodanti ypatingos svarbos infrastruktūros gebėjimą užkirsti kelią įvykiams, kuriais labai sutrikdomas arba gali būti labai sutrikdytas esminių paslaugų (t. y. paslaugų, kurios yra būtinos gyvybiškai svarbioms visuomenės ir ekonomikos funkcijoms, visuomenės saugai ir saugumui, gyventojų sveikatai ar aplinkai) teikimas vidaus rinkoje, apsaugoti nuo tokių įvykių, į juos reaguoti, juos atlaikyti, sušvelninti jų poveikį, juos amortizuoti, prie jų prisitaikyti ar po jų atsigauti;

---

2 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).

3 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).

(8) kad būtų koordinuojamas darbas, kuriuo siekiama užtikrinti didesnį bendrą ypatingos svarbos infrastruktūros atsparumo ir apsaugos lygį, kuris turi būti užtikrintas naujomis ypatingos svarbos subjektams taikytinomis taisyklėmis, turėtų būti sušaukti nacionaliniai ekspertai. Tas koordinuojamas darbas sudarytų sąlygas valstybėms narėms bendradarbiauti ir dalytis informacija apie veiklą, pavyzdžiui, metodikų, pagal kurias nustatoma, kokias esmines paslaugas teikia ypatingos svarbos infrastruktūros objektas, rengimą. Komisija jau pradėjo kviesti minėtus ekspertus į susitikimus, ėmėsi pastangų palengvinti jų darbą ir ketina tęsti šį darbą. Įsigaliojus naujai Direktyvai dėl ypatingos svarbos subjektų atsparumo ir pagal tą direktyvą įsteigus Ypatingos svarbos subjektų atsparumo klausimų grupę, ši grupė turėtų tęsti tokią parengiamąją veiklą vykdydama savo užduotis;

(9) pripažįstant, kad grėsmių panorama yra pakitusi, reikėtų toliau plėtoti potencialą nacionaliniu lygmeniu vykdyti ypatingos svarbos infrastruktūros testavimą nepalankiausiomis sąlygomis, nes toks testavimas galėtų būti naudingas ypatingos svarbos infrastruktūros atsparumui didinti. Atsižvelgiant į ypatingą energetikos sektoriaus svarbą ir į pasekmes visai Sąjungai, kurias sukeltų galimas jo sutrikimas, testavimas nepalankiausiomis sąlygomis vadovaujantis bendrai sutartais principais tam sektoriui būtų naudingiausias. Toks testavimas nepalankiausiomis sąlygomis patenka į valstybių narių kompetencijos sritį ir jos, laikydamosi savo nacionalinių teisinių sistemų, turėtų skatinti ir remti ypatingos svarbos infrastruktūros objektų operatorius, kad jie atliktų tokį testavimą nepalankiausiomis sąlygomis, kai vertinama, kad jis būtų naudingas;

(10) siekiant užtikrinti koordinuotą ir veiksmingą reagavimą į dabartines ir numatomas grėsmes, Komisija raginama teikti valstybėms narėms papildomą paramą, visų pirma teikiant atitinkamą informaciją pranešimų, neprivalomų vadovų ir gairių forma. Europos išorės veiksmų tarnyba (EIVT), visų pirma ES žvalgybos ir situacijų centras ir jo hibridinių grėsmių analizės ir informavimo centras, pagal ES bendro žvalgybinės informacijos analizės centro (SIAC) sistemą padedant Europos Sąjungos karinio štabo (EUMS) žvalgybos direktoratui, turėtų teikti grėsmių vertinimus. Komisijos taip pat prašoma, bendradarbiaujant su valstybėmis narėmis, skatinti naudotis Sąjungos finansuojamais mokslinių tyrimų ir inovacijų projektais;

(11) didėjant fizinės ir skaitmeninės infrastruktūros tarpusavio priklausomybei, įmanoma, kad kibernetinė kenkimo veikla, nukreipta į ypatingos svarbos sritis, sutrikdytų fizinę infrastruktūrą arba jai pakenktų, o dėl fizinės infrastruktūros sabotažo gali būti neįmanoma naudotis skaitmeninėmis paslaugomis. Valstybių narių prašoma kuo greičiau paspartinti naujosios ypatingos svarbos subjektams taikomos teisinės sistemos ir sustiprintos kibernetinio saugumo teisinės sistemos perkėlimo į nacionalinę teisę ir taikymo parengiamąjį darbą remiantis Direktyva (ES) 2016/1148 įsteigtoje bendradarbiavimo grupėje (TIS bendradarbiavimo grupėje) įgyta patirtimi, kartu nepamirštant perkėlimo į nacionalinę teisę terminų, taip pat prašoma, kad toks parengiamasis darbas vyktų vienu metu ir darniai;

(12) be parengties stiprinimo, taip pat svarbu stiprinti pajėgumus greitai ir veiksmingai reaguoti tuo atveju, jei sutriktų ypatingos svarbos infrastruktūros esminių paslaugų teikimas. Todėl šioje rekomendacijoje nurodytos priemonės tiek Sąjungos, tiek nacionaliniu lygmeniu, be kita ko, akcentuojamas pagalbinis vaidmuo ir pridėtinė vertė, kurie gali būti užtikrinti vykdant tvirtesnį bendradarbiavimą ir keičiantis informacija Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES[4] sukurto Sąjungos civilinės saugos mechanizmo (SCSM) kontekste ir naudojantis atitinkamais Europos Parlamento ir Tarybos reglamentu (ES) 2021/696[5] nustatytos Sąjungos kosmoso programos ištekliais;

(13) Komisija, Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai (vyriausiasis įgaliotinis) ir TIS bendradarbiavimo grupė, bendradarbiaudami su atitinkamomis civilinėmis ir karinėmis įstaigomis bei agentūromis ir jau sukurtais tinklais, įskaitant Europos ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (EU-CyCLONe), turi atlikti rizikos vertinimą ir parengti rizikos scenarijus. Be to, atsižvelgdama į Nevere paskelbtą bendrą ministrų raginimą, rizikos vertinimą šiuo metu atlieka TIS bendradarbiavimo grupė, padedama Komisijos bei Europos Sąjungos kibernetinio saugumo agentūros (ENISA) ir bendradarbiaudama su Europos elektroninių ryšių reguliuotojų institucija (BEREC). Šie du procesai bus nuoseklūs ir koordinuojami su šiuo metu Komisijos ir valstybių narių rengiamu scenarijų rengimo procesu pagal SCSM, įskaitant kibernetinio saugumo įvykius ir jų poveikį realiame gyvenime. Siekiant veiksmingumo, rezultatyvumo ir nuoseklumo, taip pat siekiant užtikrinti tinkamą šios rekomendacijos taikymą, į tų procesų rezultatus turėtų būti atsižvelgiama nacionaliniu lygmeniu;

---

4 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).

5 2021 m. balandžio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/696, kuriuo sudaroma Sąjungos kosmoso programa, įsteigiama Europos Sąjungos kosmoso programos agentūra ir panaikinami reglamentai (ES) Nr. 912/2010, (ES) Nr. 1285/2013 bei (ES) Nr. 377/2014 ir Sprendimas Nr. 541/2014/ES (OL L 170, 2021 5 12, p. 69).

(14) siekdama nedelsiant sustiprinti parengtį ir pajėgumą reaguoti į didelio masto kibernetinio saugumo incidentus, Komisija parengė trumpalaikę paramos valstybėms narėms programą, skirdama papildomą finansavimą ENISA. Siūlomos paslaugos, be kita ko, apima pasirengimo veiksmus, pavyzdžiui, subjektų skverbimosi testavimą siekiant nustatyti pažeidžiamumą. Programa taip pat gali padidinti galimybes padėti valstybėms narėms didelio masto kibernetinio saugumo incidentų, darančių poveikį ypatingos svarbos subjektams, atveju. Tai pirmas žingsnis vadovaujantis 2022 m. gegužės 23 d. Tarybos išvadomis dėl Europos Sąjungos pozicijos kibernetiniais klausimais (toliau – Tarybos išvados dėl ES pozicijos kibernetiniais klausimais), kuriose Komisijos prašoma pateikti pasiūlymą dėl Reagavimo į kibernetinio saugumo krizes fondo. Valstybės narės turėtų visapusiškai pasinaudoti tomis galimybėmis pagal taikomus reikalavimus ir raginamos tęsti darbą Sąjungos kibernetinių krizių valdymo srityje, visų pirma reguliariai stebėti ir vertinti pažangą, padarytą įgyvendinant Tarybos neseniai parengtas Kibernetinių krizių valdymo veiksmų gaires. Tos veiksmų gairės yra kintantis dokumentas ir prireikus turėtų būti peržiūrimos ir atnaujinamos;

(15) pasauliniai povandeniniai ryšių kabeliai yra labai svarbūs pasauliniam ir ES vidaus junglumui. Kadangi tokie kabeliai yra labai ilgi ir įrengti jūros dugne, daugumos kabelių ruožų povandeninį vizualinį stebėjimą vykdyti itin sudėtinga. Bendra jurisdikcija ir kiti su tokiais kabeliais susiję jurisdikcijos klausimai yra ypatingas Europos ir tarptautinio bendradarbiavimo infrastruktūros apsaugos ir atkūrimo srityje atvejis. 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 povandeniniais ryšių kabeliais. Valstybės narės prašo Komisijos tuo tikslu atlikti tyrimus ir pasidalyti savo išvadomis su valstybėmis narėmis;

(16) energetikos ir transporto sektoriams taip pat gali daryti poveikį su skaitmenine infrastruktūra susijusios grėsmės, pavyzdžiui, susijusios su energetikos technologijomis, kurioms naudojami skaitmeniniai komponentai. Susijusių tiekimo grandinių saugumas yra svarbus esminių paslaugų teikimo tęstinumui ir energetikos sektoriaus ypatingos svarbos infrastruktūros objektų strateginei kontrolei. Į tas aplinkybes turėtų būti atsižvelgiama imantis priemonių ypatingos svarbos infrastruktūros objektų atsparumui didinti pagal šią rekomendaciją;

(17) kosmoso infrastruktūra, su kosmosu susiję antžeminiai ištekliai, įskaitant gamybos įrenginius, ir kosmoso paslaugos tampa vis svarbesni su saugumu susijusiai veiklai, todėl labai svarbu ne tik užtikrinti Sąjungos kosmoso ir susijusių antžeminių išteklių bei paslaugų atsparumą ir apsaugą Sąjungoje. Dėl tų pačių priežasčių įgyvendinant šią rekomendaciją labai svarbu užtikrinti, kad kosmoso sistemų ir programų teikiami kosmoso duomenys ir paslaugos būtų struktūriškiau naudojami kitų sektorių ypatingos svarbos infrastruktūros stebėjimui, sekimui ir apsaugai. Būsimoje ES kosmoso strategijoje saugumo ir gynybos srityje bus pasiūlyti atitinkami šios srities veiksmai, į kuriuos reikėtų atsižvelgti įgyvendinant šią rekomendaciją;

(18) norint veiksmingai šalinti ypatingos svarbos infrastruktūrai kylančią riziką, be kita ko, tarptautiniuose vandenyse, taip pat reikia bendradarbiauti tarptautiniu lygmeniu. Todėl valstybių narių prašoma bendradarbiauti su Komisija ir vyriausiuoju įgaliotiniu, kad būtų imtasi tam tikrų veiksmų, kuriais siekiama tokio bendradarbiavimo, nepamirštant, kad bet kokių tokių veiksmų turi būti imamasi tik atsižvelgiant į jų atitinkamas užduotis ir pareigas pagal Sąjungos teisę, visų pirma Sutarčių nuostatas dėl išorės santykių;

(19) kaip nustatyta 2022 m. vasario 15 d. Komunikate „Komisijos indėlis į Europos gynybą“, remdama planą „Saugumo ir gynybos strateginis kelrodis – Europos Sąjungai, kuri gina savo piliečius, vertybes bei interesus ir prisideda prie tarptautinės taikos ir saugumo“, ne vėliau kaip 2023 m. Komisija, bendradarbiaudama su vyriausiuoju įgaliotiniu ir valstybėmis narėmis, įvertins sektorių atsparumo hibridinėms grėsmėms bazinius kriterijus, kad nustatytų spragas ir poreikius, taip pat tų spragų šalinimo ar poreikių tenkinimo galimybes. Ta iniciatyva turėtų būti remiamasi vykdant veiklą pagal šią rekomendaciją, padedant stiprinti dalijimąsi informacija ir veiksmų koordinavimą, siekiant toliau didinti atsparumą, įskaitant ypatingos svarbos infrastruktūros atsparumą;

(20) 2014 m. ES jūrų saugumo strategijoje ir jos peržiūrėtame veiksmų plane raginama didinti ypatingos svarbos jūrų infrastruktūros, įskaitant povandeninę infrastruktūrą, visų pirma jūrų transporto, energetikos ir ryšių infrastruktūros, objektų apsaugą, be kita ko, didinant informuotumą apie padėtį jūroje pagerinus sąveikumą ir supaprastinus keitimąsi informacija (privalomą ir savanorišką). Ta strategija ir tas veiksmų planas šiuo metu atnaujinami ir į juos bus įtraukti aktyvesni veiksmai, kuriais siekiama apsaugoti ypatingos svarbos jūrų infrastruktūrą. Šie veiksmai turėtų papildyti šią rekomendaciją;

(21) didinant ypatingos svarbos infrastruktūros atsparumą prisidedama prie platesnių pastangų kovoti su hibridinėmis grėsmėmis ir kampanijomis prieš Sąjungą ir jos valstybes nares. Ši rekomendacija grindžiama bendru komunikatu Europos Parlamentui ir Tarybai „Bendra kovos su mišriomis grėsmėmis sistema. Europos Sąjungos atsakas“. Bendros sistemos 1 veiksmas, konkrečiai apklausa dėl mišrių grėsmių, atlieka svarbų vaidmenį nustatant pažeidžiamumo elementus, kurie gali daryti poveikį nacionalinėms ir visos Europos struktūroms ir tinklams. Be to, įgyvendinant 2022 m. birželio 21 d. Tarybos išvadas dėl pagrindo koordinuotam ES atsakui į hibridines kampanijas, bus numatyti tvirtesni koordinavimo veiksmai taikant ES hibridinių priemonių rinkinį visose susijusiose srityse,

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

I SKYRIUS. TIKSLAS, TAIKYMO SRITIS IR PRIORITETAI

1) Šioje rekomendacijoje nurodyti tikslinai veiksmai Sąjungos ir nacionaliniu lygmeniu, kuriais savanoriškai remiamas ir didinamas ypatingos svarbos infrastruktūros atsparumas, daugiausia dėmesio skiriant didelę tarpvalstybinę reikšmę turinčiai ypatingos svarbos infrastruktūrai ir nustatytų pagrindinių sektorių infrastruktūrai, pavyzdžiui, energetikos, skaitmeninei, transporto ir kosmoso. Tuos tikslinius veiksmus sudaro geresnė parengtis, geresnis reagavimas ir tarptautinis bendradarbiavimas.

2) Informacija, kuria dalijamasi siekiant įgyvendinti šios rekomendacijos tikslus ir kuri yra konfidenciali pagal Sąjungos ir nacionalines taisykles, taip pat taisykles dėl verslo konfidencialumo, su Komisija ir kitomis atitinkamomis institucijomis turėtų būti keičiamasi tik kai tai yra būtina norint užtikrinti tinkamą šios rekomendacijos taikymą. Ši rekomendacija nedaro poveikio valstybių narių nacionalinio saugumo, visuomenės saugumo ar gynybos esminių interesų apsaugai ir neturėtų būti tikimasi, kad kuri nors valstybė narė dalysis informacija, jei tai galėtų prieštarauti tiems interesams.

II SKYRIUS. GERESNĖ PARENGTIS

Valstybių narių lygmens veiksmai

3) Atnaujindamos rizikos vertinimus arba esamas lygiavertes analizes, valstybės narės turėtų apsvarstyti galimybę laikytis visas pavojaus rūšis apimančio požiūrio, atsižvelgdamos į kintantį dabartinių grėsmių jų ypatingos svarbos infrastruktūrai pobūdį, ypač nustatytuose pagrindiniuose sektoriuose, ir, kai įmanoma, visuose sektoriuose, kuriems taikoma rengiama nauja ypatingos svarbos subjektams taikoma teisinė sistema.

4) Valstybių narių prašoma, kai įmanoma, paspartinti parengiamąjį darbą ir priimti atsparumo didinimo priemones, kaip pavedama pagal būsimą ypatingos svarbos subjektams taikomą teisinę sistemą, ypač daug dėmesio skiriant bendradarbiavimui ir dalijimuisi atitinkama informacija tarp valstybių narių ir su Komisija, susijusiems su didelę tarpvalstybinę reikšmę turinčių ypatingos svarbos subjektų nustatymu ir paramos nustatytiems ypatingos svarbos subjektams didinimu siekiant didinti jų atsparumą.

5) Valstybės narės turėtų remti ekspertų mokymą, pratybas ir ekspertų tarpusavio dalijimąsi geriausios praktikos pavyzdžiais ir įgyta patirtimi. Valstybės narės turėtų skatinti ekspertus dalyvauti esamų nacionalinių ir tarptautinių mokymo platformų veikloje, pavyzdžiui, pagal SCSM.

6) Valstybės narės turėtų skatinti ir remti ypatingos svarbos infrastruktūros objektų operatorius, bent energetikos sektoriuje, kad jie atliktų testavimą nepalankiausiomis sąlygomis laikydamiesi Sąjungos lygmeniu bendrai sutartų principų, kai tai naudinga. Testuojant nepalankiausiomis sąlygomis turėtų būti įvertinamas ypatingos svarbos infrastruktūros atsparumas priešiškoms žmogaus sukeltoms grėsmėms. Todėl valstybės narės turėtų stengtis kuo greičiau ir ne vėliau kaip iki 2023 m. pirmo ketvirčio pabaigos nustatyti, kokios atitinkamos ypatingos svarbos infrastruktūros testavimą reikia atlikti, ir pasikonsultuoti su atitinkamos ypatingos svarbos infrastruktūros objektų operatoriais. Be to, valstybės narės turėtų remti ypatingos svarbos infrastruktūros objektų operatorius, kad jie tą testavimą atliktų kuo greičiau ir siektų jį užbaigti ne vėliau kaip iki 2023 m. pabaigos, laikydamiesi nacionalinės teisės. Taryba ketina testavimo nepalankiausiomis sąlygomis padėtį įvertinti ne vėliau kaip iki 2023 m. balandžio mėn. pabaigos.

7) Ypatingos svarbos infrastruktūrai kylančios grėsmes sparčiai kinta, todėl itin svarbu išlaikyti aukštą apsaugos lygį. Valstybės narės raginamos skirti pakankamai finansinių išteklių savo atitinkamų nacionalinių institucijų pajėgumams stiprinti ir jas remti, kad jos galėtų padidinti ypatingos svarbos infrastruktūros atsparumą. Valstybės narės taip pat raginamos skirti pakankamai finansinių išteklių valdžios institucijoms, atsakingoms už didelio masto kibernetinio saugumo incidentų valdymą, jas remti ir užtikrinti, kad jų reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT) ir kompetentingos institucijos visapusiškai dalyvautų atitinkamai CSIRT tinkle ir EU-CyCLONe.

8) Valstybių narių prašoma, laikantis taikytinų reikalavimų, pačioms pasinaudoti potencialiomis Sąjungos ir nacionalinio lygmens finansavimo galimybėmis, kad padidintų ypatingos svarbos infrastruktūros atsparumą Sąjungoje, taip pat skatinti ypatingos svarbos infrastruktūros, įskaitant, pavyzdžiui, transeuropinius tinklus, objektų operatorius pasinaudoti tokiomis finansavimo galimybėmis, kad apsisaugotų nuo visų didelių grėsmių, visų pirma pagal programas, finansuojamas Vidaus saugumo fondo, nustatyto Europos Parlamento ir Tarybos reglamentu (ES) 2021/1149[6], Europos regioninės plėtros fondo, įsteigto Europos Parlamento ir Tarybos reglamentu (ES) Nr. 1301/2013[7], SCSM ir Komisijos plano „REPoweEU“ lėšomis. Valstybės narės taip pat raginamos kuo geriau pasinaudoti pagal mokslinių tyrimų programas, pavyzdžiui, programą „Europos horizontas“, sukurtą Europos Parlamento ir Tarybos reglamentu (ES) 2021/695[8], vykdomų atitinkamų projektų rezultatais.

---

6 2021 m. liepos 7 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/1149, kuriuo nustatomas Vidaus saugumo fondas (OL L 251, 2021 7 15, p. 94).

7 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1301/2013 dėl Europos regioninės plėtros fondo ir dėl konkrečių su investicijų į ekonomikos augimą ir darbo vietų kūrimą tikslu susijusių nuostatų, kuriuo panaikinamas Reglamentas (EB) Nr. 1080/2006 (OL L 347, 2013 12 20, p. 289).

8 2021 m. balandžio 28 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/695, kuriuo sukuriama bendroji mokslinių tyrimų ir inovacijų programa „Europos horizontas“, nustatomos su ja susijusios dalyvavimo ir sklaidos taisyklės ir panaikinami reglamentai (ES) Nr. 1290/2013 ir (ES) Nr. 1291/2013 (OL L 170, 2021 5 12, p. 1).

9) Kalbant apie Sąjungos ryšių ir tinklų infrastruktūrą, TIS bendradarbiavimo grupės prašoma, jai veikiant pagal Direktyvos (ES) 2016/1148 11 straipsnį, paspartinti vykdomą darbą, grindžiamą Nevere paskelbtu bendru ministrų raginimu dėl tikslinio rizikos vertinimo, ir ji turėtų kuo greičiau pateikti pirmąsias rekomendacijas. Tame rizikos vertinime turėtų būti pateikta informacija vykdomam tarpsektoriniam kibernetinės rizikos vertinimui ir scenarijams, kurių Taryba paprašė išvadose dėl ES pozicijos kibernetiniais klausimais. Be to, tas darbas turėtų būti atliekamas užtikrinant nuoseklumą ir papildomumą su TIS bendradarbiavimo grupės darbu, vykdomu pagal informacinių ir ryšių technologijų tiekimo grandinės saugumo darbo kryptį, taip pat kitų atitinkamų grupių darbu.

10) TIS bendradarbiavimo grupės taip pat prašoma, padedant Komisijai ir ENISA, tęsti darbą, susijusį su skaitmeninės infrastruktūros saugumu, be kita ko, povandeninės infrastruktūros, konkrečiai povandeninių ryšių kabelių, saugumu. Jos taip pat prašoma pradėti su kosmoso sektoriumi susijusį darbą, be kita ko, prireikus, remiantis visas pavojaus rūšis apimančiu požiūriu ir rizika grindžiamu požiūriu, parengti kosmoso sektoriaus veiklos vykdytojams skirtas politikos gaires ir kibernetinio saugumo valdymo metodikas, kurių tikslas – didinti 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, pavyzdžiui, skverbimosi testavimu siekiant nustatyti pažeidžiamumo atvejus, ir šiomis aplinkybėmis jos raginamos teikti pirmenybę ypatingos svarbos infrastruktūros objektus energetikos, skaitmeninės infrastruktūros ir transporto sektoriuose eksploatuojantiems subjektams.

12) Valstybės narės turėtų visapusiškai naudotis Europos kibernetinio saugumo kompetencijos centru (ECCC). Valstybės narės turėtų skatinti savo nacionalinius koordinavimo centrus iniciatyviai bendradarbiauti su kibernetinio saugumo bendruomenės nariais, kad būtų stiprinami Sąjungos ir nacionalinio lygmens pajėgumai geriau remti esminių paslaugų operatorius.

13) Svarbu, kad valstybės narės įgyvendintų ES 5G kibernetinio saugumo priemonių rinkinyje rekomenduojamas priemones, visų pirma, kad valstybės narės nustatytų apribojimus didelės rizikos tiekėjams, atsižvelgiant į tai, kad dėl prarasto laiko gali padidėti Sąjungos tinklų pažeidžiamumas, taip pat stiprinti 5G tinklų ypatingos svarbos ir didesnės rizikos dalių fizinę ir nefizinę apsaugą, be kita ko, taikant griežtą prieigos kontrolę. Be to, valstybės narės, bendradarbiaudamos su Komisija, turėtų įvertinti, ar reikia imtis papildomų veiksmų, kad būtų užtikrintas nuoseklus 5G tinklų saugumo ir atsparumo lygis.

14) Valstybės narės, kartu su Komisija ir ENISA, turėtų sutelkti dėmesį į 2022 m. spalio 17 d. Tarybos išvadų dėl IRT tiekimo grandinių saugumo įgyvendinimą.

15) Valstybės narės turėtų atsižvelgti į būsimą tinklo kodeksą, skirtą tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektams, [...] remdamosi patirtimi, įgyta įgyvendinant Direktyvą (ES) 2016/1148, ir atitinkamomis TIS bendradarbiavimo grupės parengtomis gairėmis, visų pirma jos informaciniu dokumentu dėl esminių paslaugų operatoriams skirtų saugumo priemonių.

16) Valstybės narės turėtų plėtoti „Copernicus“, GALILEO ir Europos geostracionarinės navigacinės tinklo sistemos (EGNOS) naudojimą stebėjimui, kad būtų dalijamasi 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 krizių numatymui bei reagavimui į jas remti.

Sąjungos lygmens veiksmai

17) Turėtų būti stiprinamas valstybių narių paskirtų ekspertų dialogas ir bendradarbiavimas tarpusavyje ir su Komisija, kad būtų didinamas ypatingos svarbos infrastruktūros fizinis atsparumas, visų pirma šiomis priemonėmis:

a) padedant rengti, plėtoti ir skatinti bendras savanoriškas priemones, kuriomis valstybėms narėms padedama didinti tokį atsparumą, įskaitant metodikas ir rizikos scenarijus;

b) padedant valstybėms narėms įgyvendinti ypatingos svarbos subjektams taikomą naują teisinę sistemą, be kita ko, raginant Komisiją laiku priimti deleguotąjį aktą;

c) remti 6 punkte nurodytą testavimą nepalankiausiomis sąlygomis, grindžiamą bendrais principais, pradedant tokiu testavimu, kuriame daugiausia dėmesio skiriama priešiškoms žmogaus sukeltoms grėsmėms energetikos sektoriuje, o vėliau ir kituose pagrindiniuose sektoriuose, taip pat valstybės narės prašymu teikti paramą ir konsultacijas, susijusias su tokiu testavimu nepalankiausiomis sąlygomis;

d) savanoriškai rinkti geriausios praktikos pavyzdžius, nacionalinės įgytos patirties pavyzdžius ir kitą su tokiu atsparumu susijusią informaciją, ją vertinti ir ja dalytis naudojantis bet kuria saugia platforma, kai Komisija ją sukurs.

Tų paskirtų ekspertų darbe ypatingas dėmesys turėtų būti skiriamas tarpsektorinei priklausomybei ir didelę tarpvalstybinę reikšmę turinčiai ypatingos svarbos infrastruktūrai, o Taryboje ir Komisijoje, kai tinkama, turėtų būti vykdoma tolesnė susijusi veikla.

18) Valstybės narės skatinamos naudotis visa Komisijos teikiama parama, pavyzdžiui, rengiamais vadovais ir gairėmis, tokiais kaip Ypatingos svarbos infrastruktūros ir viešųjų erdvių apsaugos nuo bepiločių orlaivių sistemų vadovas, ir rizikos vertinimo priemonėmis. EIVT, visų pirma per ES žvalgybos ir situacijų centrą ir jo hibridinių grėsmių analizės ir informavimo centrą, pagal SIAC sistemą padedant EUMS žvalgybos direktoratui, prašoma rengti informacinius pranešimus apie grėsmes Sąjungoje esančiai ypatingos svarbos infrastruktūrai, kad būtų pagerintas informuotumas apie padėtį.

19) Valstybės narės turėtų remti Komisijos veiksmus, kurių imamasi ypatingos svarbos infrastruktūros atsparumo projektų, finansuojamų pagal Sąjungos mokslinių tyrimų ir inovacijų programas, rezultatų įsisavinimui. Taryba atkreipia dėmesį į Komisijos ketinimą, laikantis 2021–2027 m. daugiametėje finansinėje programoje programai „Europos horizontas“ skirto biudžeto, didinti tokiam atsparumui skiriamą finansavimą nedarant neigiamo poveikio kitų su civiline sauga susijusių mokslinių tyrimų finansavimui ir inovacijų projektams pagal programą „Europos horizontas“.

20) Komisijos, vyriausiojo įgaliotinio ir TIS bendradarbiavimo grupės, kuriems pavestos Tarybos išvadose dėl ES pozicijos kibernetiniais klausimais nurodytos užduotys, prašoma, atsižvelgiant į Sąjungos teisėje nustatytas jų atitinkamas užduotis ir pareigas, intensyviau dirbti su atitinkamais tinklais ir civilinėmis bei karinėmis įstaigomis ir agentūromis atliekant rizikos vertinimą ir rengiant kibernetinio saugumo rizikos scenarijus, visų pirma atsižvelgiant į energetikos, skaitmeninės infrastruktūros, transporto ir kosmoso infrastruktūros svarbą ir sektorių bei valstybių narių tarpusavio priklausomybę. Atliekant tą darbą reikėtų atsižvelgti į susijusią riziką infrastruktūrai, nuo kurios tie sektoriai priklauso. Kai naudinga, rizikos vertinimas ir scenarijai turėtų būti rengiami reguliariai ir turėtų papildyti esamus arba planuojamus rizikos vertinimus tuose sektoriuose, jais remtis ir jų nedubliuoti, taip pat šiais vertinimais ir scenarijais turėtų būti remiamasi diskutuojant apie tai, kaip didinti bendrą ypatingos svarbos infrastruktūros objektus eksploatuojančių subjektų atsparumą ir spręsti pažeidžiamumo problemas.

21) Komisijos prašoma, atsižvelgiant į atitinkamus savo uždavinius krizių valdymo srityje, sparčiau įgyvendinti veiklą, kuria remiamas valstybių narių pasirengimas didelio masto kibernetinio saugumo incidentams ir reagavimas į juos, visų pirma:

a) kad būtų papildyti atitinkami rizikos vertinimai, susiję su tinklų ir informacijos saugumu, atlikti išsamų tyrimą[9], kuriame būtų apžvelgta povandeninių kabelių infrastruktūra, visų pirma povandeniniai ryšių kabeliai, jungianti valstybes nares ir Europą su visu pasauliu, o to tyrimo išvadomis turėtų būti pasidalyta su valstybėmis narėmis;

b) remti valstybių narių ir Sąjungos institucijų, įstaigų ir agentūrų pasirengimą didelio masto kibernetinio saugumo incidentams arba didelio masto incidentams pagal sustiprintą kibernetinio saugumo teisinę sistemą ir kitas atitinkamas taikytinas taisykles[10] ir reagavimą į juos;

c) sparčiau rengti Reagavimo į kibernetinio saugumo krizes fondo pagrindinę koncepciją vedant tinkamas diskusijas su valstybėmis narėmis.

22) Komisija raginama: intensyviau dirbti rengiant į ateitį orientuotus išankstinius veiksmus, be kita ko, bendradarbiaujant su valstybėmis narėmis pagal Sprendimo 1313/2013/ES 6 ir 10 straipsnius ir vykdant nenumatytų atvejų planavimą, kad būtų remiamas Reagavimo į nelaimes koordinavimo centro (RNKC) operatyvinis pasirengimas ir reagavimas į ypatingos svarbos infrastruktūros sutrikimus; didinti investicijas į prevencinius metodus ir gyventojų pasirengimą ir didinti paramą, susijusią su gebėjimų stiprinimu Sąjungos civilinės saugos žinių tinkle.

---

9 Šiame tyrime turėtų būti apžvelgti jos pajėgumai ir dubliavimas, pažeidžiamumas, grėsmės ir rizika paslaugų prieinamumui, (transatlantinių) povandeninių kabelių neveikimo laikotarpių poveikis valstybėms narėms ir visai Sąjungai ir rizikos mažinimas, kartu atsižvelgiant į tokios informacijos neskelbtinumą ir poreikį ją apsaugoti.

10 Ypatingas dėmesys taip pat turėtų būti skiriamas visai veiklai, kuria rengiamasi veiksmingam koordinuotam Sąjungos lygmens reagavimui didelio tarpvalstybinio kibernetinio incidento ar susijusios grėsmės, kuri galėtų padaryti sisteminį poveikį Sąjungos finansų sektoriui, atveju, kaip pavedama pagal naująją skaitmeninės veiklos atsparumo teisinę sistemą.

23) Komisija turėtų skatinti naudoti Sąjungos stebėjimo išteklius („Copernicus“, GALILEO ir EGNOS), kad padėtų valstybėms narėms stebėti ypatingos svarbos infrastruktūros objektus ir, kai aktualu, teritoriją prie pat jų, ir remti kitas Sąjungos kosmoso programoje numatytas stebėjimo galimybes, pavyzdžiui, informuotumo apie padėtį kosmose ir ES kosmoso stebėjimo ir sekimo sistemas.

24) Sąjungos agentūrų ir kitų atitinkamų įstaigų prašoma, kai aktualu ir laikantis savo atitinkamų įgaliojimų, teikti paramą klausimais, susijusiais su ypatingos svarbos infrastruktūros atsparumu, visų pirma:

a) Europos Sąjungos teisėsaugos bendradarbiavimo agentūros (Europolo) – informacijos rinkimo, kriminalinės žvalgybos informacijos analizės ir paramos tyrimams vykdant tarpvalstybinius teisėsaugos veiksmus srityse ir, kai aktualu ir tinkama, dalytis rezultatais su valstybėmis narėmis;

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

c) Europos Sąjungos kosmoso programos agentūra (EUSPA) ir Europos Sąjungos palydovų centras (SATCEN) gali padėti vykdydami operacijas pagal Sąjungos kosmoso programą;

d) ECCC, kiek tai susiję su veikla, susijusia su kibernetiniu saugumu, taip pat bendradarbiaujant su ENISA, galėtų remti inovacijas ir pramonės politiką kibernetinio saugumo srityje.

III SKYRIUS. SUSTIPRINTAS REAGAVIMAS

Valstybių narių lygmens veiksmai

25) Valstybių narių prašoma:

a) kai aktualu, toliau koordinuoti savo reagavimą ir stebėti, kaip vyksta bendras tarpsektorinis reagavimas į ypatingos svarbos infrastruktūros teikiamų esminių paslaugų didelius sutrikimus. Tai būtų galima daryti: pagal būsimą Koordinuojamo reagavimo į didelę tarpvalstybinę reikšmę turinčios ypatingos svarbos infrastruktūros sutrikimus planą; tarpvalstybinės reikšmės turinčios ypatingos svarbos infrastruktūros atveju naudojantis esamomis integruoto politinio atsako į krizes (IPCR) priemonėmis, skirtomis politinio atsako koordinavimui; pagal Didelio masto kibernetinio saugumo incidentų ir krizių planą pagal Komisijos rekomendaciją (ES) 2017/1584[11]; EU-CyCLONe, hibridinių grėsmių ir kampanijų atveju pagal koordinuotam ES atsakui į hibridines kampanijas skirtą priemonę ir ES hibridinių priemonių rinkinį ir dezinformacijos atveju Greitojo perspėjimo sistemoje;

b) aktyviau keistis operatyvinio lygmens informacija su RNKC pagal SCSM, kad būtų sustiprintas ankstyvasis perspėjimas ir koordinuojamas jų reagavimas pagal SCSM didelės tarpvalstybinės reikšmės turinčios ypatingos svarbos infrastruktūros sutrikimų atveju, taip prireikus užtikrinant spartesnį Sąjungos tarpininkaujamą reagavimą;

c) kai aktualu, didinti savo pasirengimą esamomis priemonėmis arba priemonėmis, kurios turi būti parengtos, reaguoti į tokius didelius a punkte nurodytus sutrikimus;

[11] 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).

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

e) skatinti ypatingos svarbos infrastruktūros objektų operatorius ir atitinkamas nacionalines institucijas stiprinti savo pajėgumus, kad galėtų greitai atkurti pagrindinį tų ypatingos svarbos infrastruktūros operatorių teikiamų esminių paslaugų veikimą;

f) skatinti ypatingos svarbos infrastruktūros objektų operatorius atstatant savo ypatingos svarbos infrastruktūros objektus užtikrinti kuo didesnį jų atsparumą (atsižvelgiant į priemonių proporcingumą rizikos vertinimo ir sąnaudų atžvilgiu) visų rūšių didelei rizikai, kuri gali jiems kilti, įskaitant nepalankaus klimato scenarijus.

26) Valstybių narių prašoma, kai įmanoma, paspartinti parengiamąjį darbą, pavestą pagal sustiprintą kibernetinio saugumo teisinę sistemą, siekiant stiprinti nacionalinių CSIRT pajėgumus, atsižvelgiant į naujas CSIRT užduotis ir padidėjusį subjektų iš naujų sektorių skaičių, laiku peržiūrint ir atnaujinant jų kibernetinio saugumo strategijas ir kuo greičiau priimant nacionalinius reagavimo į kibernetinio saugumo incidentus ir krizes planus, jeigu jie dar nepriimti.

27) Valstybių narių prašoma nacionaliniu lygmeniu apsvarstyti, kokios priemonės yra tinkamiausios siekiant užtikrinti, kad atitinkami suinteresuotieji subjektai žinotų apie poreikį didinti ypatingos svarbos infrastruktūros atsparumą bendradarbiaujant su patikimais pardavėjais ir partneriais. Svarbu investuoti į papildomus pajėgumus, ypač tuose sektoriuose, kuriuose dabartinės infrastruktūros gyvavimo laikotarpis jau baigiasi (pavyzdžiui, povandeninių ryšių kabelių infrastruktūra), kad būtų galima užtikrinti esminių paslaugų teikimo tęstinumą sutrikimų atveju ir sumažinti nepageidaujamą priklausomybę.

28) Valstybės narės raginamos skirti dėmesio iniciatyviai strateginei nacionalinio lygmens komunikacijai kovos su hibridinėmis grėsmėmis ir kampanijomis kontekste, taip pat atsižvelgiant į galimybę, kad priešiškos jėgos gali siekti vykdyti užsienio manipuliavimą informacija ir kišimąsi formuodamos su incidentais, nukreiptais prieš ypatingos svarbos infrastruktūros objektus, susijusius naratyvus.

Sąjungos lygmens veiksmai

29) Komisijos prašoma glaudžiai bendradarbiauti su valstybėmis narėmis, toliau plėtoti atitinkamas įstaigas, priemones ir reagavimo pajėgumus, siekiant sustiprinti operatyvinį pasirengimą šalinti atitinkamų esminių paslaugų, kurias teikia ypatingos svarbos infrastruktūros objektai, sutrikimų tiesioginį ir netiesioginį poveikį, visų pirma pasitelkti ekspertus ir turimus išteklius iš Europos civilinės saugos rezervo ir „rescEU“ pagal SCSM arba būsimas greitojo reagavimo į hibridines grėsmes grupes.

30) Komisijos prašoma, atsižvelgiant į kintančią grėsmių panoramą ir bendradarbiaujant su valstybėmis narėmis, pagal SCSM:

a) nuolat analizuoti ir testuoti esamų reagavimo pajėgumų tinkamumą ir operacinę parengtį;

b) reguliariai stebėti ir nustatyti galimus didelius Europos civilinės saugos rezervo ir „rescEU“ pajėgumų reagavimo pajėgumų trūkumus;

c) toliau intensyvinti tarpsektorinį bendradarbiavimą, kad būtų užtikrintas tinkamas reagavimas Sąjungos lygmeniu, ir bendradarbiaujant su viena ar daugiau valstybių narių rengti reguliarius mokymus ar pratybas tokiam bendradarbiavimui išbandyti;

d) toliau plėtoti RNKC kaip tarpsektorinį Sąjungos lygmens ekstremaliųjų situacijų centrą, skirtą paramai nukentėjusioms valstybėms narėms koordinuoti.

31) Taryba yra pasiryžusi pradėti darbą, kad būtų patvirtintas Koordinuojamo reagavimo į didelę tarpvalstybinę reikšmę turinčios ypatingos svarbos infrastruktūros sutrikimus planas, kuriame aprašomi ir nustatomi valstybių narių ir Sąjungos institucijų, įstaigų, organų ir agentūrų bendradarbiavimo tikslai ir būdai joms reaguojant į incidentus prieš tokius ypatingos svarbos infrastruktūros objektus. Taryba laukia, kol Komisija parengs tokio plano projektą remdamasi atitinkamų Sąjungos agentūrų parama ir pasiūlymais. Planas turi būti visapusiškai suderintas ir sąveikus su peržiūrėtu Sąjungos operatyvinių veiksmų protokolu dėl kovos su hibridinėmis grėsmėmis (ES hibridinių grėsmių vadovu) ir jame turi būti atsižvelgiama į esamą Koordinuoto atsako į didelio masto tarpvalstybinius kibernetinio saugumo incidentus ir krizes planą[12] ir EU-CyCLONe įgaliojimus, nustatytus TIS 2 direktyvoje, taip pat turi būti vengiama struktūrų ir veiklos dubliavimo. Tame plane turėtų būti visapusiškai atsižvelgiama į esamas IPCR priemones, kuriomis koordinuojami reagavimo veiksmai.

[12] 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.

32) Komisijos prašoma konsultuotis su atitinkamais suinteresuotaisiais subjektais ir ekspertais dėl tinkamų priemonių, susijusių su galimais dideliais su povandenine infrastruktūra susijusiais incidentais; tos priemonės turi būti pristatytos kartu su 20 punkto a papunktyje nurodytu padėties vertinimo tyrimu, taip pat toliau plėtoti nenumatytų atvejų planavimą, rizikos scenarijus ir Sąjungos atsparumo nelaimėms tikslus, išdėstytus Sprendime Nr. 1313/2013/ES.

IV SKYRIUS. TARPTAUTINIS BENDRADARBIAVIMAS

Valstybių narių lygmens veiksmai

33) Valstybės narės turėtų, kai tinkama ir laikantis Sąjungos teisės, bendradarbiauti su atitinkamomis trečiosiomis valstybėmis dėl didelės tarpvalstybinės reikšmės turinčios ypatingos svarbos infrastruktūros atsparumo.

34) Valstybės narės skatinamos bendradarbiauti su Komisija ir vyriausiuoju įgaliotiniu, kad būtų veiksmingai šalinama rizika tarptautiniuose vandenyse esančiai ypatingos svarbos infrastruktūrai.

35) Valstybių narių prašoma, bendradarbiaujant su Komisija ir vyriausiuoju įgaliotiniu, prisidėti prie ES hibridinių priemonių rinkinio ir įgyvendinimo gairių, nurodytų 2022 m. birželio 21 d. Tarybos išvadose dėl koordinuotam ES atsakui į hibridines kampanijas skirtų priemonių, spartesnio rengimo ir įgyvendinimo, ir vėliau jais naudotis, kad būtų užtikrintas visapusiškas koordinuotam Sąjungos atsakui į hibridines kampanijas skirtų priemonių veiksmingumas, visų pirma svarstant ir rengiant visapusišką ir koordinuotą Sąjungos atsaką į hibridines kampanijas ir hibridines grėsmes, be kita ko, nukreiptas prieš ypatingos svarbos infrastruktūros objektų operatorius.

Sąjungos lygmens veiksmai

36) Komisijos ir vyriausiojo įgaliotinio prašoma, kai tikslinga ir atsižvelgiant į Sąjungos teisėje nustatytus jų atitinkamas užduotis ir atsakomybę, remti atitinkamas trečiąsias valstybes, kad būtų didinamas jų teritorijoje esančios ypatingos svarbos infrastruktūros, visų pirma tos infrastruktūros, kuri yra fiziškai sujungta tarp jų teritorijos ir vienos iš valstybių narių teritorijos, atsparumas.

37) Komisija ir vyriausiasis įgaliotinis, atsižvelgdami į Sąjungos teisėje nustatytus atitinkamas savo užduotis ir atsakomybę, stiprins veiksmų koordinavimą su NATO bendro intereso ypatingos svarbos infrastruktūros atsparumo srityje pasitelkiant ES ir NATO struktūrinį dialogą atsparumo klausimais, visapusiškai atsižvelgdami į Sutartyse nustatytą Sąjungos ir valstybių narių kompetenciją ir pagrindinius principus, kuriais grindžiamas ES ir NATO bendradarbiavimas, kaip patvirtinta Europos Vadovų Tarybos, visų pirma abipusiškumo, įtraukumo ir sprendimų priėmimo autonomiškumo principus. Šiomis aplinkybėmis tas bendradarbiavimas bus tęsiamas vedant ES ir NATO struktūrinį dialogą atsparumo klausimais, kuris įtvirtintas esamame štabų tarpusavio ryšių mechanizme, kuriuo įgyvendinamos bendros deklaracijos, kartu užtikrinant visišką skaidrumą ir visų valstybių narių dalyvavimą.

38) Komisijos prašoma apsvarstyti galimybę leisti atitinkamiems trečiųjų valstybių atstovams dalyvauti, kai reikalinga ir tinkama, vykdant valstybių narių bendradarbiavimą ir keitimąsi informacija ypatingos svarbos infrastruktūros, kuri yra fiziškai sujungta su valstybės narės ir tos trečiosios valstybės teritorija, atsparumo srityje.

Priimta …

Tarybos vardu

Pirmininkas / Pirmininkė