Europos Sąjungos Taryba

Briuselis, 2025 m. birželio 6 d.
(OR. en)

9794/25

Tarpinstitucinė byla:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
data:	2025 m. birželio 6 d.
kam:	Delegacijoms
Dalykas:	Tarybos rekomendacija dėl ES kibernetinių krizių valdymo plano – Tarybos rekomendacija, kurią Taryba patvirtino 2025 m. birželio 6 d. posėdyje

Delegacijoms priede pateikiama Tarybos rekomendacija, kurią Taryba patvirtino 2025 m. birželio 6 d. posėdyje.

PRIEDAS

TARYBOS REKOMENDACIJA

dėl ES kibernetinių krizių valdymo plano

EUROPOS SĄJUNGOS TARYBA,

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

atsižvelgdama į Europos Komisijos pasiūlymą,

kadangi:

(1) skaitmeninės technologijos ir visuotinis junglumas sudaro Sąjungos ekonomikos augimo, konkurencingumo ir ypatingos svarbos infrastruktūros transformacijos pagrindą. Tačiau dėl tarpusavyje susijusios ekonomikos ir vis didesnės jos skaitmenizacijos taip pat didėja kibernetinio saugumo incidentų ir kibernetinių išpuolių rizika. Be to, augant geopolitinei įtampai, gausėjant konfliktams ir didėjant strateginei konkurencijai atitinkamai didėja ir kibernetinės kenkimo veiklos poveikis, apimtis bei sudėtingumas. Tokia veikla gali būti hibridinių kampanijų arba karinių operacijų dalis. Ji taip pat gali tiesiogiai paveikti Sąjungos saugumą, ekonomiką ir visuomenę. Be to, tokios kenkimo veiklos poveikis gali persiduoti, ypač kai ji yra nukreipta prieš šalis, kurios yra tarptautinės strateginės partnerės, tokios kaip šalys kandidatės ar kaimyninės šalys;

(2) didelio masto kibernetinio saugumo incidentas gali sukelti tokio lygio sutrikimą, į kurį viena valstybė narė nepajėgtų reaguoti arba kuris darytų didelį poveikį daugiau nei vienai valstybei narei. Toks incidentas, priklausomai nuo jo priežasties ir poveikio, galėtų eskaluotis ir virsti plataus masto krize, kuri sutrikdytų tinkamą vidaus rinkos veikimą arba sukeltų rimtą pavojų visuomenės saugumui ir subjektų ar piliečių saugai keliose valstybėse narėse ar visoje Sąjungoje. Veiksmingas krizių valdymas yra itin svarbus siekiant išlaikyti ekonominį stabilumą ir apsaugoti Europos šalių vyriausybes, ypatingos svarbos infrastruktūrą, įmones ir piliečius, taip pat prisidėti prie tarptautinio saugumo ir stabilumo kibernetinėje erdvėje. Taigi kibernetinių krizių valdymas yra neatsiejama visa apimančios ES krizių valdymo sistemos dalis;

(3) atsižvelgiant į Sąjungos subjektų ir valstybių narių IRT aplinkos tarpusavio priklausomybę ir tarpusavio jungtis, Sąjungos subjektą paveikęs incidentas gali kelti kibernetinio saugumo riziką valstybėms narėms ir atvirkščiai. ES kibernetinių krizių valdymo plano (toliau – Kibernetinio saugumo planas) kontekste labai svarbu dalytis atitinkama informacija ir koordinuoti veiksmus, kiek tai susiję su didelio masto kibernetinio saugumo incidentais ir dideliais incidentais, kaip apibrėžta Reglamento (ES, Euratomas) 2023/2841[1] 3 straipsnio 8 punkte;

[1] 2023 m. gruodžio 13 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2023/2841, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti, OL L, 2023/2841, 2023 12 18, p. 1–27.

(4) kilus krizei, dėl kurios pagal Tarybos įgyvendinimo sprendimą (ES) 2018/1993[2] buvo aktyvuotas ES integruotas politinio atsako į krizes mechanizmas (toliau – IPCR mechanizmas), Kibernetinio saugumo planu koordinavimo ir atsako tikslais turėtų būti visapusiškai atsižvelgiama į IPCR mechanizmą. Politinis ir strateginis koordinavimas būtų vykdomas per IPCR. IPCR mechanizmas yra horizontalaus koordinavimo ir atsako Sąjungos politiniu lygmeniu priemonė. Laikantis IPCR mechanizmo, sprendimą aktyvuoti arba deaktyvuoti IPCR priima Europos Sąjungos Tarybai pirmininkaujanti valstybė narė. Komisijos tarnybų ir Europos išorės veiksmų tarnybos (EIVT) parengtomis integruoto informuotumo apie padėtį ir jos analizės (ISAA) ataskaitomis padedama vykdyti IPCR darbą tiek dalijimosi informacija režimu, tiek veikimo visa apimtimi režimu;

(5) pagrindinė atsakomybė už kibernetinio saugumo incidentų ir kibernetinių krizių valdymą tenka valstybėms narėms. Visgi dėl kibernetinio saugumo incidentų galimo tarpvalstybinio ir tarpsektorinio pobūdžio valstybės narės ir atitinkami Sąjungos subjektai turi bendradarbiauti techniniu, operatyviniu ir politiniu lygmenimis, kad veiksmai būtų veiksmingai koordinuojami visoje Sąjungoje. Visas kibernetinių krizių valdymo ciklas apima parengtį ir bendrą informuotumą apie padėtį tam, kad būtų galima numatyti didelio masto kibernetinio saugumo incidentus, būtinus aptikimo pajėgumus siekiant nustatyti reikiamas atsako ir veiklos atkūrimo priemones didelio masto kibernetinio saugumo incidentams sušvelninti ir suvaldyti, taip pat reikiamus reagavimo pajėgumus, kad būtų atgrasyta nuo kitų incidentų ir jiems būtų užkirstas kelias;

[2] 2018 m. gruodžio 11 d. Tarybos įgyvendinimo sprendimas (ES) 2018/1993 dėl ES integruoto politinio atsako į krizes mechanizmo, OL L 320, 2018 12 17, p. 28–34.

(6) Komisijos rekomendacijoje (ES) 2017/1584[3] dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes nustatyti valstybių narių ir Sąjungos subjektų bendradarbiavimo reaguojant į didelio masto kibernetinio saugumo incidentus ir kibernetines krizes tikslai ir būdai. Joje apžvelgti atitinkami techninio, operatyvinio ir politinio lygmenų subjektai ir paaiškinta, kaip jie integruoti į esamus Sąjungos krizių valdymo mechanizmus, pavyzdžiui, IPCR mechanizmą. Pagrindiniai Rekomendacijoje (ES) 2017/1584 nustatyti principai išlieka: tai – subsidiarumas, papildomumas ir informacijos konfidencialumas, taip pat veikimas trimis lygmenimis (techniniu, operatyviniu ir politiniu); Ši rekomendacija grindžiama tais pagrindiniais principais ir ja ketinama pakeisti Rekomendaciją (ES) 2017/1584, nustatant naują Sąjungos kibernetinio saugumo krizių valdymo sistemą;

(7) kai kurios šioje rekomendacijoje vartojamos apibrėžtys grindžiamos Direktyvoje (ES) 2022/2555[4] vartojamomis apibrėžtimis ir terminais. Tačiau šios rekomendacijos taikymo sritis skiriasi nuo Direktyvos (ES) 2022/2555 taikymo srities. Šioje rekomendacijoje nustatoma Sąjungos kibernetinių krizių valdymo sistema, atsižvelgiant į bendrą ES parengtį didelio masto kibernetinio saugumo incidentams ir dėl tokių incidentų kylančioms kibernetinėms krizėms, nepriklausomai nuo to, kurį sektorių ar subjektą jie veikia. Kiek įmanoma, apibrėžtys grindžiamos Direktyvoje (ES) 2022/2555 pateiktomis apibrėžtimis;

---

[3] 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. 36–58.

[4] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva), OL L 333, 2022 12 27, p. 80–152.

(8) atnaujintas Kibernetinio saugumo planas yra reikalingas tam, kad būtų pateiktos aiškios ir prieinamos gairės, paaiškinančios, kas yra didelio masto kibernetinio saugumo incidentas arba Sąjungos lygmens kibernetinė krizė, kaip aktyvuojama krizių valdymo sistema, kokius vaidmenis atlieka atitinkami Sąjungos lygmens tinklai, subjektai bei mechanizmai ir kokia yra šių subjektų ir mechanizmų sąveika per visą kibernetinės krizės ciklą. Kibernetinio saugumo planu siekiama prisidėti prie platesnės ES civilinių ir karinių santykių sistemos kibernetinių krizių valdymo kontekste, be kita ko, atsižvelgiant į ES ir NATO santykių stiprinimą, kai įmanoma, be kita ko, pasitelkiant įtraukius, abipusius ir nediskriminacinius patobulintus dalijimosi informacija mechanizmus kibernetinių krizių valdymo srityje;

(9) tarpsektorinis krizių valdymas Sąjungos lygmeniu turėtų būti sustiprintas siekiant sudaryti sąlygas integruotam atsakui į krizes, ypač tais atvejais, kai didelio masto kibernetinio saugumo incidentai ir krizės sukelia fizinių pasekmių. Šia rekomendacija papildomas IPCR mechanizmas ir kiti Sąjungos krizių valdymo mechanizmai, įskaitant Komisijos bendrą skubaus įspėjimo sistemą ARGUS, Sąjungos civilinės saugos mechanizmą (SCSM), kuriam padeda Reagavimo į nelaimes koordinavimo centras (RNKC), įsteigtas prie SCSM Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo[5] (toliau – SCSM sprendimas), EIVT reagavimo į krizes mechanizmą, taip pat kitus procesus, tokius kaip aprašytieji ES kibernetinio saugumo diplomatijos priemonių rinkinyje[6], hibridinių priemonių rinkinyje[7] ir peržiūrėtame ES protokole dėl kovos su hibridinėmis grėsmėmis[8]. Ji taip pat papildo ir turėtų nuosekliai atitikti Tarybos rekomendaciją (ES) 2024/4371 dėl plano koordinuoti reagavimą Sąjungos lygmeniu į didelę tarpvalstybinę reikšmę turinčius ypatingos svarbos infrastruktūros sutrikimus[9] (ES ypatingos svarbos infrastruktūros planas), kuri apima fizinį (ne kibernetinį) atsparumą ir kuria siekiama gerinti reagavimo Sąjungos lygmeniu šioje srityje koordinavimą;

---

5 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. 924–947.

6 Tarybos išvados dėl bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos (dok. 9916/17).

7 Tarybos išvados dėl pagrindo koordinuotam ES atsakui į hibridines kampanijas, 2022 m. birželio 22 d.

8 Bendras tarnybų darbinis dokumentas „ES protokolas dėl kovos su hibridinėmis grėsmėmis“ (SWD(2023) 116 final).

9 OL C, C/2024/4371, 2024 7 5.

(10) Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (EU-CyCLONe) yra didelio masto kibernetinio saugumo incidentų ir krizių valdymo koordinavimo operatyviniu lygmeniu, be kita ko, tarpsektorinių didelio masto kibernetinio saugumo incidentų ir kibernetinių krizių atveju, tinklas. Siekiant toliau nekomplikuoti esamų sistemų, reikėtų vengti kurti sektorines struktūras, kurios dubliuotų EU-CyCLONe užduotis. EU-CyCLONe taip pat turėtų gauti su kibernetiniu saugumu susijusią operatyvinę informaciją iš sektorių ir prisidėti politiniu lygmeniu;

(11) valstybės narės raginamos visapusiškai naudotis pagal atitinkamas Sąjungos programas kibernetinio saugumo sričiai numatytais finansiniais ištekliais. Reikėtų užtikrinti, kad šiomis programomis būtų užkraunama kuo mažesnė administracinė našta paraiškų dėl finansavimo teikėjams, o valstybių narių dalyvavimas šiose programose būtų palengvintas teikiant atitinkamas gaires dėl įmanomų finansinės paramos galimybių;

(12) šia rekomendacija prisidedama prie platesnio masto pasirengimo veiksmų, kurių Sąjungai reikia imtis kilus tarpsektorinėms krizėms, laikantis ES pasirengimo krizėms strategijoje įtvirtintų principų, t. y. integruoto visus pavojus, visus valdžios lygmenis ir visą visuomenę apimančio požiūrio, visų pirma kiek tai susiję su informuotumo apie riziką ir grėsmes didinimu ir tarpsektoriniu reagavimu į krizes,

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

I. ES kibernetinių krizių valdymo sistemos tikslas, taikymo sritis ir pagrindiniai principai

Tikslas ir taikymo sritis

1) Šioje rekomendacijoje dėl ES kibernetinių krizių valdymo plano (toliau – Kibernetinio saugumo planas) nustatoma Sąjungos kibernetinių krizių valdymo sistema bendros ES parengties didelio masto kibernetinio saugumo incidentams ir kibernetinėms krizėms kontekste. Ši sistema atspindi tiek valstybių narių, tiek Sąjungos institucijų, įstaigų, organų ir agentūrų (toliau – Sąjungos subjektai) vaidmenis pagal jų atitinkamą kompetenciją, visapusiškai laikantis nacionalinės teisės aktų ir vidaus taisyklių, siekiant užtikrinti visapusiškus ir suderintus veiksmus Sąjungos lygmeniu.

2) Kibernetinio saugumo planas turėtų būti taikomas taip, kad derėtų su ES ypatingos svarbos infrastruktūros planu, visų pirma incidentų, darančių poveikį ir fiziniam ypatingos svarbos infrastruktūros atsparumui, ir kibernetiniam jos saugumui, atveju[10].

3) Kibernetinio saugumo plane pateikiamos reagavimo į didelio masto kibernetinio saugumo incidentus ar kibernetines krizes gairės ir jis turėtų būti taikomas kartu su atitinkamais sektorių reagavimo mechanizmais, tokiais kaip išvardytieji II priede. Atitinkami kibernetinio saugumo srities suinteresuotieji subjektai turėtų padėti siekti tų sektorių mechanizmų tikslų tiek nacionaliniu, tiek Sąjungos lygmenimis.

4) Kilus kibernetinių aspektų turinčiai ES masto tarpsektorinei krizei, dėl kurios aktyvuotas IPCR, reagavimo veiksmus Sąjungos politiniu lygmeniu turėtų koordinuoti Taryba, taikydama IPCR mechanizmą. Aktyvavus IPCR, priemonėmis pagal Kibernetinio saugumo planą turėtų būti remiamas ES atsakas politiniu lygmeniu, teikiant konkrečią paramą kibernetinio saugumo srityje.

---

10 Koordinavimas tokiais atvejais išsamiau numatytas ES ypatingos svarbos infrastruktūros plano priedo I dalies 4 skirsnyje.

Pagrindiniai principai

5) Kibernetinių krizių valdymui Sąjungos lygmeniu taikomi šie pagrindiniai principai:

a) *proporcingumas*: dauguma kibernetinio saugumo incidentų, darančių poveikį valstybėms narėms, nesiekia tokio lygio, kad galėtų būti laikomi nacionaliniu ar Sąjungos didelio masto kibernetinio saugumo incidentu arba kibernetine krize. Kibernetinio saugumo incidentų ir grėsmių atveju valstybės narės savanoriškai ir reguliariai bendradarbiauja ir keičiasi informacija Reagavimo į kompiuterių saugumo incidentus tarnybų tinkle (toliau – CSIRT tinklas) ir tinkle EU-CyCLONe, laikydamosi tinklų standartinių veiklos procedūrų (SVP);

b) *subsidiarumas*: pagrindinė atsakomybė reaguoti į kibernetinio saugumo incidentus, didelio masto kibernetinio saugumo incidentus ir kibernetines krizes ir ištaisyti jų sukeltą padėtį tenka jų paveiktoms valstybėms narėms. Atsižvelgdami į galimą tarpvalstybinį poveikį, Taryba, Komisija, vyriausiasis įgaliotinis, Europos Sąjungos kibernetinio saugumo agentūra (ENISA), Sąjungos institucijų, įstaigų, organų ir agentūrų kibernetinio saugumo tarnyba (CERT-EU), Europolas ir visi kiti atitinkami Sąjungos subjektai turėtų bendradarbiauti per visą krizės ciklą. Šis vaidmuo kyla iš Sąjungos teisės ir atspindi tai, kaip didelio masto kibernetinio saugumo incidentai ir kibernetinės krizės paveikia vieną ar daugiau ekonominės veiklos sektorių bendrojoje rinkoje, Sąjungos saugumą ir tarptautinius santykius, taip pat pačius Sąjungos subjektus;

c) *papildomumas*: šioje rekomendacijoje visapusiškai atsižvelgiama į esamus II priede išdėstytus Sąjungos lygmens krizių valdymo mechanizmus, visų pirma IPCR mechanizmą, ARGUS ir EIVT reagavimo į krizes mechanizmą. Šioje rekomendacijoje atsižvelgiama į CSIRT tinklo ir EU-CyCLONe įgaliojimus, taip pat į Reglamentą (ES, Euratomas) 2023/2841. Aktyvavus IPCR, turėtų būti tęsiamas atitinkamų tinklų, subjektų ir aktyvuotų sektorių mechanizmų darbas ir juo turėtų būti naudojamasi IPCR mechanizme vykdant politinį ir strateginį koordinavimą ir toks darbas šį koordinavimą turėtų paremti;

d) *informacijos konfidencialumas*: keičiantis informacijos šios rekomendacijos kontekste visais atvejais turėtų būti laikomasi taikytinų saugumo ir asmens duomenų apsaugos taisyklių. Prireikus turėtų būti atsižvelgiama į neoficialius informacijos neatskleidimo susitarimus, pavyzdžiui, Srauto kontrolės protokolą dėl neskelbtinos informacijos žymėjimo. Keičiantis įslaptinta informacija, nepriklausomai nuo taikomos klasifikavimo sistemos, kartu su turimomis akredituotomis priemonėmis turėtų būti taikomos esamos privalomos taisyklės ir susitarimai dėl įslaptintos informacijos tvarkymo.

6) Valstybės narės ir Sąjungos subjektai, laikydamiesi pirmiau nurodytų pagrindinių principų, turėtų stiprinti bendradarbiavimą kibernetinių krizių valdymo srityje, puoselėdami tarpusavio pasitikėjimą ir naudodamiesi esamais tinklais ir mechanizmais. Šiam bendradarbiavimui pagal Kibernetinio saugumo planą naudingas Reglamento (ES, Euratomas) 2023/2841 22 ir 23 straipsnių įgyvendinimas. Visų pirma kibernetinių krizių valdymo planu, parengtu remiantis Reglamento (ES, Euratomas) 2023/2841 23 straipsniu, be kita ko, prisidedama prie reguliaraus keitimosi atitinkama informacija tarp Sąjungos subjektų ir su valstybėmis narėmis ir nustatoma Sąjungos subjektų tarpusavio koordinavimo ir informacijos srauto tvarka.

II. Terminų apibrėžtys

7) Šiame Kibernetinio saugumo plane vartojamų terminų apibrėžtys:

a) incidentas – įvykis, kuriuo sukeliamas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui;

b) reikšmingas incidentas – incidentas:

   a. dėl kurio atitinkamas subjektas patyrė arba gali patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių;

   b. kuris paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą;

c) didelio masto kibernetinio saugumo incidentas – incidentas, kurio sukeltas sutrikimo lygis yra toks, kad viena valstybė narė nepajėgia į jį reaguoti arba kuris daro didelį poveikį ne mažiau kaip dviem valstybėms narėms;

d) kibernetinė krizė – didelio masto kibernetinio saugumo incidentas, virtęs plataus masto krize, dėl kurios vidaus rinka negali tinkamai veikti arba kyla rimtas pavojus visuomenės saugumui ir subjektų ar piliečių saugai keliose valstybėse narėse arba visoje Sąjungoje.

III. Nacionalinės kibernetinių krizių valdymo struktūros ir atsakomybės sritys

8) Pagrindinė atsakomybė reaguoti į didelio masto kibernetinio saugumo incidentus ar kibernetines krizes tenka jų paveiktoms valstybėms narėms. Kiekviena valstybė narė pagal Direktyvą (ES) 2022/2555 turi vieną ar daugiau kibernetinių krizių valdymo institucijų ir vieną ar daugiau CSIRT.

9) Priimdamos Direktyvą (ES) 2022/2555 ir kitas kibernetinio saugumo srities teisėkūros ir ne teisėkūros priemones, valstybės narės derina savo kibernetinio saugumo sistemas nustatydamos būtiniausias taisykles dėl koordinuotos reguliavimo sistemos veikimo bei veiksmingo visų valstybių narių atsakingų institucijų bendradarbiavimo mechanizmus ir numatydamos veiksmingas teisių gynimo priemones bei vykdymo užtikrinimo priemones, kurios yra labai svarbios veiksmingam tų pareigų vykdymui užtikrinti.

10) Pagal Direktyvos (ES) 2022/2555 9 straipsnio 4 dalį valstybės narės turėtų priimti nacionalinius reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planus. Šie planai, be kita ko, apima nacionalines parengties priemones, kibernetinių krizių valdymo procedūras ir nacionalines procedūras bei nacionalinių institucijų ir įstaigų susitarimus, kuriais siekiama užtikrinti veiksmingą jų dalyvavimą koordinuotai Sąjungos lygmeniu valdant didelio masto kibernetinio saugumo incidentus ir kibernetines krizes ir paramą tokiam valdymui. Kibernetinių krizių valdymo procedūros apima ir nuostatas dėl jų integravimo į bendrąją nacionalinę krizių valdymo sistemą bei keitimosi informacija kanalus.

11) Pagal Direktyvos (ES) 2022/2555 9 straipsnio 1 dalį valstybės narės turėtų užtikrinti suderinamumą su esamomis bendrosiomis nacionalinėmis krizių valdymo sistemomis. Aktyvavus IPCR, nacionalinės krizių valdymo institucijos, siekdamos informuoti IPCR, turėtų rinkti informaciją iš kibernetinių krizių valdymo institucijų ir nacionalinių sektorinių krizių valdymo mechanizmų.

12) Pagal Direktyvos (ES) 2022/2555 9 straipsnio 5 dalį EU-CyCLONe atitinkamos valstybės narės prašymu turėtų keistis informacija apie atitinkamas nacionalinių reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planų dalis, visų pirma apie nuostatas, kuriomis užtikrinamas veiksmingas dalyvavimas koordinuotai Sąjungos lygmeniu valdant didelio masto kibernetinio saugumo incidentus ir kibernetines krizes ir parama tokiam valdymui, kad būtų keičiamasi geriausios praktikos pavyzdžiais ir apsvarstyta, ar bendra sistema veiktų praktiškai.

13) EU-CyCLONe ir Tarpinstitucinė kibernetinio saugumo taryba raginami, kai tikslinga, pasikeisti informacija apie Tarpinstitucinės kibernetinio saugumo tarybos pagal Reglamento (ES, Euratomas) 2023/2841 23 straipsnį parengto krizių valdymo plano suderinamumą su nacionaliniais reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planais.

14) EU-CyCLONe, padedamas ENISA, kaip savo sekretoriato, turėtų tvarkyti nuolat atnaujinamą nacionalinių kibernetinių krizių valdymo institucijų sąrašą, kuriame būtų nurodyti EU-CyCLONe pareigūnų ir vadovų kontaktiniai duomenys, ir pateikti jį EU-CyCLONe nariams.

IV. Pagrindiniai ES kibernetinių krizių valdymo ekosistemos tinklai ir subjektai

15) CSIRT tinklas yra pagrindinis techninis tinklas, kuriame keičiamasi svarbia informacija apie incidentus, visų pirmašios rekomendacijos taikymo srityje, vykdant atitinkamas užduotis, aprašytas Direktyvos (ES) 2022/2555 15 straipsnio 3 dalyje. Jis prisideda prie pasitikėjimo didinimo ir skatina greitą ir veiksmingą valstybių narių operatyvinį bendradarbiavimą. CSIRT tinklo pirmininkas gali dalyvauti Tarpinstitucinės kibernetinio saugumo tarybos veikloje stebėtojo teisėmis.

16) CERT-EU yra visų Sąjungos subjektų kibernetinio saugumo tarnyba. CERT-EU veikia kaip Sąjungos subjektų keitimosi kibernetinio saugumo informacija ir reagavimo į incidentus koordinavimo centras pagal Reglamento (ES) 2023/2841 13 straipsnį. CERT-EU yra CSIRT tinklo narė ir padeda Komisijai tinkle EU-CyCLONe. CERT-EU veikia techniniu lygmeniu ir yra atsakinga už didelių incidentų, darančių poveikį Sąjungos subjektams, valdymo koordinavimą.

17) EU-CyCLONe veikia kaip techninio ir politinio lygmenų tarpininkas, visų pirma didelio masto kibernetinio saugumo incidentų ir kibernetinių krizių metu. Jis padeda koordinuotai valdyti didelio masto kibernetinio saugumo incidentus ir kibernetines krizes operatyviniu lygmeniu ir užtikrina reguliarų keitimąsi svarbia informacija tarp valstybių narių ir Sąjungos institucijų, įstaigų, organų ir agentūrų pagal Direktyvos (ES) 2022/2555 16 straipsnį. EU-CyCLONe pirmininkas gali dalyvauti Tarpinstitucinės kibernetinio saugumo tarybos veikloje stebėtojo teisėmis.

18) ENISA yra Sąjungos agentūra, atliekanti pagal Reglamentą (ES) 2019/881[11] paskirtas užduotis, siekiant užtikrinti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje, be kita ko, aktyviai remiant valstybes nares ir Sąjungos institucijas, įstaigas ir agentūras. ENISA, be kita ko, teikia sekretoriato paslaugas CSIRT tinklui ir tinklui EU-CyCLONe, teikia informuotumo apie padėtį paslaugas ir padeda valstybėms narėms reguliariai organizuodama kibernetinio saugumo pratybas Sąjungos lygmeniu. Pagal Direktyvą (ES) 2022/2555 ir Reglamentą (ES) 2024/2847[12] ENISA gauna informaciją apie reikšmingus tarpvalstybinius incidentus ir aktyviai išnaudojamus pažeidžiamumus bei incidentus, darančius poveikį skaitmeniniams produktams.

19) Europos Sąjungos Taryba (toliau – Taryba) yra institucija, kuriai pagal Europos Sąjungos sutarties (toliau – ES sutartis) 16 straipsnį suteiktos politikos formavimo ir koordinavimo funkcijos ir kuriai patikėtas IPCR, susijęs su koordinavimu ir atsaku Sąjungos politiniu lygmeniu. Taryba veikia per įvairių sudėčių Tarybą, Nuolatinių atstovų komitetą ir atitinkamus Tarybos parengiamuosius organus, visų pirma Kibernetinių klausimų horizontaliąją darbo grupę, taip pat, kai aktualu, IPCR mechanizmą.

---

11 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013, (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15–69).

12 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828, (Kibernetinio atsparumo aktas) (OL L, 2024/2847, 2024 11 20, p. 1–81.

20) Komisija, kaip institucija, propaguojanti bendruosius Sąjungos interesus ir tuo tikslu besiimanti tinkamų iniciatyvų, taip pat užtikrinanti Sutarčių ir institucijų pagal ES sutarties 17 straipsnį patvirtintų priemonių taikymą, yra atsakinga už tam tikrus bendrus Sąjungos lygmens pasirengimo veiksmus ir tam tikrus informuotumo apie padėtį veiksmus, įskaitant RNKC ir Bendros ekstremalių situacijų ryšių ir informacijos sistemos (CECIS) administravimą, laikantis sprendimo dėl SCSM. Ji palengvina susijusių Sąjungos lygmens reagavimo į krizes veiksmų nuoseklumą ir koordinavimą operatyviniu lygmeniu. Su ja konsultuojamasi dėl sprendimų aktyvuoti arba deaktyvuoti IPCR mechanizmą. Komisijos tarnybos kartu su EIVT rengia ISAA ataskaitas. Tais atvejais, kai potencialus arba vykstantis didelio masto kibernetinio saugumo incidentas daro arba gali daryti didelį poveikį paslaugoms ir veiklai, patenkančioms į Direktyvos (ES) 2022/2555 taikymo sritį, Komisija yra EU-CyCLONe narė, o kitais atvejais – stebėtoja. Ji yra Tarpinstitucinės kibernetinio saugumo tarybos kontaktinis punktas tinkle EU-CyCLONe. Ji dalyvauja CSIRT tinkle kaip stebėtoja.

21) Vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai (toliau – vyriausiasis įgaliotinis), padedamas EIVT, vykdo Sąjungos bendrą užsienio ir saugumo politiką (toliau – BUSP) ir savo pasiūlymais prisideda prie tos politikos, įskaitant bendrą saugumo ir gynybos politiką (toliau – BSGP), plėtojimo. Tai apima diplomatines, žvalgybos ir karines struktūras ir mechanizmus, visų pirma Bendrą žvalgybinės informacijos analizės centrą (toliau – SIAC), kuris veikia kaip viena bendra prieiga valstybių narių žvalgybinei informacijai teikti, ES karinį štabą (toliau – EUMS), kaip karinių ekspertinių žinių šaltinį, ES kibernetinio saugumo diplomatijos priemonių rinkinį, taip pat ES delegacijų tinklą, kurie gali prisidėti prie krizių valdymo išorės aspektu. EIVT kartu su Komisija taip pat rengia ISAA ataskaitas.

22) II priede aprašomi atitinkamų Sąjungos lygmens subjektų, įskaitant pagrindinius tinklus ir subjektus, vaidmenys ir kompetencija, susiję su kibernetinių krizių valdymu.

V. Pasirengimas didelio masto kibernetinio saugumo incidentams ir kibernetinei krizei

Grėsmių panorama

23) Valstybės narės ir atitinkami Sąjungos subjektai turėtų imtis būtinų priemonių informuotumui apie padėtį didinti ir pripažinti, kad atsižvelgiant į grėsmių panoramą ir siekiant užtikrinti informuotumą apie padėtį konkrečių incidentų atžvilgiu reikalingi skirtingi veikimo būdai. Valstybės narės ir atitinkami Sąjungos subjektai turėtų bendradarbiauti remdamiesi patikrintais ir patikimais duomenimis, įskaitant duomenis apie incidentų tendencijas, taktiką, metodus ir procedūras, taip pat aktyviai išnaudojamus pažeidžiamumus.

24) Dalydamosi informacija ES lygmeniu valstybės narės turėtų visapusiškai naudotis esamomis techninio ir operatyvinio bendradarbiavimo platformomis, kaip antai tomis, kuriomis naudojasi CSIRT tinklas ir EU-CyCLONe.

25) Siekiant didinti bendrą informuotumą apie padėtį ir palengvinti ES poveikio vertinimą, EU-CyCLONe ir CSIRT tinklas, padedami ENISA, turėtų naudotis viduje sutartu ataskaitų teikimo mechanizmu, kad parengtų techninės ir operatyvinės veiklos ES apžvalgą, grindžiamą nacionaliniu lygmeniu surinkta informacija.

26) EU-CyCLONe ir CSIRT tinklas turėtų:

a) bendradarbiauti tobulinant dalijimąsi informacija tarp techninio ir operatyvinio lygmenų ir gerinant informuotumą apie padėtį apskritai;

b) toliau kurti tarpusavio pasitikėjimo atmosferą tarp savo narių ir tarp tinklų;

c) visapusiškai pasinaudoti turimomis dalijimosi informacija priemonėmis, padedant ENISA, ir apsvarstyti, kaip patobulinti šias priemones ir užtikrinti tinklų sąveikumą.

27) EU-CyCLONe, CSIRT tinklas ir Tarpinstitucinė kibernetinio saugumo taryba turėtų bendradarbiauti, kad užtikrintų veiksmingą keitimąsi atitinkama informacija.

28) ENISA, kaip CSIRT tinklo ir EU-CyCLONe sekretoriatas, atlieka vieną iš pagrindinių vaidmenų remiant valstybes nares ir Sąjungos institucijas, įstaigas ir agentūras, kad būtų užtikrintas bendras ES informuotumas apie padėtį techniniu ir operatyviniu lygmenimis, siekiant padėti pasirengti didelio masto kibernetinio saugumo incidentams ir krizėms.

29) Pagal Direktyvą (ES) 2022/2555 ir Reglamentą (ES) 2019/881 valstybės narės ir atitinkami Sąjungos subjektai turėtų koordinuoti veiksmus su privačiuoju sektoriumi, įskaitant atvirojo kodo bendruomenes ir gamintojus, kad būtų pagerintas dalijimasis informacija. Visų pirma ENISA šiuo tikslu turėtų pasinaudoti savo partnerystės programa. Be to, valstybės narės ir atitinkami Sąjungos subjektai taip pat galėtų remtis esamais ES ir nacionalinio lygmenų keitimosi informacija ir jos analizės centrais (ISAC), kad padidintų kibernetinio saugumo pajėgumus ir reaguotų į kibernetinio saugumo incidentus, be kita ko, rengdami bendrus privačiojo sektoriaus susitikimus su EU-CyCLONe arba CSIRT tinklu.

30) Siekiant pagerinti dalijimąsi informacija tinkluose ir tarp jų ir išsiaiškinti bendrus tokio dalijimosi lūkesčius, EU-CyCLONe, padedamas ENISA kaip sekretoriato ir pasikonsultavęs su CSIRT tinklu bei TIS bendradarbiavimo grupe, per 24 mėnesius nuo šios rekomendacijos priėmimo turėtų susitarti dėl bendros suderintos incidentų sunkumo lygių taksonomijos. Ši taksonomija turėtų sudaryti sąlygas palyginti incidentų sunkumo lygius visose valstybėse narėse, atsižvelgiant į poveikį paslaugų teikimui, paveiktų subjektų skaičių ir atitinkamą jų svarbą, poveikį kitoms paslaugoms ir infrastruktūrai, taip pat padarytą piniginę žalą, žalą reputacijai ir politinę žalą. Ji turėtų būti grindžiama atitinkamomis esamomis skalėmis arba taksonomijomis, pavyzdžiui, orientacine incidentų klasifikavimo taksonomija.

Techninis lygmuo

31) CSIRT tinklas yra techninio bendradarbiavimo ir dalijimosi informacija tarp visų valstybių narių ir (per CERT-EU) su Sąjungos subjektais platforma.

32) Pagal Direktyvą (ES) 2022/2555 kiekvienos CSIRT užduotis yra stebėti ir analizuoti kibernetines grėsmes, pažeidžiamumus ir incidentus nacionaliniu lygmeniu. CSIRT turėtų keistis atitinkama informacija tiek CSIRT tinkle, tiek dvišaliu pagrindu apie incidentus, vos neįvykusius incidentus, kibernetines grėsmes, riziką ir pažeidžiamumus, kad būtų užtikrintas bendras informuotumas apie padėtį.

33) Siekdamas intensyvinti operatyvinį bendradarbiavimą Sąjungos lygmeniu, CSIRT tinklas turėtų apsvarstyti galimybę pakviesti savo darbe dalyvauti kibernetinio saugumo politikos srityje veikiančias Sąjungos įstaigas ir agentūras, pavyzdžiui, Europolą.

34) Pagal Reglamentą (ES) 2023/2841 CERT-EU turėtų rinkti, valdyti, analizuoti ir dalytis su Sąjungos institucijomis, įstaigomis, organais ir agentūromis informacija apie kibernetines grėsmes, pažeidžiamumus ir incidentus neįslaptintoje IRT infrastruktūroje ir prireikus teikti konkrečius pasiūlymus Tarpinstitucinei kibernetinio saugumo tarybai dėl gairių ir rekomendacijų Sąjungos institucijoms, įstaigoms, organams ir agentūroms. CERT-EU turėtų bendradarbiauti ir keistis informacija su lygiavertėmis valstybių narių tarnybomis, be kita ko, per CSIRT tinklą.

Operatyvinis lygmuo

35) Pagal Direktyvą (ES) 2022/2555 EU- CyCLONe turėtų būti valstybių narių kibernetinių krizių valdymo institucijų bendradarbiavimo ir bendradarbiavimo (per Komisiją) su atitinkamais Sąjungos subjektais platforma, kurios tikslas – didinti parengties valdyti didelio masto kibernetinio saugumo incidentus ir kibernetines krizes lygį ir plėtoti bendrą informuotumą apie padėtį didelio masto kibernetinio saugumo incidentų ir kibernetinių krizių atvejais.

36) Pagal Direktyvą (ES) 2022/2555 ir Reglamentą (ES) 2024/2847 ENISA gauna informaciją apie reikšmingus tarpvalstybinius incidentus ir aktyviai išnaudojamus pažeidžiamumus bei incidentus, darančius poveikį skaitmeniniams produktams. ENISA, veikdama kaip sekretoriatas, turėtų patarti CSIRT tinklui ir EU-CyCLONe, kad padėtų šiems tinklams nustatyti, ar reikėtų imtis tolesnių veiksmų, ir prisidėti prie bendro informuotumo apie padėtį.

Politinis lygmuo

37) Valstybės narės ir atitinkami Sąjungos subjektai turėtų stebėti tarptautinius pokyčius, darančius poveikį kibernetiniam saugumui (įskaitant kibernetines grėsmes, hibridines grėsmes ir užsienio vykdomą manipuliavimą informacija ir kišimąsi (FIMI), įskaitant, kai aktualu, dezinformaciją). Reikėtų atsižvelgti į tokias iniciatyvas kaip bendros kibernetinio saugumo vertinimo ataskaitos (JCAR), SIAC pateiktas analizes ir kitus atitinkamus produktus, kuriuose pateikiamos specializuotos įžvalgos.

38) Vyriausiasis įgaliotinis turėtų toliau informuoti valstybes nares ir jas įtraukti į Sąjungos diplomatines pastangas, susijusias su kibernetinėmis grėsmėmis, ypač tas, kuriose dalyvauja valstybiniai subjektai, jo bendradarbiavimu su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis, įskaitant NATO, ir diplomatinių priemonių, įskaitant ribojamąsias priemones, įgyvendinimu.

39) Europos Sąjungos Tarybai pirmininkaujanti valstybė narė IPCR interneto platformoje gali pasiūlyti naudoti stebėsenos puslapį, kuriame valstybės narės ir ES institucijos bei įstaigos galėtų keistis informacija apie galimą kylančią krizę.

Bendros pratybos

40) Komisija, koordinuodama veiksmus su vyriausiuoju įgaliotiniu, padedama ENISA, pasikonsultavusi su EU-CyCLONe ir CSIRT tinklu, turėtų parengti veiksmingą metinę tęstinę kibernetinio saugumo pratybų programą, kad būtų pasirengta kibernetinėms krizėms ir padidintas organizacinis veiksmingumas. Tęstinėje kibernetinio saugumo pratybų programoje turėtų būti atsižvelgiama į SCSM pratybas ir kitas Sąjungos lygmens reagavimo į krizes mechanizmų pratybas, įskaitant ES ypatingos svarbos infrastruktūros plane išdėstytas pratybas. Pirmoji tęstinė programa turėtų būti parengta per 12 mėnesių nuo Kibernetinio saugumo plano priėmimo, o vėlesnės programos turi būti užbaigtos iki kiekvienų metų kovo 31 d. Tęstinė programa turėtų būti pateikta Tarybai susipažinti.

41) Tęstinė programa taip pat turėtų apimti pratybas, parengtas pagal ES koordinuotų rizikos vertinimų scenarijus. Ji turėtų apimti pratybas, kuriose dalyvautų visi susiję subjektai, visų pirma privatusis sektorius ir NATO.

42) ENISA, atlikdama CSIRT tinklo ir EU-CyCLONe sekretoriato vaidmenį, turėtų užtikrinti, kad būtų sistemingai renkami per pratybas įgytos patirties pavyzdžiai, taip pat nustatomi tolesni veiksmai ir siūlomi jų įgyvendinimo būdai, kad būtų užtikrintas veiksmingas jų vykdymas ir teigiamas poveikis ES bendram atsparumui, įskaitant atitinkamas standartines veiklos procedūras (SVP).

43) Visi subjektai ir tinklai turėtų gerinti koordinavimą didelio masto kibernetinio saugumo incidento arba kibernetinės krizės atveju, remdamiesi per pratybas įgyta patirtimi. Visų pirma EU-CyCLONe ir CSIRT tinklas, siekdami pagerinti koordinavimą, turėtų spręsti per pratybas nustatytus sunkumus, visų pirma susijusius su tinklų bendradarbiavimu, ir prireikus greitai pritaikyti SVP.

44) TIS bendradarbiavimo grupė turėtų pakviesti CSIRT tinklą, EU-CyCLONe ir ENISA pristatyti per pratybas įgytą patirtį, taip pat nustatyti tolesnius veiksmus ir pasiūlyti jų įgyvendinimo būdus.

45) Taryba gali pakviesti CSIRT tinklo, EU-CyCLONe, TIS bendradarbiavimo grupės ir ENISA pirmininkus pristatyti, kaip buvo įgyvendinta per pratybas įgyta patirtis.

46) ENISA, bendradarbiaudama su Komisija ir vyriausiuoju įgaliotiniu, raginama surengti pratybas, skirtas kibernetinio saugumo planui išbandyti per kitas pratybas „Cyber Europe“. Pratybose turėtų dalyvauti visi susiję, be kita ko, politinio lygmens, subjektai. ENISA prašoma koordinuoti politinio lygmens dalyvavimą su Europos Sąjungos Tarybai pirmininkaujančia valstybe nare. Pratybose taip pat gali dalyvauti privatusis sektorius ir NATO.

VI. Incidento, kuris galėtų virsti didelio masto kibernetinio saugumo incidentu arba kibernetine krize, aptikimas

47) Visi subjektai, laikydamiesi savo atitinkamų įgaliojimų ir vadovaudamiesi visus pavojus apimančiu požiūriu, turėtų atitinkamiems tinklams teikti informaciją, rodančią galimą didelio masto kibernetinio saugumo incidentą arba kibernetinę krizę.

48) Pagal Reglamentą (ES) 2025/38[13], kai tarpvalstybiniai kibernetinio saugumo centrai gauna informacijos, susijusios su potencialiu arba vykstančiu didelio masto kibernetinio saugumo incidentu, jie bendro informuotumo apie padėtį tikslais turėtų užtikrinti, kad per EU-CyCLONe ir CSIRT tinklą valstybių narių institucijoms ir Komisijai būtų nepagrįstai nedelsiant teikiama svarbi informacija.

[13] 2024 m. gruodžio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2025/38, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694, (Kibernetinio solidarumo aktas) (OL L, 2025/38, 2025 1 15, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

49) Reikšmingo incidento, kuris visų pirma sukelia tiesioginį poveikį, atveju apie jį gali būti pranešama CSIRT, taip pat valstybių narių kibernetinių krizių valdymo institucijoms ar kitoms sektorių institucijoms arba šios institucijos gali jį aptikti. Valstybės narės raginamos dalytis su tokiu incidentu susijusia informacija tinkluose, kurie turėtų apsvarstyti galimybę imtis tinkamų veiksmų. CSIRT tinklas ir EU-CyCLONe gali būti aktyvuoti nepriklausomai vienas nuo kito, atsižvelgiant į incidento pobūdį ir būtiną atsaką. Tačiau abu tinklai raginami tęsti tarpusavio bendradarbiavimą remiantis sutarta procedūrine tvarka. Sprendimą dėl aktyvavimo nepriklausomai priima tik kiekvienas atitinkamas tinklas.

50) CSIRT tinklas turėtų konsultuoti EU-CyCLONe dėl to, ar stebimas kibernetinio saugumo incidentas laikytinas potencialiu arba vykstančiu didelio masto kibernetinio saugumo incidentu.

51) Kaip nurodyta Direktyvoje (ES) 2022/2555, CSIRT tinklas ir EU-CyCLONe turėtų nedelsdami susitarti dėl procedūrinės tvarkos, taikytinos potencialaus arba vykstančio didelio masto kibernetinio saugumo incidento atveju, kad būtų užtikrintas techninis ir operatyvinis koordinavimas ir būtų laiku teikiama aktuali informacija politiniu lygmeniu.

VII. Reagavimas į didelio masto kibernetinio saugumo incidentą arba kibernetinę krizę Sąjungos lygmeniu

Reagavimas į didelio masto kibernetinio saugumo incidentą arba kibernetinę krizę, kai IPCR nėra aktyvuotas visa apimtimi

52) Veiksmingas reagavimas į didelio masto kibernetinio saugumo incidentus arba kibernetines krizes ES lygmeniu priklauso nuo veiksmingo techninio, operatyvinio ir politinio bendradarbiavimo taikant požiūrį, pagal kurį imamasi veiksmų visais valdžios lygmenimis, įskaitant, kai įmanoma, teisėsaugą.

53) Kalbant apie kiekvieną lygmenį, dalyvaujantys subjektai turėtų vykdyti konkrečią veiklą, kad būtų užtikrintas bendras informuotumas apie padėtį ir koordinuotas atsakas. Tokiomis priemonėmis užtikrinama, kad informacija būtų platinama tvarkingai ir veiksmingai.

54) Atsakas turėtų būti tinkamas atsižvelgiant į didelio masto kibernetinio saugumo incidento arba kibernetinės krizės poveikį. Pagal Direktyvą (ES) 2022/2555 valstybių narių kibernetinių krizių valdymo institucijos turėtų užtikrinti sektorių atsako į kibernetinę krizę nuoseklumą ir koordinavimą nacionaliniu lygmeniu.

55) Didelio masto kibernetinio saugumo incidento arba kibernetinės krizės atveju visi subjektai ir tinklai turėtų reaguoti aktyviai koordinuodami veiksmus, kaip nurodyta toliau:

a) techniniu lygmeniu:

i. paveiktos valstybės narės ir jų CSIRT turėtų bendradarbiauti su paveiktais subjektais, kad reaguotų į incidentus ir, kai taikytina, teiktų pagalbą;

ii. CSIRT turėtų bendradarbiauti per CSIRT tinklą, kad dalytųsi atitinkama techninė informacija apie incidentą; CSIRT bendradarbiauja analizuodamos turimus techninius artefaktus ir kitą su incidentu susijusią techninę informaciją, kad nustatytų priežastį ir galimas techninės padarinių mažinimo priemones;

iii. kai CSIRT arba valstybės narės kibernetinių krizių valdymo institucija sužino apie didelį incidentą, jos raginamos dalytis informacija CSIRT tinkle arba tinkle EU-CyCLONe;

iv. CSIRT tinklas, padedamas ENISA, turėtų parengti CSIRT teikiamų nacionalinių ataskaitų suvestinę ir ji turėtų būti pateikta tinklui EU-CyCLONe;

v. kai kibernetinio saugumo incidentas gali virsti didelio masto kibernetinio saugumo incidentu arba kibernetine krize, CSIRT tinklas turėtų dalytis atitinkama informacija su EU-CyCLONe; EU-CyCLONe, naudodamasis šia informacija, turėtų informuoti Tarybą;

vi. CSIRT tinklas turėtų palaikyti glaudžius ryšius su Europolu, kad būtų užtikrintas keitimasis atitinkama techninė informacija. CSIRT tinklas ir Europolas turėtų įsteigti kontaktinius punktus, kad, kai aktualu, didelio masto kibernetinio saugumo incidento atveju būtų aktyviau dalijamasi informacija;

b) operatyviniu lygmeniu:

i. valstybės narės turėtų mažinti incidento poveikį nacionaliniu lygmeniu taikydamos tinkamas priemones;

ii. CSIRT tinklas turėtų tinklui EU-CyCLONe teikti vykstančių incidentų techninius vertinimus, o pastarasis turėtų galėti jais naudotis;

iii. EU-CyCLONe turėtų įvertinti atitinkamų didelio masto kibernetinio saugumo incidentų ir kibernetinių krizių padarinius ir poveikį, pasiūlyti galimas mažinimo priemones ir remti koordinuotą didelio masto kibernetinio saugumo incidentų ir kibernetinių krizių valdymą, taip pat remti sprendimų priėmimą politiniu lygmeniu;

iv. jei dėl didelio masto kibernetinio saugumo incidento, turinčio tarpsektorinį poveikį, reikėtų imtis Sąjungos lygmens reagavimo veiksmų, visų pirma atitinkamų II priede išvardytų Sąjungos lygmens horizontaliųjų ir sektorinių krizių valdymo mechanizmų,

(a) atitinkami subjektai, priklausomai nuo Sąjungos lygmens sektorinių krizių valdymo mechanizmų rūšies, gali pareikalauti aktyvuoti tokį mechanizmą;

(b) tokio sektorinio mechanizmo aktyvavimo atveju atitinkami subjektai padeda sektoriaus subjektams mažinti incidento poveikį;

(c) Komisija turėtų palengvinti būtinos informacijos srautą tarp II priede išvardytų atitinkamų horizontaliųjų bei sektorinių Sąjungos lygmens krizių valdymo mechanizmų kontaktinių punktų ir EU-CyCLONe ir atlikti integruotą tarpsektorinę analizę bei pasiūlyti tinkamo integruoto atsako plano galimybes;

(d) Komisija per EU-CyCLONe, kai aktualu, bendradarbiaudama su vyriausiuoju įgaliotiniu, turėtų užtikrinti ES lygmens operatyvinių priemonių kibernetinėje srityje suderinamumą ir koordinavimą su susijusiais Sąjungos lygmens reagavimo veiksmais, visų pirma, kiek tai susiję su pagalbos prašymais pagal SCSM;

(e) jei inicijuotas IPCR stebėsenos puslapis, per IPCR interneto platformą tarp valstybių narių ir Sąjungos subjektų taip pat turėtų dalijamasi informacija apie incidentą, jo poveikį ir priemones, kurių imtasi;

v. valstybės narės pagal Reglamento (ES) 2025/38 15 straipsnį gali prašyti ES kibernetinio saugumo rezervo paslaugų. Nedarant poveikio jokiems būsimiems įgyvendinimo aktams pagal tą reglamentą, ES kibernetinio saugumo rezervo paslaugos turėtų būti suteiktos per 24 valandas nuo prašymo pateikimo;

c) politiniu lygmeniu:

i. Taryba gali prašyti, kad pagrindiniai suinteresuotieji subjektai, visų pirma Komisija, vyriausiasis įgaliotinis ir EU-CyCLONe, teiktų informacinius pranešimus, kad būtų galima imtis tinkamo politinio ir strateginio atsako;

ii. Taryba, remiama Komisijos ir vyriausiojo įgaliotinio, galėtų nuspręsti dėl tinkamų reagavimo į didelio masto kibernetinio saugumo incidentą priemonių, įskaitant galimą diplomatinį atsaką pagal IX skyrių;

iii. valstybės narės, atsižvelgdamos į incidento pobūdį ir poveikį, gali aktyvuoti papildomus kibernetinių krizių valdymo mechanizmus ar priemones;

iv. kai IPCR aktyvuojamas keitimosi informacija režimu, pasitelkiami ISAA rėmimo pajėgumai, tad intensyviau keičiamasi informacija per IPCR interneto platformą ir užtikrinama bendra padėties apžvalga. EU-CyCLONe ir CSIRT tinklo teikiamos padėties ataskaitos ir toliau turėtų būti pagrindinės priemonės, kuriomis užtikrinamas bendras informuotumas apie padėtį atitinkamai operatyviniu ir techniniu lygmenimis. Šiomis ataskaitomis gali būti remiamasi rengiant ISAA ataskaitas;

v. incidento, dėl kurio reikia imtis Sąjungos lygmens reagavimo veiksmų, visų pirma aktyvuoti atitinkamus II priede išvardytus Sąjungos lygmens horizontaliuosius ir sektorinius krizių valdymo mechanizmus, atveju Taryba, bendradarbiaudama su Komisija ir vyriausiuoju įgaliotiniu, turėtų užtikrinti reagavimo į kibernetinę krizę ir susijusių Sąjungos lygmens reagavimo veiksmų nuoseklumą ir koordinavimą;

vi. kai prašoma galimybės naudoti atitinkamus mechanizmus, visų pirma kibernetinio saugumo rezervo paslaugas, Komisijos tarnybos ir, kai tinkama, EIVT, taip pat atitinkami Tarybos organai, visų pirma Kibernetinių klausimų horizontalioji darbo grupė ir Atsparumo didinimo ir kovos su hibridinėmis grėsmėmis horizontalioji darbo grupė (HWP-ERCHT), turėtų atitinkamai koordinuoti priemonių rengimą ir įgyvendinimą, taip pat tinkamą sprendimų priėmimo procesą dėl papildomų priemonių, vadovaujantis hibridinių priemonių rinkiniu[14] kibernetinės kenkimo veiklos, kuri yra platesnės hibridinės kampanijos dalis, atveju.

Reagavimas į didelio masto kibernetinio saugumo incidentą arba kibernetinę krizę, kai IPCR yra aktyvuotas visa apimtimi

56) Turėtų būti įgyvendinti skirsnyje „*Reagavimas į didelio masto kibernetinio saugumo incidentą arba kibernetinę krizę, kai IPCR nėra aktyvuotas visa apimtimi“* išvardyti veiksmai.

57) Kai IPCR aktyvuojamas visa apimtimi, ISAA ataskaitos padeda užtikrinti bendrą informuotumą apie padėtį politiniu lygmeniu. EU-CyCLONe ir CSIRT tinklo teikiamos padėties ataskaitos ir toliau turėtų būti pagrindinės priemonės, kuriomis užtikrinamas bendras informuotumas apie padėtį atitinkamai operatyviniu ir techniniu lygmenimis. Šiomis ataskaitomis gali būti remiamasi rengiant ISAA ataskaitas.

58) Didelio masto kibernetinio saugumo incidento arba kibernetinės krizės, dėl kurios IPCR aktyvuojamas visa apimtimi, atveju visi subjektai turėtų glaudžiai koordinuoti veiksmus, laikydamiesi požiūrio, pagal kurį imamasi veiksmų visais valdžios lygmenimis:

a) reagavimo veiksmus Sąjungos politiniu lygmeniu koordinuoja Taryba, naudodama IPCR mechanizmą;

---

14 Hibridinių priemonių rinkinys – tai sistema, skirta koordinuotam atsakui į hibridines kampanijas, darančias poveikį ES ir jos valstybėms narėms, apimanti, pavyzdžiui, prevencines, bendradarbiavimo, stabilumo, ribojamąsias ir veiklos atkūrimo priemones, taip pat solidarumo ir savitarpio pagalbos rėmimą.

b) EU-CyCLONe, bendradarbiaudamas su CSIRT tinklu, turėtų politiniu lygmeniu teikti aiškią informaciją apie incidento poveikį, galimus padarinius ir reagavimo bei žalos ištaisymo priemones, be kita ko, prisidėdamas prie ISAA ataskaitų;

c) be ISAA pajėgumų, Europos Sąjungos Tarybai pirmininkaujanti valstybė narė sušauktų IPCR apskritojo stalo posėdžius, kad būtų sudarytos sąlygos politiniam ir strateginiam ES atsako koordinavimui, o veiksmais pagal Kibernetinio saugumo planą ir atitinkamų sektorių mechanizmų darbu būtų prisidedama prie IPCR darbo. Apskritojo stalo posėdžiuose taip pat galima nustatyti tam tikras konkrečias atsako spragas ir paraginti konkrečius ES subjektus jas pašalinti ir pranešti apie tai būsimuose apskritojo stalo posėdžiuose, kad būtų remiamas politinis ir strateginis koordinavimas IPCR;

d) Europos Sąjungos Tarybai pirmininkaujanti valstybė narė turėtų apsvarstyti galimybę pakviesti EU-CyCLONe į atitinkamus posėdžius, įskaitant apskritojo stalo posėdžius IPCR mechanizmo kontekste ir kitus atitinkamus Tarybos posėdžius;

e) valstybių narių krizių valdymo institucijos turėtų užtikrinti sektorinių atsako į kibernetinę krizę priemonių, kurias remia kibernetinių krizių valdymo institucijos, suderinamumą ir koordinavimą;

f) galimos diplomatinio atsako priemonės turėtų būti apsvarstytos ir vykdomos laikantis IX skyriaus.

VIII. Viešosios komunikacijos veikla

59) Atskiros valstybės narės gyventojų informavimas apie vykstantį didelio masto kibernetinio saugumo incidentą arba kibernetinę krizę, be kita ko, kaip informuotumo didinimo veiklos dalis, priklauso nacionalinei kompetencijai, tačiau valstybės narės, Komisija ir vyriausiasis įgaliotinis turėtų siekti kuo labiau koordinuoti savo viešąją komunikaciją. Atitinkamai gali įsitraukti IPCR neformalus informacijos apie krizes teikėjų tinklas.

60) Siekiant pasirengti didelio masto kibernetinio saugumo incidentams ir kibernetinėms krizėms, valstybių narių ir atitinkamai Komisijos ir CERT-EU prašoma keistis informacija apie savo komunikacijos veiklą EU-CyCLONe ir CSIRT tinkle, įskaitant geriausią praktiką, pavyzdžiui, rekomendacinius pranešimus ar informuotumo didinimo kampanijas. ENISA turėtų teikti priemones, kuriomis būtų remiamas toks keitimasis informacija ir užtikrinta lengva prieiga.

61) Didelio masto kibernetinio saugumo incidento arba kibernetinės krizės atveju valstybės narės raginamos EU-CyCLONe dalytis informacija apie savo viešosios komunikacijos veiklą siekiant didinti bendrą informuotumą ir koordinuoti veiksmus. EU-CyCLONe savo iniciatyva arba Tarybos prašymu gali pasidalyti su Taryba tokių metodų apžvalga.

IX. Diplomatinis atsakas ir bendradarbiavimas su strateginiais partneriais

62) Vyriausiasis įgaliotinis, glaudžiai bendradarbiaudamas su Komisija ir kitais atitinkamais Sąjungos subjektais, turėtų:

a) remti sprendimų priėmimą Taryboje, be kita ko, analizėmis, ataskaitomis ir pasiūlymais dėl galimų priemonių, kurios būtų ES kibernetinio saugumo diplomatijos priemonių rinkinio dalis, naudojimo. Taip bus sudaromos sąlygos naudotis visomis esamomis Sąjungos priemonėmis siekiant užkirsti kelią kibernetinei kenkimo veiklai, atgrasyti nuo jos ir į ją reaguoti, stiprinant Sąjungos poziciją kibernetinėje erdvėje ir skatinant tarptautinę taiką, saugumą ir stabilumą kibernetinėje erdvėje;

b) nustačius atitinkamą incidentą, palengvinti keitimąsi būtina informacija su strateginiais partneriais, įskaitant, kai aktualu, su NATO;

c) stiprinti veiksmų koordinavimą su strateginiais partneriais, įskaitant, kai aktualu, su NATO, reaguojant į nuolatinę grėsmę keliančių subjektų kibernetinę kenkimo veiklą, visų pirma naudodamasis ES kibernetinio saugumo diplomatijos priemonių rinkiniu pagal jo įgyvendinimo gaires.

63) Valstybės narės, vyriausiasis įgaliotinis, Komisija ir kiti atitinkami Sąjungos subjektai turėtų bendradarbiauti su strateginiais partneriais ir tarptautinėmis organizacijomis siekdami propaguoti gerąją praktiką ir atsakingą valstybių elgesį kibernetinėje erdvėje ir užtikrinti greitą ir koordinuotą reagavimą potencialių ar didelio masto kibernetinių incidentų atveju.

64) Europos Sąjunga ir NATO bendradarbiavimas turėtų būti vykdomas laikantis sutartų pagrindinių įtraukumo, abipusiškumo ir skaidrumo principų ir visapusiškai gerbiant savarankišką Sąjungos sprendimų priėmimą.

65) Komisija ir vyriausiasis įgaliotinis, atsižvelgdami į esamus susitarimus, pavyzdžiui, 2016 m. CERT-EU ir NATO techninį susitarimą, turėtų įsteigti kontaktinius punktus, kurie kibernetinės krizės atveju koordinuotų veiksmus su NATO, kad būtų galima keistis būtina informacija apie padėtį ir reagavimo į krizes mechanizmų naudojimą siekiant sustiprinti bendradarbiavimą ir efektyvumą reaguojant. Šiuo tikslu Sąjunga turėtų išnagrinėti būdus, kaip pagerinti dalijimąsi informacija su NATO įtraukiu, abipusiu ir nediskriminaciniu būdu, visų pirma užtikrinant saugiojo ryšio priemones, kartu atsižvelgiant į skirtingų valstybių narių dalijimosi informacija standartus.

66) Įgyvendindamos V skyriuje nurodytą tęstinę Sąjungos kibernetinio saugumo pratybų programą, Komisijos tarnybos ir EIVT turėtų apsvarstyti galimybę organizuoti pratybas darbuotojų lygmeniu kartu su NATO, kad būtų išbandytas civilinių ir karinių subjektų bendradarbiavimas didelio masto kibernetinio saugumo incidento arba kibernetinės krizės atveju, kai valstybės narės arba NATO sąjungininkės siekia reaguoti į kibernetinį išpuolį, kuris daro poveikį jų saugumui. Pratybos turėtų būti vykdomos užtikrinant įtraukumą ir nediskriminavimą, visapusiškai laikantis sutartų ES ir NATO bendradarbiavimo parametrų principų. Pratybos turėtų būti vykdomos pratybų „EU Integrated Resolve“ (lygiagrečios ir koordinuotos pratybos, PACE) kontekste. Turėtų būti imtasi visų būtinų priemonių siekiant užtikrinti visų Kibernetinio saugumo plane nurodytų subjektų dalyvavimą.

67) Konsultuojantis su Taryba, Komisija ir vyriausiuoju įgaliotiniu taip pat turėtų būti apsvarstyta galimybė surengti bendras Sąjungos lygmens kibernetinio saugumo pratybas su Vakarų Balkanų šalimis, Moldovos Respublika, Ukraina, taip pat kitais strateginiais partneriais ir bendramintėmis trečiosiomis valstybėmis.

X. Kibernetinių krizių valdymo koordinavimas su kariniais subjektais ES lygmeniu

68) Valstybės narės turėtų toliau stiprinti civilinių ir karinių kibernetinio saugumo subjektų bendradarbiavimą nacionaliniu lygmeniu.

69) EU-CyCLONe ir CSIRT tinklas turėtų nustatyti galimus bendradarbiavimo su atitinkamais ES kariniais subjektais, pavyzdžiui, ES kibernetinės gynybos vadų konferencija ir operatyviniu karinių kompiuterinių incidentų tyrimo tarnybų tinklu (MICNET), būdus ir procedūras, kad būtų galima pasinaudoti bendra karine ir civiline perspektyva, visų pirma rengiant bendrus posėdžius. EU-CyCLONe ir CSIRT tinklas turėtų informuoti Tarybą apie pažangą, padarytą vykdant tokį bendradarbiavimą.

70) Paveiktos valstybės narės prašoma informuoti EU-CyCLONe ir EIVT, jei didelio masto kibernetinio saugumo incidento arba kibernetinės krizės kontekste naudojami atitinkami nacionaliniai ar daugiašaliai kariniai reagavimo pajėgumai, o tokių reagavimo pajėgumų naudotojas ir teikėjas yra tarpusavyje susitarę dėl šios informacijos teikimo.

71) Įgyvendindami V skyriuje nurodytą tęstinę Sąjungos kibernetinio saugumo pratybų programą, Komisija ir vyriausiasis įgaliotinis turėtų apsvarstyti galimybę organizuoti bendras pratybas, kad būtų išbandytas tiek civilinių, tiek karinių kibernetinio saugumo subjektų bendradarbiavimas didelio masto kibernetinio saugumo incidento, darančio poveikį valstybėms narėms, atveju.

XI. Veiklos atkūrimas po kibernetinės krizės ir įgyta patirtis

72) Valstybės narės, atitinkami Sąjungos subjektai ir tinklai turėtų bendradarbiauti veiklos atkūrimo po kibernetinės krizės etape, kad būtų užtikrintas greitas pagrindinių funkcijų atkūrimas. Teisėsaugos bendruomenės taip pat turėtų, kai aktualu, įsitraukti į tokį bendradarbiavimą. Šiame etape itin svarbus bendradarbiavimas su privačiuoju sektoriumi, visų pirma siekiant palengvinti duomenų atkūrimą ir sistemų atkūrimą. Vykdant efektyvų suinteresuotųjų subjektų veiksmų koordinavimą pirmenybė turėtų būti teikiama sutrikimo mažinimui ir veiklos tęstinumo užtikrinimui.

73) Valstybės narės, atitinkami Sąjungos subjektai ir tinklai turėtų bendradarbiauti veiklos atkūrimo etape, remdamiesi patirtimi, įgyta ankstesnių kibernetinių krizių ar suvaldytų kibernetinio saugumo incidentų metu, taip pat incidentų ataskaitomis, visų pirma pagal Reglamentu (ES) 2025/38 nustatytą Europos kibernetinio saugumo incidentų peržiūros mechanizmą.

74) EU-CyCLONe turėtų pateikti CSIRT tinklui, TIS bendradarbiavimo grupei ir Tarybai išsamų patirties, įgytos ankstesnių kibernetinių krizių ar suvaldytų kibernetinio saugumo incidentų metu, ir geriausios praktikos pavyzdžių sąrašą. ENISA turėtų užtikrinti, kad ši įgyta patirtis būtų tinkamai atspindėta būsimoje pasirengimo veikloje ir svarstant būsimų pratybų planavimą.

XII. Saugusis ryšys

75) Remdamasi esamų saugiojo ryšio priemonių žemėlapiu[15], Komisija iki 2026 m. pabaigos turėtų pasiūlyti sąveikių saugiojo ryšio sprendimų rinkinį. Taryba, Komisija, vyriausiasis įgaliotinis, EU-CyCLONe ir CSIRT tinklas dėl šio rinkinio turėtų susitarti iki 2027 m. pabaigos. Šiems sprendimams turėtų būti naudingi veiksmai saugiojo ryšio srityje, kurių ES institucijos galėtų imtis pagal ES pasirengimo krizėms strategiją; šie sprendimai turėtų apimti visus reikiamus komunikacijos būdus (balso ryšio, duomenų perdavimo, vaizdo telekonferencijų, pranešimų siuntimo, bendradarbiavimo, dalijimosi dokumentais ir konsultavimosi). Sprendimai turėtų atitikti bendrai apibrėžtus neskelbtinos neįslaptintos informacijos apsaugos reikalavimus. Turėtų būti naudojami sprendimai, grindžiami atviru protokolu su atvirojo kodo programomis, tinkamomis tikralaikei komunikacijai, kuriuos administruoja subjektas, kuris yra ES rezidentas.

76) EU-CyCLONe ir CSIRT tinklas, keitimosi slaptumo žyma „RESTREINT UE/EU RESTRICTED“ pažymėta informacija tikslu prireikus turėtų galėti naudotis saugiojo ryšio kanalais, kurie užtikrinami ES institucijoms, įstaigoms ir agentūroms tarpusavyje ir su valstybėmis narėmis keičiantis įslaptinta informacija.

[15] Dok. WK 862/2023.

77) Nedarant poveikio būsimai daugiametei finansinei programai, Reglamentu (ES) 2021/887[16] įsteigtas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras (ECCC) turėtų apsvarstyti galimybę finansavimu pagal Skaitmeninės Europos programą padėti valstybėms narėms diegti saugiojo ryšio priemones. Turėtų būti vengiama investicijų į sąveikias saugias sistemas dubliavimosi.

78) Visų pirma, ES subjektai ir valstybės narės turėtų parengti nenumatytų atvejų planus dėl didelių krizių, kai sutrikdomi arba tampa neprieinami įprasti ryšio kanalai, kurių veikimas priklauso nuo interneto ar telekomunikacijų tinklų.

79) Turėtų būti sukurti teisėsaugos ir kibernetinio saugumo tinklų ryšio ir keitimosi informacija mechanizmai, visų pirma techniniu lygmeniu, kad būtų galima veiksmingai reaguoti į kibernetines krizes. Šiuose mechanizmuose turėtų būti paisoma kiekvieno dalyvio vaidmens, vengiama kištis į vykdomas operacijas ir užtikrinamas atsarginis ryšys. Šiuo metu kuriama ES ypatingos svarbos ryšių sistema (EUCCS) gali būti naudinga bendram reagavimui kartu su atitinkamomis kibernetinės srities bendruomenėmis.

XIII. Baigiamosios nuostatos

80) EU-CyCLONe, bendradarbiaudamas su CSIRT tinklu ir kitais pagrindiniais ES kibernetinių krizių valdymo ekosistemos subjektais, remiamas ENISA, per vienus metus nuo šios rekomendacijos paskelbimo turėtų parengti išsamias proceso srauto diagramas, kuriose būtų nurodyti informacijos srautai tarp atitinkamų subjektų, sprendimų priėmimo procesai ir ataskaitos, rengiamos valdant didelio masto kibernetinio saugumo incidentą arba kibernetinę krizę, kaip aprašyta šioje rekomendacijoje. Srauto diagramose turėtų būti nurodyti skirtingi bendradarbiavimo būdai ir lygmenys. Prireikus jos turėtų būti atnaujinamos.

[16] 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas (OL L 202, 2021 6 8, p. 1–31).

81) Siekdama remti veiksmingą peržiūrėto Kibernetinio saugumo plano taikymą, Taryba prireikus gali parengti įgyvendinimo gairių rinkinį, remdamasi patirtimi, įgyta pagal šį planą vykdant bendras kibernetinio saugumo pratybas. Šiomis gairėmis būtų galima nurodyti, kaip įveikti pratybose nustatytus praktinius iššūkius ir pašalinti nustatytas koordinavimo, komunikacijos ir operatyvinės sąveikos spragas, taip pat sukurti trūkstamas jungiamąsias grandis.

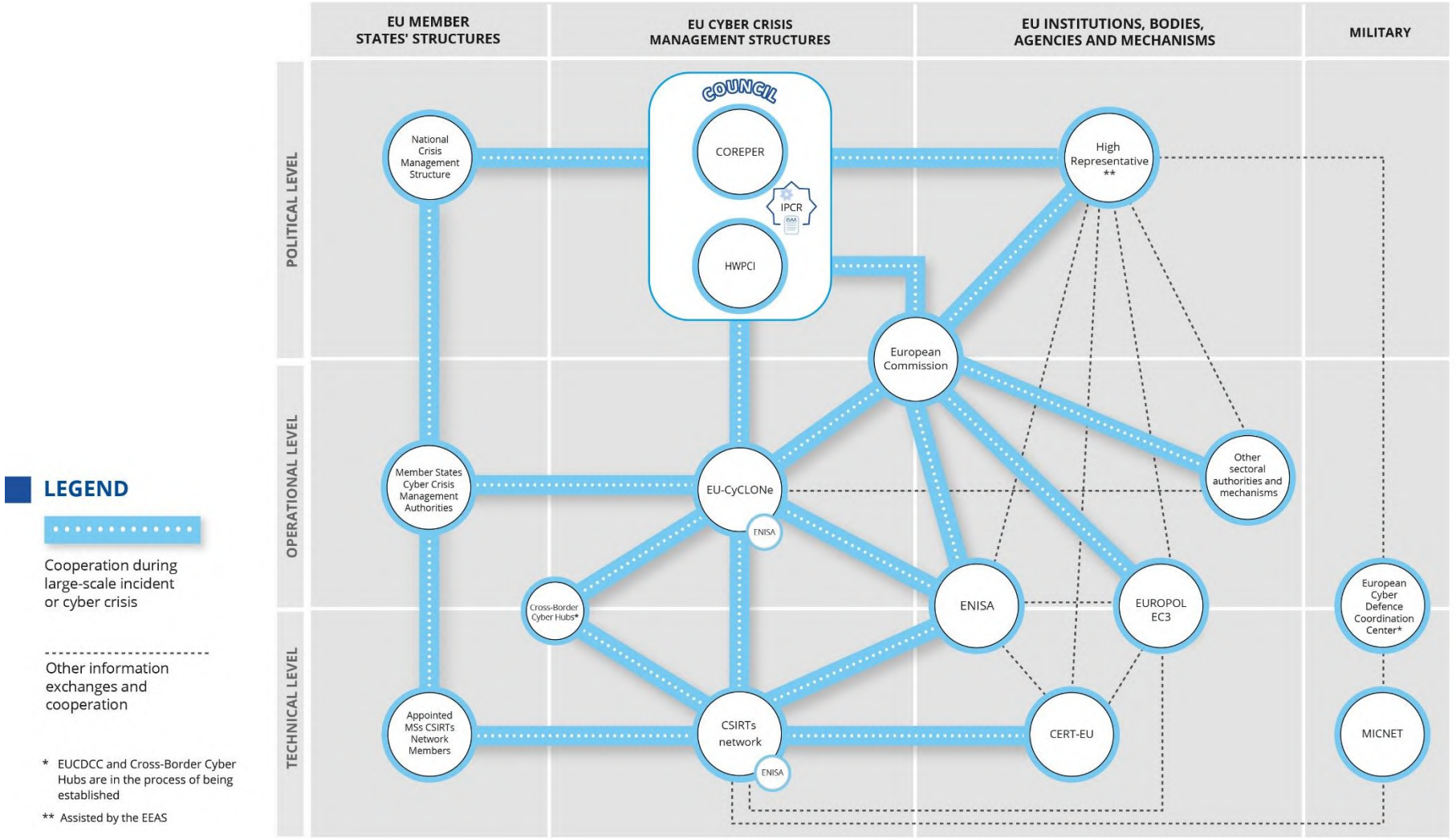
82) Komisija, bendradarbiaudama su valstybėmis narėmis, turėtų peržiūrėti šią rekomendaciją bent kas ketverius metus po jos paskelbimo. Po kiekvienos peržiūros Komisija turėtų paskelbti ataskaitą ir pateikti ją Tarybai. Komisija ir valstybės narės turėtų visų pirma atsižvelgti į kintančios grėsmių panoramos poveikį, bendrų pratybų rezultatus ir teisės aktų pakeitimus, visų pirma į visus galimus pokyčius dėl Reglamento (ES) 2019/881 peržiūros.

Priimta Briuselyje

Tarybos vardu

Pirmininkas / Pirmininkė

I PRIEDAS. Sąjungos reagavimo į kibernetinio saugumo krizę planas



II PRIEDAS. ATITINKAMI SĄJUNGOS LYGMENS VEIKĖJAI (SUBJEKTAI IR TINKLAI) IR KRIZIŲ VALDYMO MECHANIZMAI

(1) Pagrindinių veikėjų dalyvavimas visą kibernetinės krizės valdymo ciklą (didelio masto kibernetinio saugumo incidentai ir kibernetinės krizės)

	Parengtis	Aptikimas	Reagavimas į didelio masto kibernetinio saugumo incidentą arba kibernetinę krizę			Viešoji komunikacija	Veiklos atkūrimas ir įgyta patirtis
			techniniu lygmeniu	operatyviniu lygmeniu	politiniu lygmeniu		
Valstybės narės	X	X	X	X	X	X	X
Komisija	X			X	X	X	
Vyriausiasis įgaliotinis, kuriam padeda EIVT	X			X	X	X	
Taryba	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
CSIRT tinklas	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Atitinkamų Sąjungos lygmens veikėjų ir mechanizmų (išvardytų abėcėlės tvarka) vaidmenys ir kompetencija kibernetinių krizių valdymo srityje

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
CERT-EU	Techninis / operatyvinis	Koordinuoja reagavimą į krizes techniniu lygmeniu ir didelių incidentų, darančių poveikį Sąjungos subjektams, valdymą. Tvarko turimų techninių ekspertinių žinių, kurių reikėtų reaguojant į incidentus didelių incidentų atveju, aprašą ir padeda Tarpinstitucinei kibernetinio saugumo tarybai koordinuoti Sąjungos subjektų kibernetinės krizės valdymo planus didelių incidentų atvejais. CSIRT tinklo narė. Teikia Komisijai paramą tinkle EU-CyCLONe dėl koordinuoto didelio masto kibernetinio saugumo incidentų ir krizių valdymo. Veikia kaip keitimosi kibernetinio saugumo informacija ir reagavimo į incidentus koordinavimo centras, palengvinantis Sąjungos subjektų ir partnerių keitimąsi informacija apie incidentus, kibernetines	Reglamentas (ES, Euratomas) 2023/2841 Reglamentas (ES) 2025/38

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		grėsmes, pažeidžiamumus ir vos neįvykusius incidentus. Sąjungos subjektų vardu prašo naudoti ES kibernetinio saugumo rezervą. Bendradarbiauja su NATO kibernetinio saugumo centru pagal tarpusavio techninį susitarimą.	
Europos Sąjungos Taryba	Politinis	Politikos formavimo ir koordinavimo funkcijos. Jai patikėtas IPCR, susijęs su koordinavimu ir reagavimu Sąjungos politiniu lygmeniu.	Europos Sąjungos sutarties 16 straipsnis
Europos Sąjungos Tarybai pirmininkaujanti valstybė narė	Politinis	Sprendžia (išskyrus atvejus, kai pagal SESV 222 straipsnį taikoma solidarumo sąlyga), ar aktyvuoti IPCR, atitinkamai konsultuodamasi su paveiktomis valstybėmis narėmis, taip pat su Komisija ir vyriausiuoju įgaliotiniu.	Europos Sąjungos sutarties 16 straipsnis Tarybos įgyvendinimo sprendimas (ES) 2018/1993
Tarpvalstybiniai kibernetinio saugumo centrai	Techninis	Tarpvalstybinis kibernetinio saugumo centras – pagal rašytinį konsorciumo susitarimą įsteigta daugiašalė platforma, kuri į koordinuojamą tinklo struktūrą	Reglamentas (ES) 2025/38

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		sujungia bent trijų valstybių narių nacionalinius kibernetinio saugumo centrus ir kurios paskirtis – gerinti kibernetinių grėsmių stebėseną, aptikimą ir analizę siekiant užkirsti kelią incidentams ir padėti rengti kibernetinių grėsmių žvalgybos informaciją, visų pirma keičiantis svarbiais ir, kai tinkama, anonimizuotais duomenimis ir informacija, taip pat dalijantis naujausiomis priemonėmis ir bendrai plėtojant kibernetinio saugumo srityje aptikimo, analizės ir prevencijos bei apsaugos pajėgumus patikimoje aplinkoje. Glaudžiai bendradarbiauja su CSIRT tinklu dalydamiesi informacija. Per EU-CyCLONe ir CSIRT tinklą teikia valstybių narių institucijoms ir Komisijai informaciją, susijusią su potencialiu arba vykstančiu didelio masto kibernetinio saugumo incidentu.	

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
CSIRT tinklas	Techninis	Prisideda prie pasitikėjimo didinimo ir skatina greitą valstybių narių operatyvinį bendradarbiavimą. Pagrindinis tinklas, kuriame keičiamasi svarbia informacija apie incidentus, vos neįvykusius incidentus, kibernetines grėsmes, riziką ir pažeidžiamumus. Nario, kuris galėjo būti paveiktas incidento, prašymu tinkle keičiamasi informacija apie susijusį incidentą ir susijusias kibernetines grėsmes ir ji apsvarstoma. Tinklas taip pat gali palengvinti koordinuotą atsaką į incidentą, kuris buvo nustatytas prašančiojo nario jurisdikcijoje. Teikia pagalbą valstybėms narėms valdant tarpvalstybinius incidentus ir nagrinėja kitas bendradarbiavimo formas, įskaitant savitarpio pagalbą.	Direktyva (ES) 2022/2555 Reglamentas (ES) 2025/38

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		Iš valstybių narių gauna informaciją apie jų prašymus ES kibernetinio saugumo rezervui.	
Kibernetinės gynybos vadų konferencija		Forumas, kuriame dalyvauja kibernetinės gynybos vadai nacionaliniu lygmeniu valstybėse narėse, siekiant bendradarbiauti ir keistis itin svarbia informacija apie kibernetinėje erdvėje vykdomas operacijas ir didelio masto kibernetinių incidentų padarinių mažinimo strategijas. Ją organizuoja rotacijos tvarka Europos Sąjungos Tarybai pirmininkaujanti valstybė narė, padedama Europos gynybos agentūros (EGA) ir Europos išorės veiksmų tarnybos (EIVT), įskaitant ES karinį štabą (EUMS).	Bendras komunikatas dėl ES kibernetinės gynybos politikos (2022 m.)
Komisija	Operatyvinis / politinis	Europos Sąjungos vykdomoji institucija. Sklandaus vidaus rinkos veikimo užtikrinimas. Palengvina susijusių Sąjungos lygmens reagavimo į krizes	Europos Sąjungos sutarties 17 straipsnis Įgyvendinimo sprendimas (ES) 2018/1993 Sprendimas Nr. 1313/2013/ES

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		veiksmų nuoseklumą ir koordinavimą. Tam tikri bendrieji Sąjungos lygmens pasirengimo veiksmai pagal Sprendimą dėl SCSM, įskaitant Reagavimo į nelaimes koordinavimo centro ir Bendros ekstremalių situacijų ryšių ir informacijos sistemos valdymą. Tinklo EU-CyCLONe stebėtoja ir narė tais atvejais, kai potencialus arba vykstantis didelio masto incidentas daro arba gali daryti didelį poveikį paslaugoms ir veiklai, patenkančioms į Direktyvos (ES) 2022/2555 taikymo sritį. Dalyvauja CSIRTS tinkle kaip stebėtoja. Bendra atsakomybė už ES kibernetinio saugumo rezervo įgyvendinimą. Tarpinstitucinės kibernetinio saugumo tarybos kontaktinis punktas dalijantis svarbia su	Direktyva (ES) 2022/2555 Reglamentas (ES) 2025/38 Reglamentas (ES, Euratomas) 2023/2841

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		dideliais incidentais susijusia informacija su EU-CyCLONe. Konsultuoja Tarybai pirmininkaujančią valstybę narę dėl sprendimų aktyvuoti arba deaktyvuoti IPCR (išskyrus atvejus, kai pagal SESV 222 straipsnį remiamasi solidarumo sąlyga). Komisijos tarnybos kartu su EIVT rengia ISAA ataskaitas.	
Europos Sąjungos kibernetinio saugumo agentūra (ENISA)	Techninis / operatyvinis	Vykdo užduotis, kurių tikslas yra visoje Sąjungoje užtikrinti aukštą kibernetinio saugumo lygį, be kita ko, aktyviai padeda valstybėms narėms ir Sąjungos institucijoms. Atlieka CSIRT tinklo ir EU-CyCLONe sekretoriato funkcijas. Rengia reguliarias ES kibernetinio saugumo techninės padėties ataskaitas dėl incidentų ir kibernetinių grėsmių (kartu su EC3 ir CERT-EU, taip pat glaudžiai bendradarbiaudama su valstybėmis narėmis).	Direktyva (ES) 2022/2555 Reglamentas (ES) 2019/881 Reglamentas (ES) 2025/38 Reglamentas (ES) 2024/2847

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		Padeda rengti bendrą atsaką į didelio masto tarpvalstybinius incidentus ar krizes, daugiausia: – apibendrindama ir analizuodama pranešimus iš nacionalinių šaltinių; – užtikrindama informacijos srautą tarp techninio, operatyvinio ir politinio lygmenų; – gavusi prašymą – palengvindama incidentų valdymą; – teikdama Sąjungos subjektams paramą viešosios komunikacijos srityje; – gavusi prašymą – teikdama valstybėms narėms paramą viešosios komunikacijos srityje; – testuodama reagavimo į incidentus pajėgumus ir reguliariai organizuodama kibernetinio saugumo pratybas. Veikia kaip perkančioji organizacija, kai jai pavesta iš dalies arba visiškai valdyti ir administruoti ES kibernetinio saugumo rezervą. Kas dvejus metus Sąjungos lygmeniu organizuoja plataus masto išsamias kibernetinio saugumo pratybas su techniniais,	

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		operatyviniais ar strateginiais elementais. Kartu su atitinkama valstybe nare ir kitais suinteresuotaisiais subjektais parengia incidento peržiūros ataskaitą, kad būtų įvertintos incidento priežastys, poveikis ir padarinių mažinimas (Komisijos arba EU-CyCLONe prašymu ir pritarus atitinkamai valstybei narei). Informuoja EU-CyCLONe, jei informacija, pateikta vykdant Kibernetinio saugumo akte nustatytas ataskaitų teikimo pareigas, yra aktuali koordinuotam didelio masto kibernetinio saugumo incidentų ir krizių valdymui operatyviniu lygmeniu.	
Europos ryšių palaikymo dėl kibernetinių krizių organizacinis tinklas (EU-CyCLONe)	Operatyvinis	Remia koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą operatyviniu lygmeniu. Užtikrina reguliarų valstybių narių ir Sąjungos institucijų, organų,	Direktyva (ES) 2022/2555 Reglamentas (ES) 2025/38

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		įstaigų ir agentūrų keitimąsi aktualia informacija. Koordinuoja didelio masto kibernetinio saugumo incidentų ir krizių valdymą ir padeda politiniu lygmeniu priimti sprendimus, susijusius su tokiais incidentais ir krizėmis. Įvertina atitinkamų didelio masto kibernetinio saugumo incidentų ir krizių padarinius ir poveikį ir siūlo galimas padarinių mažinimo priemones. Atitinkamos valstybės narės prašymu aptaria nacionalinius reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planus. Kartu su ENISA ir Komisija parengia šabloną, kad būtų lengviau teikti prašymus dėl paramos iš ES kibernetinio saugumo rezervo. Iš valstybių narių gauna informaciją apie jų prašymus ES kibernetinio saugumo rezervui.	

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		Iš tarpvalstybinių kibernetinių centrų arba CSIRT tinklo gauna informaciją, susijusią su potencialiu arba vykstančiu didelio masto kibernetinio saugumo incidentu.	
Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai, padedamas Europos išorės veiksmų tarnybos	Politinis	Vadovauja Sąjungos pastangoms kovoti su išorės saugumo grėsmėmis hibridinėje ir kibernetinėje srityse ir jas koordinuoja. Atsakingas už Sąjungos kibernetinės diplomatijos ir kibernetinės gynybos priemones, kuriomis siekiama atgrasyti nuo išorės grėsmių ir į jas reaguoti, be kita ko, naudojantis Sąjungos hibridinių ir kibernetinio saugumo diplomatijos priemonių rinkiniais. Bendradarbiauja su išorės partneriais, be kita ko, dalyvaudamas BSGP veikloje. Padeda užtikrinti Sąjungos ir valstybių narių informuotumą apie padėtį ir pajėgumą reaguoti į hibridines ir kibernetines grėsmes, pavyzdžiui, per praktines pratybas, mokymą ir tinklus.	Tarybos sprendimas 2010/427/ES

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		Sprendžia Sąjungos kosmoso išteklių saugumo ir gynybinio pobūdžio klausimus, visų pirma pagal Sąjungos bendrą saugumo ir gynybos politiką (BSGP). Remia ES kibernetinės gynybos vadų konferenciją. Remia ES operatyvinį karinių kompiuterinių incidentų tyrimo tarnybų tinklą (MICNET). Konsultuoja Tarybai pirmininkaujančią valstybę narę dėl sprendimų aktyvuoti arba deaktyvuoti IPCR (išskyrus atvejus, kai pagal SESV 222 straipsnį remiamasi solidarumo sąlyga). EIVT kartu su Komisijos tarnybomis rengia ISAA ataskaitas.	
ES kibernetinės gynybos koordinavimo centras	Horizontalusis	Jo pradinis tikslas – visų pirma didinti Sąjungos ir jos valstybių narių bendrą informuotumą apie padėtį, susijusią su kenkimo veikla kibernetinėje erdvėje, visų pirma kiek tai susiję su karinėmis BSGP misijomis ir operacijomis.	Bendras komunikatas dėl ES kibernetinės gynybos politikos (2022 m.)

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
Europolas	Operatyvinis	Teikia operatyvinę ir techninę paramą valstybių narių institucijoms, kompetentingoms kibernetinių nusikaltimų prevencijos ir atgrasymo nuo jų srityje. Valstybių narių kompetentingų institucijų prašymu padeda joms reaguoti į, kaip įtariama, nusikalstamo pobūdžio kibernetinius išpuolius.	Reglamentas (ES) 2016/794, įskaitant visus pakeitimus
Tarpinstitucinė kibernetinio saugumo taryba		Parengia kibernetinių krizių valdymo planą, kuriuo siekiama operatyviniu lygmeniu remti koordinuotą didelių incidentų, darančių poveikį Sąjungos subjektams, valdymą ir prisidėti prie reguliaraus keitimosi atitinkama informacija. Koordinuoja atskirų Sąjungos subjektų kibernetinių krizių valdymo planų priėmimą. Remdamasi CERT-EU pasiūlymu, priima gaires ar rekomendacijas dėl bendradarbiavimo reaguojant į	Reglamentas (ES, Euratomas) 2023/2841

Veikėjas	Lygmuo	Vaidmuo ir kompetencija	Nuoroda
		reikšmingus incidentus, susijusius su Sąjungos subjektais.	
Operatyvinis karinių kompiuterinių incidentų tyrimo tarnybų tinklas (MICNET)	Techninis	Skatina tvirtesnį ir labiau koordinuotą atsaką į kibernetines grėsmes, darančias poveikį Sąjungos gynybos sistemoms, įskaitant sistemas, naudojamas karinėms BSGP misijoms ir operacijoms, padedant Europos gynybos agentūrai.	2022 m. Bendras komunikatas dėl kibernetinės gynybos
Bendras žvalgybinės informacijos analizės centras (SIAC)		Jį sudaro: 1) ES žvalgybos ir situacijų centras (EU INTCEN) ir 2) ES karinio štabo Žvalgybos direktorato (EUMS INT) SIAC. Teikia strateginę žvalgybos informaciją apie užsienio politiką, terorizmą bei hibridines grėsmes ir tvarko karinę žvalgybos informaciją, skirtą BSGP misijoms, ir remia Sąjungos gynybos ir krizių valdymo operacijas. Yra pavaldus vyriausiajam įgaliotiniui.	Europos Sąjungos sutarties 38 ir 42–46 straipsniai

(3) Atitinkami Sąjungos lygmens krizių valdymo mechanizmai ir platformos

Mechanizmas	Horizontalusis / sektorinis / kibernetinis	Apibūdinimas	Nuorodos
ARGUS	Horizontalusis	Komisijos koordinavimo procesas ir bendra įspėjimo sistema, kad būtų galima suderintai reaguoti kilus didelei tarpvalstybinei krizei, dėl kurios reikia imtis ES lygmens veiksmų. Priimant sprendimus dėl priemonių ir jas koordinuojant dalyvauja visos atitinkamos tarnybos ir kabinetai. Suteikia Komisijai galimybę keistis aktualia informacija apie kylančias daugiasektores krizes arba numatomas ar neišvengiamas grėsmes, dėl kurių reikia imtis Sąjungos lygmens veiksmų.	Komisijos komunikatas (2005)662
EIVT reagavimo į krizes centras (CRC)	Horizontalusis	Vieno langelio principu veikiantis EIVT centras, kurio tikslas – spręsti visus su krizėmis susijusius klausimus ir užtikrinti nuolatinius kasdien visą parą prieinamus reagavimo į krizes pajėgumus, skirtus naudoti susidarius ekstremaliosioms situacijoms, keliančioms grėsmę ES delegacijų darbuotojų saugumui, ir (arba)	Saugumo ir gynybos strateginis kelrodis – Europos Sąjungai, kuri gina savo piliečius, vertybes bei interesus ir prisideda prie tarptautinės taikos ir saugumo (2022 m. kovo 21 d.).

Mechanizmas	Horizontalusis / sektorinis / kibernetinis	Apibūdinimas	Nuorodos
		reaguojant į krizes, darančias poveikį Sąjungos piliečiams užsienyje. Jo veikloje dalyvauja saugumo, konsulinių klausimų ir informuotumo apie padėtį ekspertai, kartu pasikliaunant Sąjungos delegacijose vietoje dirbančiais atsakingais specialistais.	
Ypatingos svarbos infrastruktūros planas	Horizontalusis	Juo koordinuojamas reagavimas Sąjungos lygmeniu į didelę tarpvalstybinę reikšmę turinčius ypatingos svarbos infrastruktūros sutrikimus.	Tarybos rekomendacija C/2024/4371
Kibernetinio saugumo įspėjimo sistema	Kibernetinis	Užtikrina pažangius Sąjungos pajėgumus, kad būtų stiprinami su kibernetinėmis grėsmėmis ir incidentų Sąjungoje prevencija susiję aptikimo, analizės ir duomenų apdorojimo pajėgumai.	Reglamentas (ES) 2025/38
Kibernetinio saugumo diplomatijos priemonių rinkinys (Bendro ES diplomatinio atsako į kibernetinę	Kibernetinis	Sudaro sąlygas bendram Sąjungos diplomatiniam atsakui į kibernetinę kenkimo veiklą: prisideda prie konfliktų prevencijos, kibernetinio saugumo grėsmių mažinimo ir didesnio tarptautinių santykių stabilumo.	2017 m. birželio 19 d. Tarybos išvados Peržiūrėtos įgyvendinimo gairės, dok. 10289/23, 2023 m. birželio 8 d.

Mechanizmas	Horizontalusis / sektorinis / kibernetinis	Apibūdinimas	Nuorodos
kenkimo veiklą sistema)			
ES kibernetinio saugumo rezervas	Kibernetinis	Sutelkia kibernetinio saugumo ekspertus ir išteklius per krizes, kad būtų remiamos reagavimo pastangos valstybėse narėse, Sąjungos institucijose, organuose ar agentūrose	Reglamentas (ES) 2025/38
Tinklo kodeksas dėl konkretiems sektoriams taikomų taisyklių, susijusių su tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektais	Sektorinis	Nustato pasikartojančių kibernetinio saugumo rizikos vertinimų elektros energijos sektoriuje Sąjungos, valstybės narės, regiono ir subjekto lygmeniu procesą. Į jį įtrauktos konkrečios nuostatos dėl krizių valdymo ir bendradarbiavimo su CSIRT ir EU-CyCLONe tais atvejais, kai didelio masto kibernetinio saugumo incidentas daro poveikį kitiems sektoriams, priklausomiems nuo elektros energijos tiekimo saugumo.	Komisijos deleguotasis reglamentas (ES) 2024/1366
Hibridinių priemonių rinkinys	Horizontalusis	Į jį įtrauktos nuostatos, kuriomis siekiama užtikrinti, kad būtų apžvelgta tai, kas ES lygmeniu prieinama reagavimui į visų rūšių hibridines grėsmes, ir tos priemonės būtų koordinuotai naudojamos	Tarybos išvados dėl pagrindo koordinuotam ES atsakui į hibridines

Mechanizmas	Horizontalusis / sektorinis / kibernetinis	Apibūdinimas	Nuorodos
		užtikrinant mūsų veiksmų įvairiose srityse nuoseklumą. Hibridinių priemonių rinkinys padeda užtikrinti, kad sprendimai būtų priimami remiantis išsamiu informuotumu apie padėtį ir įgyta patirtimi.	kampanijas, 2022 m. birželio 22 d. Pagrindo koordinuotam ES atsakui į hibridines kampanijas įgyvendinimo gairės, 2022 m. gruodžio 14 d.
Greitojo reagavimo į hibridines grėsmes grupės (ES HRRT)	Horizontalusis	Kaip ES hibridinių priemonių rinkinio dalis, ES greitojo reagavimo į hibridines grėsmes grupės remiasi atitinkamų sektorių nacionaline ir ES civiline ir karine kompetencija, teikdamos konkretiems poreikiams pritaikytą tikslinę trumpalaikę pagalbą valstybėms narėms, bendros saugumo ir gynybos politikos misijoms bei operacijoms ir šalims partnerėms joms kovojant su hibridinėmis grėsmėmis ir kampanijomis.	ES greitojo reagavimo į hibridines grėsmes grupių praktinio sudarymo orientacinė sistema (2024 m. gegužės 21 d.) Veiklos gairės dėl greitojo reagavimo į hibridines grėsmes grupių dislokavimo, Nuolatinių atstovų komiteto patvirtinta 2024 m. gruodžio 4 d.

Mechanizmas	Horizontalusis / sektorinis / kibernetinis	Apibūdinimas	Nuorodos
IPCR	Horizontalusis	Remiamas greitas ir koordinuotas sprendimų priėmimas politiniu Sąjungos lygmeniu didelių ir sudėtingų krizių atveju. Sprendimą dėl šio mechanizmo aktyvavimo ir deaktyvavimo priima Tarybai pirmininkaujanti valstybė narė, konsultuodamasi (išskyrus atvejus, kai remiamasi solidarumo sąlygą) su paveiktomis valstybėmis narėmis, Komisija ir vyriausiuoju įgaliotiniu. TGS, Komisijos tarnybos ir EIVT, konsultuodamiesi su pirmininkaujančia valstybe nare, taip pat gali susitarti aktyvuoti IPCR keitimosi informacija režimu. IPCR darbas grindžiamos ISAA ataskaitomis, kurias rengia Komisijos tarnybos ir EIVT. Tokios ataskaitos grindžiamos aktualia informacija ir analize, kurią teikia valstybės narės (pvz., atitinkami nacionaliniai krizių centrai) ir atitinkamos Sąjungos agentūros ir organai.	Tarybos įgyvendinimo sprendimas (ES) 2018/1993

Mechanizmas	Horizontalusis / sektorinis / kibernetinis	Apibūdinimas	Nuorodos
ES teisėsaugos institucijų reagavimo į ekstremaliąsias situacijas protokolas	Horizontalusis	Priemonė, kuria Sąjungos teisėsaugos institucijoms padedama nedelsiant reaguoti į didelius tarpvalstybinius kibernetinius išpuolius: atliekamas greitas vertinimas, saugiai ir laiku dalijamasi ypatingos svarbos informacija ir veiksmingai koordinuojami tarptautiniai jų tyrimų aspektai.	Tarybos išvados (2018 m. birželio 26 d.) dėl ES koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.
PESCO greitojo reagavimo į kibernetinius incidentus komandos (CRRT)	Kibernetinis	PESCO CRRT yra bendrai išplėtoti ES valstybių narių civiliniai ir kariniai kibernetinės gynybos pajėgumai, kurių paskirtis yra greitai reaguoti į kibernetinius incidentus ir kibernetines krizes, taip pat atlikti prevencinius veiksmus, pavyzdžiui, pažeidžiamumo vertinimus ir rinkimų stebėseną. PESCO CRRT misija – gavus prašymą teikti kibernetinę paramą ES valstybėms narėms, ES institucijoms, įstaigoms ir agentūroms, karinėms ES BSGP misijoms ir operacijoms, taip pat šalims partnerėms.	Europos Sąjungos sutarties 42 straipsnio 6 dalis, 46 straipsnis ir 10 protokolas.

Reagavimo į kosmoso grėsmes struktūra (STRA)	Sektorinis (Kosmoso grėsmės, įskaitant su kibernetine veikla susijusias grėsmes)	Reagavimo į kosmoso grėsmes struktūra (STRA) dėl pareigų, kurias Taryba ir vyriausiasis įgaliotinis turi vykdyti, kad būtų išvengta grėsmės, kylančios dėl pagal Sąjungos kosmoso programą sukurtų sistemų ir teikiamų paslaugų diegimo, eksploatavimo ar naudojimo	Tarybos sprendimas (BUSP) 2021/698
Sisteminių kibernetinių incidentų koordinavimo sistema (EU-SCICF)	Sektorinis	Komunikacijos ir koordinavimo reikmėms kuriama sistema, skirta reagavimui į potencialius sisteminius kibernetinio saugumo įvykius finansų sektoriuje ir jų valdymui. Ji bus grindžiama vienu iš numatytų Europos priežiūros institucijų (EPI) vaidmenų pagal Reglamentą (ES) 2022/2554: laipsniškai sudaryti sąlygas veiksmingam koordinuotam Sąjungos lygmens reagavimui didelio tarpvalstybinio su informacinėmis ir ryšių technologijomis (IRT) susijusio incidento arba susijusios grėsmės, darančios sisteminį poveikį visam Sąjungos finansų sektoriui, atveju.	2021 m. gruodžio 2 d. Europos sisteminės rizikos valdybos rekomendacija dėl Europos sisteminių kibernetinių incidentų koordinavimo tarp atitinkamų institucijų sistemos (ESRV/2021/17)
Sąjungos civilinės saugos	Horizontalusis	Užtikrina bendradarbiavimą civilinės saugos srityje, kad būtų pagerinta	Sprendimas 1313/2013/ES

mechanizmas (SCSM)		nelaimių prevencija, parengtis joms ir reagavimas į jas.	
BKIA – bendra keitimosi informacija aplinka	Skirta jūrų sričiai, apima septynis sektorius.	BKIA – tinklas, jungiantis ES ir EEE institucijų, atsakingų už jūrų stebėjimą, sistemas. BKIA sudaro sąlygas sklandžiai ir automatizuotai keistis svarbia informacija tarpvalstybiniu mastu ir tarp įvairių sektorių.	Saugumo ir gynybos strateginis kelrodis – Europos Sąjungai, kuri gina savo piliečius, vertybes bei interesus ir prisideda prie tarptautinės taikos ir saugumo (2022 m. kovo 21 d.).

(4) Ypatingos svarbos sektoriai ir kiti itin svarbūs sektoriai pagal Direktyvą (ES) 2022/2555 ir Sąjungos lygmens sektoriniai krizių valdymo mechanizmai (kai taikytina)		
Sektoriai	**Subsektorius**	**Taikytini sektoriniai krizių valdymo mechanizmai**
Energetika	Elektros energija	Elektros energijos srities veiklos koordinavimo grupė
	Centralizuotas šilumos ir vėsumos tiekimas	Netaikytina
	Nafta	Naftos koordinavimo grupė Europos Sąjungos už jūroje vykdomą naftos ir dujų sektoriaus veiklą atsakingų institucijų grupė (EUOAG)
	Dujos	Dujų koordinavimo grupė
	Vandenilis	Netaikytina
Transportas	Oro	Europos aviacijos krizių koordinavimo padalinys (EACCC)
	Geležinkelių	Netaikytina

	Vandens	Europos žuvininkystės kontrolės agentūra (EŽKA) SafeSeaNet (SSN) Integruotos jūrų paslaugos (IMS) Laivų nuotolinio identifikavimo ir stebėjimo duomenų centras (LRIT) EMSA pagalbinės laivybos paslaugos
	Kelių	Netaikytina
	Horizontalusis	Transporto kontaktinių centrų tinklas, sukurtas pagal Transporto sektoriui skirtą nenumatytų atvejų planą (COM(2022) 211)
Bankininkystė		EU-SCICF
Finansų rinkų infrastruktūra		EU-SCICF Europos finansinės padėties stabilizavimo priemonė

Sveikata		Ankstyvojo įspėjimo ir reagavimo sistema (AĮRS) Ekstremaliųjų sveikatos situacijų valdymo priemonės (HEOF) Skubių pranešimų apie audinių, ląstelių ir kraujo komponentus sistema (RATC/RAB) Ekstremaliųjų visuomenės sveikatos situacijų sistema Skubaus įspėjimo apie cheminių medžiagų sukeltus incidentus sistema (RASCHEM) Europos infekcinių ligų stebėjimo portalas Pasirengimas ekstremaliosioms sveikatos situacijoms ir reagavimas į jas (HERA) Medicininės sveikatos informacijos sistema (MediSys) Vykdomoji medicinos priemonių iniciatyvinė grupė (MDSSG) Skubūs pranešimai farmakologinio budrumo srityje ES sveikatos darbo grupė (EUHTF)

		Sveikatos saugumo komitetas
Geriamasis vanduo		Netaikytina
Nuotekos		Netaikytina
Skaitmeninė infrastruktūra		Netaikytina
IRT paslaugų valdymas		Netaikytina
Viešasis administravimas		Netaikytina
Kosmosas		Reagavimo į kosmoso grėsmes struktūra (STRA)
Pašto ir pasiuntinių paslaugos		Netaikytina
Atliekų tvarkymas		Netaikytina
Cheminių medžiagų gamyba ir platinimas		Skubaus įspėjimo apie cheminių medžiagų sukeltus incidentus sistema (RASCHEM)

Maisto gamyba, perdirbimas ir platinimas		Europos pasėlių stebėsenos sistema Pasaulinis žemės ūkio gamybos anomalijų zonų nustatymas (ASAP) Europos informavimo apie fitosanitarijos tikslais sulaikytas siuntas sistema (EUROPHYT) ES veterinarinių nepaprastųjų padėčių grupė (EUVET) Skubių pranešimų apie nesaugų maistą ir pašarus sistema (RASFF) Europos pasirengimo apsirūpinimo maistu krizėms ir reagavimo į jas mechanizmas (EFSCM) Vidaus rinkos veikimo užtikrinimo ekstremaliomis sąlygomis ir atsparumo didinimo aktas (IMERA)
Gamyba	Medicinos priemonės	Netaikytina
	Kompiuteriniai, elektroniniai ir optiniai gaminiai	Netaikytina
	Mašinos ir įrenginiai	Netaikytina
	Motorinių transporto priemonių, priekabų ir puspriekabių gamyba	Netaikytina

	Kitos transporto įrangos gamyba	Netaikytina
Skaitmeninių paslaugų teikėjai		Netaikytina
Moksliniai tyrimai		Netaikytina

III PRIEDAS. ES kibernetinio saugumo krizių valdymo sistema ir susijusios priemonės

Nuo 2017 m. Sąjunga išplėtojo savo kibernetinio saugumo sistemą priimdama kelis teisės aktus, į kuriuos įtrauktos kibernetinio saugumo krizių valdymui svarbios nuostatos:

- Europos Parlamento ir Tarybos reglamentas (ES) 2019/881[1],
- Europos Parlamento ir Tarybos direktyva (ES) 2022/2555[2],
- Komisijos įgyvendinimo reglamentas (ES) 2024/2690[3], Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2023/2841[4],
- Europos Parlamento ir Tarybos reglamentas (ES) 2021/887[5],
- Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847[6] ir
- Europos Parlamento ir Tarybos reglamentas (ES) 2025/38 (Kibernetinio solidarumo aktas)[7].

Tarp konkrečių sektorinių kibernetinio saugumo krizėms skirtų priemonių yra Komisijos deleguotasis reglamentas (ES) 2024/1366[8] ir būsima sisteminių kibernetinių incidentų koordinavimo sistema (EU-SCICF) pagal Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554[9].

Remiantis Direktyva 2013/40/ES[10] apibrėžiama su kibernetiniais išpuoliais susijusi nusikalstama veikla ir nustatytos Sąjungos taisyklės dėl tarpvalstybinės prieigos prie elektroninių įrodymų, o Europos Parlamento ir Tarybos reglamentu (ES) 2023/1543[11], kai jis bus įgyvendintas, bus labai palengvinti teisėsaugos veiksmai šioje srityje.

ES kibernetinės gynybos politikoje[12] apibūdinti ES operatyvinio karinių kompiuterinių incidentų skubaus tyrimo tarnybų tinklo (MICNET) ir ES kibernetinės gynybos vadų konferencijos vaidmenys ir numatoma įsteigti ES kibernetinės gynybos koordinavimo centrą (EUCDCC).

Kai kuriuose iš Direktyvos (ES) 2022/2555 I ir II prieduose nurodytų ypatingos svarbos sektorių veikia kiti, ne kibernetinės srities informuotumo apie padėtį ir reagavimo į krizes mechanizmai.

Tarybos rekomendacijoje dėl plano koordinuoti reagavimą Sąjungos lygmeniu į didelę tarpvalstybinę reikšmę turinčius ypatingos svarbos infrastruktūros sutrikimus[13] numatytas atitinkamų subjektų bendradarbiavimas tais atvejais, kai incidentas daro poveikį tiek fiziniams ypatingos svarbos infrastruktūros aspektams, tiek jos kibernetiniam saugumui.

[1] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] 2024 m. spalio 17 d. Komisijos įgyvendinimo reglamentas (ES) 2024/2690, kuriuo nustatomos Direktyvos (ES) 2022/2555 taikymo taisyklės, susijusios su kibernetinio saugumo rizikos valdymo priemonių techniniais ir metodiniais reikalavimais ir išsamesniu atvejų, kuriais incidentas laikomas dideliu, apibūdinimu, skirtais DNS paslaugų teikėjams, aukščiausio lygio domenų vardų registrams, debesijos kompiuterijos paslaugų teikėjams, duomenų centrų paslaugų teikėjams, turinio teikimo tinklų teikėjams, valdomų paslaugų teikėjams, valdomų saugumo paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams (OL L, 2024/2690, 2024 10 18). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] 2023 m. gruodžio 13 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2023/2841, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti (OL L, 2023/2841, 2023 12 18, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/887, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas (OL L 202, 2021 6 8, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas) (OL L, 2024/2847, 2024 11 20, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] 2024 m. gruodžio 19 d. Europos Parlamento ir Tarybos reglamentas (ES) 2025/38, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės ir iš dalies keičiamas Reglamentas (ES) 2021/694 (Kibernetinio solidarumo aktas) (OL L, 2025/38, 2025 1 15, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] 2024 m. kovo 11 d. Komisijos deleguotasis reglamentas (ES) 2024/1366, kuriuo Europos Parlamento ir Tarybos reglamentas (ES) 2019/943 papildomas nustatant tinklo kodeksą dėl tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektų sektorinių taisyklių, (OL L, 2024/1366, 2024 5 24, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 (OL L 333, 2022 12 27, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL L 218, 2013 8 14, p. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] 2023 m. liepos 12 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/1543 dėl Europos įrodymų pateikimo orderių ir Europos įrodymų saugojimo orderių elektroniniams įrodymams baudžiamajame procese ir laisvės atėmimo bausmių vykdymui pasibaigus baudžiamajam procesui ir 2023 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva (ES) 2023/1544, kuria nustatomos suderintos paskirtųjų įmonių ir teisinių atstovų skyrimo elektroniniams įrodymams baudžiamajame procese rinkti taisyklės (OL L 191, 2023 7 28, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/lt/TXT/PDF/?uri=CELEX:52022JC0049

[13] *OL C, C/2024/4371, 2024 7 5.* https://eur-lex.europa.eu/legal-content/lt/TXT/PDF/?uri=CELEX:52022JC0049