Europos Sąjungos
Taryba

Briuselis, 2021 m. spalio 20 d.
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
data:	2021 m. spalio 19 d.
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	12534/21
Dalykas:	Tarybos išvados dėl pasinaudojimo Jungtinio kibernetinio saugumo padalinio iniciatyvos galimybėmis, papildant ES koordinuotą atsaką į didelio masto kibernetinio saugumo incidentus ir krizes - Tarybos išvados (2021 m. spalio 19 d.)

Delegacijoms priede pateikiamos Tarybos išvados dėl pasinaudojimo Jungtinio kibernetinio saugumo padalinio iniciatyvos galimybėmis, papildant ES koordinuotą atsaką į didelio masto kibernetinio saugumo incidentus ir krizes, kurias Taryba priėmė 2021 m. spalio 19 d.

PRIEDAS

Tarybos išvados dėl pasinaudojimo Jungtinio kibernetinio saugumo padalinio iniciatyvos galimybėmis, papildant ES koordinuotą atsaką į didelio masto kibernetinio saugumo incidentus ir krizes

EUROPOS SĄJUNGOS TARYBA,

PRIMINDAMA savo išvadas dėl:

– ES skaitmeninio dešimtmečio kibernetinio saugumo strategijos[1],

– ES koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes[2],

– kibernetinio saugumo diplomatijos[3],

– bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos („Kibernetinio saugumo diplomatijos priemonių rinkinio“)[4],

– saugumo ir gynybos[5],

– ES kibernetinės gynybos politikos metmenų[6],

– Europos skaitmeninės ateities kūrimo[7],

– 2018 m. gruodžio 11 d. Tarybos įgyvendinimo sprendimą (ES) 2018/1993 dėl ES integruoto politinio atsako į krizes mechanizmo,

---

1 Dok. 7290/21.
2 Dok. 10086/18.
3 Dok. 6122/15 + COR 1.
4 Dok. 10474/17.
5 Dok. 8396/21.
6 Dok. 15585/14.
7 Dok. 8711/20.

– Bendrą komunikatą Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“[8],

– kibernetinio saugumo pajėgumų ir gebėjimų stiprinimo ES[9],

1. AKCENTUOJA kibernetinio saugumo svarbą kuriant atsparią, skaitmeninę ir žalią Europą. PABRĖŽIA, kad kibernetinis saugumas yra būtinas ES ir jos valstybių narių, jų gyventojų, įmonių ir institucijų klestėjimui ir saugumui, taip pat mūsų laisvos ir demokratinės visuomenės vientisumui išsaugoti.

2. PRIPAŽĮSTA daugelio kibernetinio saugumo grėsmių tarpvalstybinį ir tarpsektorinį pobūdį ir nuolatinių stipresnio poveikio, rafinuotesnių, geriau nukreiptų, sudėtingesnių, labiau nuolatinių ir (arba) įsigalėjusių kibernetinės kenkimo veiklos kampanijų riziką ir galimus padarinius[10]. COVID-19 pandemija dar labiau atskleidė mūsų visuomenės pažeidžiamumą ir galimą didelio masto kibernetinių incidentų žalą ekonomikai, demokratijai, esminėms paslaugoms ir ypatingos svarbos infrastruktūrai, ypač sveikatos sektoriuje. Ji taip pat sustiprino sujungiamumo svarbą ir visuomenės priklausomybę nuo patikimų, užtikrintų ir saugių tinklų ir informacinių sistemų. Galiausiai ji išryškino poreikį užtikrinti visuotinį, atvirą, laisvą, stabilų ir saugų internetą, taip pat pasitikėjimą informacinių ir ryšių technologijų (IRT) produktais, procesais ir paslaugomis bei jų saugumu, įskaitant poreikį užtikrinti atsparią tiekimo grandinę.

---

8 Dok. 14435/17 + COR 1.
9 Dok. 7737/19.
10 ENISA 2020 m. grėsmių padėtis.

3. PAKARTOJA, jog svarbu stiprinti kibernetinį atsparumą ir toliau plėtoti ES kibernetinio saugumo krizių valdymo sistemą[11] siekiant užtikrinti, kad ES lygmeniu būtų veiksmingai laiku reaguojama į didelio masto kibernetinio saugumo incidentus ir krizes, ir toliau šiuos aspektus integruoti į esamus horizontaliuosius ir sektorinius ES reagavimo į krizes mechanizmus. PABRĖŽIA Tarybos ir integruoto politinio atsako į krizes mechanizmo (IPCR) priemonių vaidmenį užtikrinant, kad Sąjungos politiniu lygmeniu būtų laiku koordinuojami su krizėmis, kilusiomis Sąjungoje ar už jos ribų, kurios turi plataus masto poveikį arba yra didelės politinės reikšmės, susiję veiksmai ir į jas būtų laiku reaguojama. AKCENTUOJA, kad svarbu reguliariai testuoti tokias sistemas ir mechanizmus.

4. PRIMENA, kad veikla, susijusi su didelio masto kibernetiniais incidentais ir krizėmis, ES lygmeniu vykdoma vadovaujantis subsidiarumo, proporcingumo, papildomumo, nedubliavimo ir konfidencialumo principų. PAKARTOJA, kad pagrindinė atsakomybė už reagavimą į didelio masto kibernetinio saugumo incidentus ir krizes tenka valstybėms narėms, kurias jie paveikia. PRIMENA, kad svarbu gerbti valstybių narių kompetenciją ir jų išimtinę atsakomybę už nacionalinį saugumą pagal Europos Sąjungos sutarties 4 straipsnio 2 dalį, be kita ko, kibernetinio saugumo srityje.

5. Tuo pačiu metu PRIMENA, kad svarbu gerbti ES institucijų, organų ir agentūrų kompetenciją ir įgaliojimus. Vyriausiajam įgaliotiniui, Komisijai ir kitoms ES institucijoms, organams ir agentūroms taip pat tenka svarbus vaidmuo pagal Sąjungos teisę, be kita ko, dėl galimo didelio masto kibernetinio saugumo incidentų ir krizių poveikio bendrajai rinkai, taip pat pačių ES institucijų, organų ir agentūrų veikimui.

[11] Dok. 10086/18.

6. PABRĖŽIA, kad reikia vengti nereikalingo dubliavimo ir siekti papildomumo bei pridėtinės vertės toliau plėtojant ES kibernetinio saugumo krizių valdymo sistemą ir užtikrinti suderinimą su esamais mechanizmais, iniciatyvomis, tinklais, procesais, procedūromis nacionaliniu ir Europos lygmenimis. AKCENTUOJA, kad svarbu racionalizuoti esamus procesus ir struktūras siekiant sumažinti sudėtingumą, o sanglaudos užtikrinimo Sąjungoje tikslais – gerinti prieinamumą ir reagavimą į poreikius tų, kurie prašo pagalbos ir solidarumo.

7. PRIPAŽĮSTA tarptautinės teisės, įskaitant visą Jungtinių Tautų Chartiją, tarptautinę humanitarinę teisę ir žmogaus teisių teisę, taikymą kibernetinei erdvei ir SKATINA prisijungti prie atsakingos valstybės elgesio kibernetinėje erdvėje savanoriškų neprivalomų normų, taisyklių ir principų, kuriuos yra patvirtinusios visos JT valstybės narės.

8. PALANKIAI VERTINA pažangą, kuri pastaraisiais metais buvo padaryta Taryboje, ypač Kibernetinių klausimų horizontaliojoje darbo grupėje (HWPCI) ir kitose atitinkamose Tarybos darbo grupėse, taip pat rengiant kitas valstybių narių bendradarbiavimo ir dalijimosi informacija iniciatyvas, tinklus ir mechanizmus, konkrečiai, TIS bendradarbiavimo grupėje ir CSIRT tinkle, sukurtame 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148, Europos ryšių palaikymo dėl kibernetinių krizių organizaciniame tinkle (CyCLONe), taip pat įgyvendinant atitinkamus su kibernetine gynyba susijusius projektus, pradėtus pagal nuolatinį struktūrizuotą bendradarbiavimą (PESCO)[12], Jungtinėje elektroninių nusikaltimų klausimų darbo grupėje (J-CAT), Europos teisminiame kovos su kibernetiniais nusikaltimais tinkle, valstybių narių savanoriškus įnašus ES žvalgybos ir situacijų centrui (EU INTCEN) ir veiksmų koordinavimą bei bendradarbiavimą Kibernetinio saugumo diplomatijos priemonių rinkinio kontekste.

[12] Visų pirma projektą „Greitojo reagavimo į kibernetinius incidentus komandos ir savitarpio pagalba kibernetinio saugumo srityje“, kurį koordinuoja Lietuva, projektą „Kibernetinės ir informacinės srities koordinavimo centras“, kurį koordinuoja Vokietija, ir projektą „Dalijimosi informacija apie reagavimą į kibernetines grėsmes ir incidentus platforma“, kurį koordinuoja Graikija.

9. PRIMENA esamas ES institucijų, organų ir agentūrų bendradarbiavimo sistemas, pavyzdžiui, struktūrinį ENISA ir Europos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU) bendradarbiavimą, ENISA, Europos gynybos agentūros (EGA), Europolo Europos kovos su elektroniniu nusikalstamumu centro (EC3) ir CERT-EU susitarimo memorandumą. PABRĖŽIA, kad svarbu su Taryba toliau reguliariai dalytis informacija apie tolesnius šių bendradarbiavimo sistemų pokyčius.

10. AKCENTUOJA, kad svarbu stiprinti ES ir jos valstybių narių įvairių kibernetinės srities bendruomenių bendradarbiavimą ir dalijimąsi informacija visais reikiamais lygmenimis – techniniu, operaciniu ir strateginiu / politiniu – ir susieti esamus krizių valdymo mechanizmus, tinklus, struktūras, procesus ir procedūras, kai tai padeda reaguoti į didelio masto kibernetinius incidentus bei krizes ir šias pastangas pagerina.

11. PRIPAŽĮSTA pažangą, kurią padarė valstybių narių grupė kuriant bendrus operatyvinius kibernetinius pajėgumus – greitojo reagavimo komandas pagal PESCO sistemą, siekiant stiprinti savanorišką bendradarbiavimą kibernetinėje srityje teikiant savitarpio pagalbą, be kita ko, reaguojant į didelio masto kibernetinius incidentus ir krizes.

12. PRIPAŽĮSTA teisėsaugos srities bendruomenės patirtį ir reagavimo pajėgumus (teikiamus visą parą 7 dienas per savaitę) operacinio bendradarbiavimo ir saugaus keitimosi informacija kovojant su dideliais tarpvalstybiniais kibernetiniais išpuoliais srityje, pasinaudojant ES teisėsaugos institucijų reagavimo į ekstremaliąsias situacijas protokolu.

13. PRIPAŽĮSTA nuolatinį bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos (toliau – „kibernetinio saugumo diplomatijos priemonių rinkinio“) įgyvendinimą. PRIMENA, kad kiekviena valstybė narė gali pati kiekvienu atveju atskirai priimti suverenius sprendimus dėl kibernetinės kenkimo veiklos priskyrimo. PRIMENA, kad priemonės, kurių imamasi įgyvendinant bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemą, turėtų būti grindžiamos valstybių narių sutartu bendru informuotumu apie padėtį. ES žvalgybos ir situacijų centras (EU INTCEN) atlieka esminį vaidmenį kaip centras, kuris Europos Sąjungai užtikrina informuotumą apie padėtį ir vertina grėsmes kibernetinėje srityje, remdamasis savanoriškais valstybių narių žvalgybos duomenimis ir nepažeisdamas jų kompetencijos.

14. PAKARTOJA savitarpio pagalbos ir solidarumo svarbą pagal Europos Sąjungos sutarties 42 straipsnio 7 dalį bei Sutarties dėl Europos Sąjungos veikimo 222 straipsnį, taip pat RAGINA vykdyti tolesnes pratybas, susijusias su kibernetiniais aspektais. PRIMENA, kad reikia apsvarstyti ES kibernetinio saugumo krizių valdymo sistemos, kibernetinio saugumo diplomatijos priemonių rinkinio ir pirmiau minėtų straipsnių nuostatų sąsajas didelio masto kibernetinio incidento ar krizės atveju. Taip pat PRIMENA, kad iš Europos Sąjungos sutarties 42 straipsnio 7 dalies kylančios valstybių narių pareigos nepažeidžia tam tikrų valstybių narių saugumo ir gynybos politikos specifinio pobūdžio. Be to, PRIMENA, kad NATO tebėra valstybių, kurios yra jos narės, kolektyvinės gynybos pagrindas.

15. PRIPAŽĮSTA ES ir NATO bendradarbiavimą kibernetinio saugumo ir gynybos srityje, be kita ko, CERT-EU ir NATO reagavimo į kompiuterinius incidentus tarnybos (NCIRC) dalijimąsi informacija visapusiškai laikantis skaidrumo, abipusiškumo ir įtraukimo principų, taip pat abiejų organizacijų sprendimų priėmimo autonomiškumo.

16. PRIPAŽĮSTA, kad, kai tikslinga, svarbu bendradarbiauti su privačiuoju sektoriumi vykdant dalijimosi informacija veiklą, teikiant atitinkamas ekspertines žinias, taip pat priimant patikimus sprendimus ir teikiant patikimas paslaugas, įskaitant, pavyzdžiui, paramą įvairioms kibernetinės srities bendruomenėms reaguojant į incidentus ir gerinant informuotumą apie padėtį.

17. PABRĖŽIA, kad svarbu užtikrinti saugius ryšių kanalus keitimuisi įslaptinta ir neskelbtina informacija. AKCENTUOJA, kad reikia tolesnės pažangos.

Šiuo atžvilgiu ir atsižvelgiant į tai, kas išdėstyta pirmiau:

18. PRIPAŽĮSTA Komisijos rekomendaciją dėl Jungtinio kibernetinio saugumo padalinio sukūrimo, nes tai yra iniciatyva, kurią reikia apsvarstyti toliau plėtojant ES kibernetinio saugumo krizių valdymo sistemą[13].

19. RAGINA ES ir jos valstybes nares toliau dėti pastangas siekiant visapusiškesnės ir veiksmingesnės ES kibernetinio saugumo krizių valdymo sistemos, grindžiamos esamais mechanizmais ir jau padaryta pažanga, taip pat atsižvelgti į Jungtinio kibernetinio saugumo padalinio iniciatyvos galimybes papildyti šiuos mechanizmus laikantis laipsniško požiūrio. PABRĖŽIA, kad didinant pasitikėjimą ypač svarbus pakopinis, skaidrus ir įtraukus procesas, todėl labai svarbu toliau plėtoti ES kibernetinio saugumo krizių valdymo sistemą. Vykdant šį procesą turėtų būti atsižvelgiama į esamus valstybių narių ir ES institucijų, organų ir agentūrų vaidmenis, kompetenciją ir įgaliojimus, taip pat į šiose išvadose išdėstytus principus, įskaitant proporcingumo, subsidiarumo, įtraukumo, papildomumo, nedubliavimo ir informacijos konfidencialumo principus. Tuo pačiu metu PABRĖŽIA, kad bet koks galimas valstybių narių dalyvavimas galimo Jungtinio kibernetinio saugumo padalinio veikloje ar įnašai jam bus savanoriško pobūdžio.

[13] Dok. C(2021) 4520 final (dok. 11155/21 ir dok. 11155/21 ADD 1).

20. PABRĖŽIA, jog reikia nustatyti tinkamus darbo metodus ir valdymą, kad visos valstybės narės galėtų įsitraukti ir dalyvauti svarstymuose, plėtoti veiksmingus sprendimų priėmimo procesus, susijusius su ES kibernetinio saugumo krizių valdymo sistema, be kita ko, ir su galimu Jungtiniu kibernetinio saugumo padaliniu. RAGINA pasinaudoti Tarybos prerogatyvomis pagal Sutartis ir laikytis lojalaus bendradarbiavimo principo.

21. AKCENTUOJA, kad svarbu nustatyti ir įtraukti visas ES ir jos valstybių narių atitinkamas kibernetinės srities bendruomenes, tuo pat metu atsižvelgiant į jų įvairius vaidmenis ir atsakomybę įvairių rūšių didelio masto kibernetinių incidentų ir krizių atvejais. AKCENTUOJA svarbų Tarybos vaidmenį, ypač pasitelkiant HWPCI, formuojant politiką ir imantis koordinuojamo vaidmens toliau plėtojant ES kibernetinio saugumo krizių valdymo sistemą. Todėl PRAŠO valstybių narių, Komisijos, Europos išorės veiksmų tarnybos (EIVT), ES žvalgybos ir situacijų centro (EU INTCEN), Europos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU), Europos Sąjungos kibernetinio saugumo agentūros (ENISA), Europolo (EC3), Eurojusto (Europos teisminio kovos su kibernetiniais nusikaltimais tinklo), Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro (ECCC), taip pat reagavimo į kompiuterių saugumo incidentus tarnybų tinklo, Ryšių palaikymo dėl kibernetinių krizių organizacinio tinklo (CyCLONe), TIS bendradarbiavimo grupės, EGA, atitinkamų PESCO projektų atstovų ir kitų galimų suinteresuotųjų subjektų dalyvauti šiame procese. Kaip pasiūlyta Komisijos rekomendacijoje, galėtų būti toliau svarstoma galimybė įsteigti darbo grupę, užtikrinant tinkamą atstovavimą visoms valstybėms narėms ir veikimą vadovaujantis Tarybos politinėmis gairėmis; ši grupė galėtų tapti laikinu forumu, suburiančiu visų atitinkamų kibernetinės srities bendruomenių atstovus valstybėse narėse ir ES. Tokia darbo grupė turėtų reguliariai teikti savo veiklos ataskaitas ir teikti galimus pasiūlymus Tarybai apsvarstyti, patvirtinti ir tolesnėms gairėms rengti. Be to, galėtų būti užmegztas kitų rūšių dialogas bendruomenėse ir tarp jų, be kita ko, rengiant praktinius seminarus, kitus seminarus, bendrus mokymus ir pratybas.

22. AKCENTUOJA Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro (ECCC) ir Nacionalinių koordinavimo centrų tinklo vaidmenį kuriant galimą Jungtinį kibernetinio saugumo padalinį, ypač atsižvelgiant į jo vaidmenį iš esmės gerinant Sąjungos technologinius pajėgumus, technologinius sprendimus, gebėjimus ir įgūdžius kibernetinio saugumo srityje.

23. PRAŠO ES ir jos valstybių narių įsitraukti į tolesnį ES kibernetinio saugumo krizių valdymo sistemos plėtojimą, be kita ko, pasinaudojant Jungtinio kibernetinio saugumo padalinio iniciatyvos galimybėmis, nustatant ir apibrėžiant procesą, įskaitant tarpinius tikslus ir tvarkaraštį, taip pat aiškiai išdėstant tikslus, galimus vaidmenis ir pareigas. AKCENTUOJA, kad reikia prioriteto tvarka konsoliduoti esamus tinklus ir sąveiką kiekvienoje bendruomenėje, taip pat nustatyti nuodugnią galimo dalijimosi informacija spragų ir poreikių schemą kibernetinės srities bendruomenėse ir tarp jų, taip pat Europos institucijose, organuose ir agentūrose bei tarp jų ir atitinkamai susitarti dėl galimo Jungtinio kibernetinio saugumo padalinio galimų pagrindinių tikslų ir prioritetų. Nedarant poveikio rezultatams, PABRĖŽIA, kad reikia daugiausia dėmesio skirti dalijimosi informacija poreikių nustatymui siekiant suformuoti visų atitinkamų bendruomenių bendrą informuotumą apie padėtį. Nustatant dalijimosi informacija spragas ir poreikius, be kita ko, galbūt naudojantis virtualiomis platformomis, tinkamas dėmesys turėtų būti skiriamas saugiems keitimosi įslaptinta ir neskelbtina informacija kanalams, kartu PABRĖŽIANT, kad svarbu naudotis jau esama infrastruktūra. Diegiant laipsnišką požiūrį siekiama stiprinti pasitikėjimą ir pagrindą galimiems tolesniems veiksmams, susijusiems su parengties ir operacinio bendradarbiavimo stiprinimu. PRIPAŽĮSTA, kad skirtingiems tikslams gali būti reikalingi skirtingi sprendimai ir įvairių skirtingų kibernetinės srities bendruomenių atstovų dalyvavimas ES ir jos valstybėse narėse.

24. RAGINA viso proceso metu toliau svarstyti galimo Jungtinio kibernetinio saugumo padalinio įsteigimo teisinį pagrindą, be kita ko, įvertinti užduotis ir vaidmenis, palyginti su užduotimis ir vaidmenimis, rekomendacijoje pavestais ENISA, atsižvelgiant į 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamento (ES) 2019/881 7 straipsnį. RAGINA toliau svarstyti atskirus Rekomendacijos dėl Jungtinio kibernetinio saugumo padalinio sukūrimo elementus, be kita ko, susijusius su ES greitojo reagavimo grupių idėja ir ES reagavimo į kibernetinius incidentus ir krizes planu. AKCENTUOJA, kad galimas Jungtinis kibernetinio saugumo padalinys turi atsižvelgti į jo galimų būsimų dalyvių kompetenciją, įgaliojimus ir teisinius įgaliojimus.

25. RAGINA ES ir jos valstybes nares apsvarstyti galimybes pasinaudoti Jungtinio kibernetinio saugumo padalinio iniciatyvos galimybėmis, be kita ko, ir iš ES institucijų, organų ir agentūrų perspektyvos, siekiant papildyti valstybių narių lygmeniu dedamas pastangas. PALANKIAI VERTINA Komisijos ketinimą stiprinti atitinkamų ES institucijų, organų ir agentūrų atsparumą rengiant būsimą pasiūlymą dėl reglamento dėl bendrų privalomų kibernetinio saugumo taisyklių, taikomų ES institucijoms, organams ir agentūroms.

26. Todėl DAR KARTĄ PAKARTOJA savo įsipareigojimą didinti kibernetinį atsparumą ir toliau plėtoti ES kibernetinio saugumo krizių valdymo sistemą ir REGULIARIAI STEBĖS pažangą ir teiks tolesnes gaires dėl ES kibernetinio saugumo krizių valdymo sistemos papildymo.