Europos Sąjungos
Taryba

Briuselis, 2017 m. lapkričio 20 d.
(OR. en)

14435/17

CYBER 183
TELECOM 303
ENFOPOL 534
JAI 1055
MI 845
COSI 283
JAIEX 101
RELEX 989
IND 317
CSDP/PSDC 643
COPS 360
POLMIL 145

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
data:	2017 m. lapkričio 20 d.
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	13943/17 + COR 1
Komisijos dok. Nr.:	12210/17, 12211/17
Dalykas:	Tarybos išvados dėl bendro komunikato Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“ – Tarybos išvados (2017 m. lapkričio 20 d.)

Delegacijoms priede pateikiamo 2017 m. lapkričio 20 d. Bendrųjų reikalų tarybos posėdyje priimtos Tarybos išvados dėl bendro komunikato Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“.

PRIEDAS

Tarybos išvadų dėl bendro komunikato Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“ projektas

Europos Sąjungos Taryba,

1. PRIPAŽINDAMA, koks yra svarbus kibernetinis saugumas ES klestėjimui, ekonomikos augimui bei saugumui ir mūsų laisvų ir demokratinių visuomenių vientisumui ir jų pamatiniams procesams skaitmeniniame amžiuje užtikrinant tiek teisinės valstybės, tiek žmogaus teisių ir kiekvieno asmens pagrindinių laisvių apsaugą;

2. PABRĖŽDAMA, kad kibernetinio saugumo klausimą reikia spręsti taikant nuoseklų požiūrį nacionaliniu, ES ir pasauliniu lygmeniu, kadangi kibernetinės grėsmės gali daryti poveikį mūsų demokratijai, klestėjimui, stabilumui ir saugumui;

3. PAŽYMI, kad aukšto lygio kibernetinis atsparumas visoje ES taip pat svarbus siekiant pasitikėjimo bendrąja skaitmenine rinka ir toliau plėtojant skaitmeninę Europą;

4. PAKARTODAMA, kad ES nuolat rems atvirą, pasaulinę, laisvą, taikią ir saugią kibernetinę erdvę, kurioje tiek Europos Sąjungos, tiek pasaulio mastu visapusiškai taikomos ir gerbiamos žmogaus teisės ir pagrindinės laisvės, visų pirma, saviraiškos laisvė, galimybė susipažinti su informacija, duomenų apsauga, privatumas ir saugumas, taip pat pagrindinės ES vertybės ir principai, ir AKCENTUODAMA, kad yra itin svarbu užtikrinti tinkamą pusiausvyrą tarp žmogaus teisių bei pagrindinių laisvių ir ES vidaus saugumo politikos reikalavimų laikymosi[1];

5. PRIPAŽINDAMA, kad kibernetinėje erdvėje taikoma tarptautinė teisė, įskaitant visą JT chartiją, tarptautinę humanitarinę teisę ir žmogaus teisių teisę, ir todėl PABRĖŽIA, kad reikia toliau dėti pastangas užtikrinant, kad kibernetinėje erdvėje būtų laikomasi tarptautinės teisės;

[1] Dok. 12650/17.

6. PRIMINDAMA savo išvadas dėl ES kibernetinio saugumo strategijos[2], dėl interneto valdymo[3], dėl Europos kibernetinio atsparumo sistemos stiprinimo[4], dėl kibernetinio saugumo diplomatijos[5] ir dėl bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos[6], taip pat dėl baudžiamosios teisenos kibernetinėje erdvėje stiprinimo[7], dėl saugumo ir gynybos įgyvendinant Visuotinę ES strategiją[8], dėl bendros kovos su hibridinėmis grėsmėmis sistemos[9] ir dėl atnaujintos 2015–2020 m. Europos Sąjungos vidaus saugumo strategijos laikotarpio vidurio peržiūros[10];

7. PRIPAŽINDAMA, kad Europos Tarybos konvencijoje dėl elektroninių nusikaltimų (Budapešto konvencijoje) nustatyta sistema yra patikimas pagrindas įvairioms šalims taikyti veiksmingą teisinį standartą skirtingų nacionalinės teisės aktų ir tarptautinio bendradarbiavimo kovos su kibernetiniais nusikaltimais srityje atveju.

8. PRIPAŽINDAMA, kad reikia iš naujo akcentuoti 2014 m. ES kibernetinės gynybos politikos sistemos įgyvendinimą ir ją atnaujinti siekiant kibernetinį saugumą ir gynybą labiau integruoti į bendrą saugumo ir gynybos politiką (BSGP) ir į platesnę saugumo ir gynybos darbotvarkę;

9. PRIPAŽINDAMA, kad pasauliniu mastu konkurencinga Europos pramonė yra svarbus aspektas siekiant aukšto lygio kibernetinio saugumo nacionaliniu lygmeniu ir visoje ES;

10. PRIMINDAMA, kad pagal ES sutarties 4 straipsnio 2 dalį kiekviena valstybė narė yra išimtinai atsakinga už savo nacionalinį saugumą.

---

2 Dok. 12109/13 ir dok. 6225/13 (bendras komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“ (COM JOIN(2013) 1 final).

3 Dok. 16200/14 ir dok. 6460/14 (Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Interneto politika ir valdymas. Europos vaidmuo formuojant būsimą interneto valdymą“ (COM(2014) 72 final).

4 Dok. 14540/16 ir dok. 11013/16 (Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos kibernetinio atsparumo sistemos stiprinimas ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimas (COM 2016(410) final).

5 Dok. 6122/15.

6 Dok. 9916/17.

7 Dok. 10007/16.

8 Dok. 9178/17.

9 Dok. 7688/16 (bendras komunikatas Europos Parlamentui ir Tarybai „Bendra kovos su mišriomis grėsmėmis sistema. Europos Sąjungos atsakas“.

10 Dok. 12650/17.

ŠIOSE IŠVADOSE

11. PALANKIAI VERTINA bendrą komunikatą Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, kadangi juo siūlomas plataus užmojo tikslas stiprinti kibernetinį saugumą ES. Juo taip pat prisidedama prie ES strateginės autonomijos, kaip nurodyta Tarybos išvadose dėl visuotinės Europos Sąjungos užsienio ir saugumo politikos strategijos[11], kadangi siekiama sukurti skaitmeninę Europą, kuri būtų saugesnė, kelianti pasitikėjimą, suprantanti savo stiprybes, konkurencinga, atvira pasauliui, gerbianti ES bendras vertybes, susijusias su atviru, laisvu, taikiu ir saugiu pasauliniu internetu, ir todėl atsparesnė, kad galėtų užkirsti kelią kibernetinėms grėsmėms, užtikrinti atgrasymą, tas grėsmes nustatyti ir į jas reaguoti ir taip pat sugebėtų bendrai reaguoti į kibernetines grėsmes visoje ES, ir

12. PRAŠO valstybių narių, ES institucijų, agentūrų ir įstaigų, siekiant šiose išvadose išdėstytų strateginių tikslų, bendradarbiauti laikantis atitinkamų jų kompetencijos sričių ir subsidiarumo bei proporcingumo principo, ir

13. PABRĖŽIA, kad ES, jos valstybės narės ir privatusis sektorius turi užtikrinti pakankamą finansavimą, atsižvelgiant į turimus išteklius, siekiant remti kibernetinio atsparumo stiprinimą ir kibernetinio saugumo srities mokslinių tyrimų ir plėtros pastangas visoje ES, taip pat stiprinti bendradarbiavimą, kad būtų užkirstas kelias kibernetinėms grėsmėms, užtikrintas atgrasymas, tos grėsmės nustatytos ir į jas reaguojama ir taip pat būtų galima bendrai reaguoti į didelio masto kibernetinius incidentus ir kibernetinę kenkimo veiklą visoje ES;

---

[11] Dok. 13202/16.

I skyrius

VEIKSMINGO KIBERNETINIO ATSPARUMO IR PASITIKĖJIMO BENDRĄJA SKAITMENINE RINKA UŽTIKRINIMAS

14. PABRĖŽIA, kad atsakomybė už savo kibernetinio saugumo stiprinimą ir atsako į kibernetinius incidentus ir krizes užtikrinimą visų pirma tenka kiekvienai valstybei narei, o ES gali suteikti didelės pridėtinės vertės remdama valstybių narių bendradarbiavimą. Šiame kontekste AKCENTUOJA, kad visos valstybės narės turi skirti reikiamų išteklių už kibernetinį saugumą atsakingoms nacionalinėms institucijoms, siekiant užtikrinti kibernetinių incidentų ir krizių prevenciją, nustatymą ir reagavimą į juos visoje ES;

15. PABRĖŽIA, kad, kai įmanoma, reikia pasinaudoti esamais ES lygmens mechanizmais, struktūromis ir organizacijomis;

16. PALANKIAI VERTINA:

- pažangą, kurią valstybės narės padarė į nacionalinę teisę perkeldamos Tinklų ir informacijos saugumo direktyvą (TIS direktyvą), ir PABRĖŽIA, kad reikia užtikrinti, kad ne vėliau kaip 2018 m. gegužės mėn. jį būtų visapusiškai ir veiksmingai įgyvendinama, kaip nustatyta toje direktyvoje[12];
- darbą, atliekamą TIS bendradarbiavimo grupėje stiprinant valstybių narių tarpusavio strateginį bendradarbiavimą ir keitimąsi informacija;
- darbą, atliekamą reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinkle, visų pirma siekiant stiprinti valstybių narių operatyvinį bendradarbiavimą, didinant pasikliovimą ir pasitikėjimą keičiantis informacija, kai sprendžiami didelio masto kibernetinio saugumo incidentai, ir – remiantis valstybių narių nacionalinėmis išvadomis – teikiant elementus ES lygmens bendram padėties vertinimui atlikti;
- darbą, atliekamą įgyvendinant sutartimi pagrįstą viešojo ir privačiojo sektorių partnerystę kibernetinio saugumo srityje.

[12] Nedarant poveikio valstybių narių kompetencijai dėl TIS direktyvos perkėlimo į nacionalinę teisę, visų pirma kiek tai susiję su esminių paslaugų operatoriais.

17. PALANKIAI VERTINA tai, kad bendrame komunikate patvirtinta, jog tvirtas ir patikimas šifravimas yra itin svarbus siekiant tinkamai užtikrinti žmogaus teises ir pagrindines teises ES ir visuomenės pasitikėjimui bendrąja skaitmenine rinka, kartu atsižvelgiant į tai, kad teisėsaugos institucijoms reikia prieigos prie jų atliekamiems tyrimams būtinų duomenų, ir patvirtinta, kad tiek saugiam skaitmeniniam tapatybės nustatymui, tiek komunikacijai tenka svarbus vaidmuo užtikrinant veiksmingą kibernetinį saugumą Europos Sąjungoje;

18. PALANKIAI VERTINA bendrame komunikate pateiktą planą didinti užmojį reguliariai vykdant visos Europos kibernetinio saugumo srities pratybas, remiantis „Cyber Europe“ pratybose įgyta patirtimi, derinant atsaką įvairiais lygmenimis, kadangi tai taps svarbiu aspektu gerinant valstybių narių ir ES institucijų parengtį reaguoti į didelio masto kibernetinius incidentus;

19. RAGINA ES ir jos valstybes narės reguliariai vykdyti strategines kibernetinio saugumo pratybas įvairių sudėčių Tarybos posėdžiuose, remiantis patirtimi, įgyta EU CYBRID 2017 metu, ir

20. Nedarant poveikio teisėkūros proceso rezultatams:

- PALANKIAI VERTINA pasiūlymą dėl tvirtų ir nuolatinių ENISA įgaliojimų siekiant pagrindinio tikslo – remti ir plėtoti glaudesnį valstybių narių bendradarbiavimą, padidinti jų pajėgumus ir sustiprinti pasitikėjimą skaitmenine Europa;

- DAR KARTĄ PATVIRTINA, kad ateityje ENISA turėtų būti grindžiama valstybių narių ir ES patirtimi bei ekspertinėmis žiniomis ir remti nuolatinį esamos ir būsimos ES kibernetinio saugumo politikos ir normų plėtojimą ir įgyvendinimą, kartu užtikrinant, kad visos ENISA kompetencijos būtų plėtojamos papildant valstybių narių kompetenciją;

- DAR KARTĄ PATVIRTINA tikslą – stiprinti pasitikėjimą skaitmenine Europa didinant pasikliovimą ir pasitikėjimą skaitmeniniais sprendimais ir inovacijomis, įskaitant daiktų internetą, e. prekybą ir e. valdymą, visų pirma pasaulinio lygio Europos kibernetinio saugumo sertifikavimo sistemos atžvilgiu[13]. Tai yra vienas iš svarbiausių reikalavimų siekiant stiprinti pasitikėjimą skaitmeniniais gaminiais bei paslaugomis ir didinti jų saugumą, saugoti ypatingos svarbos infrastruktūros objektus, valdžios sektoriaus, piliečių bei įmonių duomenis ir tai padės nustatyti gaminiams, paslaugoms ir procesams bendrojoje skaitmeninėje rinkoje taikomą integruotąjį saugumo požiūrį;

- PABRĖŽIA, kad vykdant teisėkūros veiklą, kad būtų sugriežtintas kibernetinio saugumo sertifikavimas ES lygmeniu, turės būti tenkinami rinkos ir naudotojų poreikiai, remiamasi patirtimi ES esamų sertifikavimo pajėgumų ir procesų (pavyzdžiui, vyresniųjų pareigūnų grupės informacinių sistemų klausimais (SOG-IS) darbo) srityje ir turėtų būti sukurta sistema, kuri pajėgtų greitai prisitaikyti prie būsimų naujausių skaitmeninių pokyčių;

- PABRĖŽIA, kad stiprinant kibernetinio saugumo sertifikavimą ES, reikėtų įtraukti visą saugumo reikalavimų spektrą, apimant ir griežčiausius reikalavimus, kai turi būti pademonstruotas atsparumas išpuolių vykdytojų pajėgumams. Pagrindiniai sėkmingo darbo veiksniai būtų patikimo, skaidraus ir nepriklausomo saugumo sertifikavimo proceso užtikrinimas siekiant skatinti patikimų ir saugių prietaisų, programinės įrangos ir paslaugų prieinamumą bendrojoje rinkoje ir už jos ribų; atitinkamos Europos pramonės, vyriausybių ir vertinimo specialistų ekspertinių žinių taikant Europos ir pasaulinius standartus pripažinimas [14]; valstybių narių vaidmens sertifikavimo procese, ypač kiek tai susiję su vertinimu aukštesniais saugumo lygmenimis ir ypač esminių saugumo poreikių ir įgūdžių vertinimo atžvilgiu, gerbimas. Tokia sertifikavimo sistema taip pat turėtų būti užtikrinta, kad visos ES masto sertifikavimo schemos būtų proporcingos užtikrinimo lygiui, kurio reikia naudojimuisi susijusiais IRT gaminiais, paslaugomis ir (arba) sistemomis, ir tai sudaro sąlygas tarpvalstybinei visokio masto įmonių prekybai siekiant kurti naujus gaminius ir jais prekiauti tiek ES, tiek ne ES rinkose.

---

13 Taikant visuotinius standartus, parengtus pagal PPO Sutarties dėl techninių prekybos kliūčių gerosios praktikos kodekso principus.

14 Taikant Europos ir visuotinius standartus, parengtus pagal PPO Sutarties dėl techninių prekybos kliūčių gerosios praktikos kodekso principus.

21. PALANKIAI VERTINA ketinimą sukurti Kibernetinio saugumo kompetencijos centrų tinklą siekiant skatinti kibernetinio saugumo technologijų plėtojimą bei diegimą ir suteikti ES pramonei papildomą postūmį inovacijų srityje pasaulinėje arenoje, kuriant naujos kartos ir didelių pokyčių technologijas, pavyzdžiui, dirbtinio intelekto, kvantinės kompiuterijos, blokų grandinės ir saugių skaitmeninių tapatybių srityje;

22. PABRĖŽIA, kad Kibernetinio saugumo kompetencijos centrų tinklas turi būti atviras visoms valstybėms narėms ir jų veikiantiems kompetencijos centrams ir ypač daug dėmesio skirti papildomumui, ir atsižvelgdama į tai ATKREIPIA DĖMESĮ į tai, kad planuojama įsteigti Europos kibernetinio saugumo ir mokslinių tyrimų centrą, kurio pagrindinė užduotis turėtų būti Kibernetinio saugumo kompetencijos centrų tinklo ir kitų ES agentūrų darbo papildomumo užtikrinimas ir šio tinklo bei tų agentūrų darbo dubliavimo vengimas;

23. PABRĖŽIA, kad Kibernetinio saugumo kompetencijos centrų tinklas turėtų spręsti įvarius klausimus – nuo mokslinių tyrimų iki pramonės srities – ir todėl turėtų prisidėti, *inter alia*, prie Europos strateginio savarankiškumo tikslo įgyvendinimo;“

24. Atsižvelgdama į pasiūlymą dėl Kibernetinio saugumo kompetencijos centrų tinklo sukūrimo, DAR KARTĄ PATVIRTINA, jog ES, pasitelkdama savo valstybes nares, turi suformuoti europinius pajėgumus, skirtus piliečiams, įmonėms ir vyriausybėms bendrojoje skaitmeninėje rinkoje siūlomuose gaminiuose ir paslaugose naudojamos kriptografijos tvirtumui įvertinti, kartu pripažindama, kad kriptografijos politika yra vienas svarbiausių nacionalinio saugumo aspektų ir todėl priklauso valstybių narių kompetencijai;

25. PRAŠO visų atitinkamų suinteresuotųjų subjektų padidinti investicijas į naujų technologijų taikymą kibernetinio saugumo srityje siekiant prisidėti prie kibernetinio saugumo užtikrinimo visuose Europos ekonomikos sektoriuose;

26. PABRĖŽIA patikimo ir koordinuojamo kibernetinio saugumo paslaugų teikimo ES institucijoms svarbą ir RAGINA KOMISIJĄ ir kitas ES institucijas toliau plėtoti Europos institucijų, įstaigų ir agentūrų Kompiuterinių incidentų tyrimo tarnybą (CERT-EU) vadovaujantis tais tikslais ir taip pat tam užtikrinti tinkamų išteklių;

27. PALANKIAI VERTINA raginimą pripažinti svarbų trečiųjų šalių saugumo srities mokslo darbuotojų vaidmenį išsiaiškinant esamų gaminių ir paslaugų silpnąsias vietas ir RAGINA valstybes narės dalytis geriausios praktikos pavyzdžiais dėl koordinuojamo silpnųjų vietų atskleidimo;

28. PABRĖŽIA visų atsakomybę kibernetinio saugumo srityje ir PRAŠO ES bei jos valstybių narių propaguoti skaitmeninius įgūdžius ir gebėjimą naudotis žiniasklaidos priemonėmis padedant naudotojams apsaugoti savo skaitmeninę informaciją internete ir didinti jų informuotumą apie riziką, susijusią su asmens duomenų skelbimu internete;

29. PALANKIAI VERTINA tai, kad bendrame komunikate akcentuojamas švietimas, kibernetinė higiena ir informuotumas valstybėse narėse ir ES;

30. RAGINA KOMISIJĄ greitai pateikti iniciatyvos dėl Kibernetinio saugumo kompetencijos centrų tinklo bei Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centro įsteigimo poveikio vertinimą ir ne vėliau kaip 2018 m. viduryje pasiūlyti atitinkamas teisines šios iniciatyvos įgyvendinimo priemones;

31. PRAŠO valstybių narių:

- informavimo kampanijose prioritetą teikti informuotumui apie kibernetinius nusikaltimus, o akademinėse, švietimo ir profesinio rengimo programose skatinti domėjimąsi kibernetiniu saugumu. Ypač daug dėmesio turėtų būti skiriama jaunimo švietimui ir skaitmeninių įgūdžių ugdymui, kad būtų parengti ateityje perspektyvūs specialistai, pasirengę iššūkiams saugumo, ekonomikos ir paslaugų srityse;

- daryti pažangą siekiant parengti specializuotas aukšto lygio kibernetinio saugumo programas, kad būtų panaikinta esama kibernetinio saugumo specialistų spraga ES;

- sukurti veiksmingą švietimo informacijos centrų bendradarbiavimo tinklą, globojamą ENISA. Švietimo informacijos centrų tinklas turėtų siekti stiprinti valstybių narių veiklos koordinavimą ir keitimąsi geriausios praktikos pavyzdžiais švietimo ir informuotumo kibernetinio saugumo klausimais, taip pat mokymo, pratybų ir gebėjimų stiprinimo srityse;

- apsvarstyti galimybes TIS direktyvos taisykles taikyti ir viešojo administravimo institucijoms, kurios dalyvauja ypatingos svarbos visuomeninėje arba ekonominėje veikloje, jei tai dar nėra numatyta nacionalinės teisės aktuose ir jei manoma, kad tai tikslinga, o su kibernetiniu saugumu susijusius mokymus rengti ir viešojo administravimo institucijose, atsižvelgiant į jų vaidmenį mūsų visuomenėje ir ekonomikoje.

II skyrius

ES GEBĖJIMŲ UŽKIRSTI KELIĄ KIBERNETINEI KENKIMO VEIKLAI, NUO JOS ATGRASYTI, JĄ NUSTATYTI IR Į JĄ REAGUOTI STIPRINIMAS

32. PABRĖŽIA, kad ypač pavojingas kibernetinis incidentas ar krizė galėtų būti pakankamas pagrindas valstybei narei pasinaudoti ES solidarumo sąlyga[15] ir (arba) savitarpio pagalbos sąlyga[16].

33. PALANKIAI VERTINA tai, kad buvo patvirtina bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistema, kuri prisideda prie konfliktų prevencijos, bendradarbiavimo ir stabilumo kibernetinėje erdvėje BUSP srityje nustatant priemones, įskaitant ribojamąsias priemones, kurios gali būti naudojamos siekiant užkirsti kelią kibernetinei kenkimo veiklai bei į ją reaguoti, ir RAGINA EIVT ir valstybes nares rengti reguliarias su šia sistema susijusias pratybas;

---

15 SESV 222 .

16 ES sutarties 42 straipsnio 7 dalis.

34. PABRĖŽIA, kad reikia veiksmingo ES lygmens atsako į didelio masto kibernetinius incidentus ir krizes, kartu atsižvelgiant į valstybių narių kompetenciją, o kibernetinio saugumo aspektas turi būti įtrauktas į esamus krizių valdymo mechanizmus ES lygmeniu[17]. Kad būtų pasiektas šis tikslas, RAGINA nuolat rengti su ES lygmens atsaku – nuo diplomatinio strateginio iki techninio atsako – į didelio masto kibernetinius incidentus susijusias pratybas, grindžiamas atitinkamomis sistemomis bei procedūromis, ir prireikus jas tobulinti[18];

35. PABRĖŽIA, kokie svarbūs gerai integruoti atsako ir įvairių bendruomenių, kurios yra itin svarbios kibernetinio saugumo užtikrinimui Europoje, be kita ko, atitinkamų ES tarnybų ir valstybių narių institucijų, keitimosi informacija mechanizmai. Tokie mechanizmai turės būti išbandyti ir patikrinti atliekant ES lygmens kibernetinio saugumo pratybas ir prireikus įforminti atitinkamuose susitarimuose;

36. ATKREIPIA DĖMESĮ Į galimybę išnagrinėti, jei Komisija pateiktų pasiūlymą dėl Reagavimo į kibernetinio saugumo krizes fondo įkūrimo siekiant papildyti valstybių narių esamas pastangas ir atsižvelgiant į turimus išteklius (visų pirma pagal ES daugiametę finansinę programą), padėti valstybėms narėms reaguoti į didelio masto kibernetinius incidentus ir švelninti jų padarinius, su sąlyga, kad valstybės narės prieš įvykstant incidentui bus įdiegusios apdairią kibernetinio saugumo sistemą, be kita ko, bus visapusiškai įgyvendinusios TIS direktyvą ir turės išsamias rizikos valdymo ir priežiūros sistemas nacionaliniu lygmeniu;

37. PRIPAŽĮSTA, jog stiprėja sąsajos tarp kibernetinio saugumo ir gynybos, ir RAGINA intensyvinti bendradarbiavimą kibernetinės gynybos srityje, be kita ko, skatinant civilinio ir karinio atsako į incidentus bendruomenių bendradarbiavimą, ir toliau stiprinti BSGP misijų ir operacijų kibernetinį saugumą;

---

17 Dok. C/2017/6100 final.
18 Dok. 9916/17 ir C/2017/6100 final.

38. PABRĖŽIA, kad gali reikėti visapusiškai pasinaudoti siūlomomis gynybos iniciatyvomis siekiant paspartinti tinkamų kibernetinių pajėgumų kūrimą Europoje, ir PRIPAŽĮSTA galimybes, kurių galėtų suteikti pagal nuolatinį struktūrizuotą bendradarbiavimą (PESCO) vykdomi kibernetinės gynybos projektai, jei tai laikytų reikalinga šiame bendradarbiavime dalyvaujančios valstybės narės, taip pat PRIPAŽĮSTA vaidmenį, kurį atlieka Europos gynybos pramoninė ir technologinė bazė (EGPTB) bei platesnė civilinė kibernetinio saugumo pramonės bazė suteikiant priemonių valstybės narėms apsaugoti savo su kibernetiniu saugumu susijusius saugumo bei gynybos interesus;

39. ATKREIPIA DĖMESĮ į Komisijos pateiktą pasiūlymą iki 2018 m. pabaigos sukurti mokymo ir švietimo kibernetinės gynybos klausimais platformą ir PABRĖŽIA, kad šia platforma turėtų būti išplėstos mokymo ir švietimo galimybės valstybėse narėse ir užtikrintas papildomumas kitų ES pastangų bei iniciatyvų, visų pirma Europos saugumo ir gynybos koledžo ir Europos gynybos agentūros veiklos, atžvilgiu;

40. RAGINA ES ir jos valstybes nares reaguoti į grėsmę, kurią kelia intelektinės nuosavybės, įskaitant komercines paslaptis ar kitą konfidencialią verslo informaciją, vagystės pasinaudojant IRT, siekiant suteikti konkurencinį pranašumą bendrovėms ar komerciniams sektoriams;

41. PRIPAŽĮSTA, kad reikia kovoti su nusikaltimais kibernetinėje erdvėje, įskaitant nusikaltimus tamsiajame internete, vaikų seksualinį išnaudojimą internete, sukčiavimą negrynosiomis mokėjimo priemonėmis ir jų klastojimą, visų pirma siekiant surinkti išsamesnės žvalgybos informacijos, vykdant jungtinius tyrimus ir dalijantis operatyvine pagalba;

42. PALANKIAI VERTINA ES ir jos valstybių narių darbą siekiant spręsti problemas, kurias kelia sistemos, suteikiančios nusikaltėliams ir teroristams galimybę bendrauti kompetentingoms institucijoms neprieinamais kanalais, PABRĖŽIA, jog dirbant šį darbą reikia atsiminti, kad tvirtas ir patikimas šifravimas yra itin svarbus kibernetiniam saugumui, pasitikėjimui bendrąja skaitmenine rinka ir žmogaus teisių bei pagrindinių laisvių užtikrinimui;

43. PABRĖŽIA, jog svarbu teisėsaugą aprūpinti priemonėmis, suteikiančiomis galimybę nustatyti kibernetinius nusikaltimus, juos tirti ir už juos patraukti atsakomybėn, kad kibernetinėje erdvėje padaryti nusikaltimai neliktų nepastebėti, o jų vykdytojai neliktų nenubausti, ir PALANKIAI VERTINA Europos teisminio kovos su kibernetiniais nusikaltimais tinklo indėlį kovojant su nusikalstamumu užtikrinant teisminių institucijų bendradarbiavimą;

44. PABRĖŽIA, kad svarbu užtikrinti suderintą ES poziciją siekiant efektyviai formuoti Europos ir pasaulinius interneto valdymo sprendimus įvairius suinteresuotuosius subjektus apimančioje bendruomenėje, pavyzdžiui, užtikrinant greitai prieinamas ir tikslias IP adresų ir domeno vardų duomenų bazes WHOIS, kad būtų užtikrinti teisėsaugos pajėgumai ir apsaugoti viešieji interesai;

45. PABRĖŽIA, kad svarbu pereiti prie IPv6 interneto protokolo, kuris yra būtinas siekiant dideliu mastu plėtoti daiktų internetą ir gerinti kibernetinėje erdvėje padarytų nusikaltimų priskyrimo galimybes;

46. RAGINA tęsti šiuo metu vykdomą darbą, susijusį su tarpvalstybine prieiga prie elektroninių įrodymų, duomenų saugojimo klausimu ir problemomis, kurių baudžiamajame procese kyla dėl sistemų, suteikiančių nusikaltėliams ir teroristams galimybę bendrauti kompetentingoms institucijoms neprieinamais kanalais, nepamirštant būtinybės gerbti žmogaus bei pagrindines laisves ir užtikrinti duomenų apsaugą;

47. RAGINA Komisiją:

- ne vėliau kaip 2017 m. gruodžio mėn. pateikti pažangos ataskaitą dėl praktinių priemonių, skirtų tarpvalstybinei prieigai prie elektroninių įrodymų gerinti, įgyvendinimo;
- 2018 m. pradžioje pateikti pasiūlymą dėl teisėkūros procedūra priimamo akto, kuriuo būtų siekiama pagerinti tarpvalstybinę prieigą prie elektroninių įrodymų;

48. PRAŠO Europolo, ENISA ir Eurojusto:

- toliau stiprinti tiek tarpusavio bendradarbiavimą kovojant su kibernetiniu nusikalstamumu, tiek su kitais atitinkamais suinteresuotaisiais subjektais, įskaitant reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) bendruomenę, Interpolą, privatųjį sektorių ir akademinę bendruomenę, užtikrinant sinergiją ir papildomumą, pagal jų atitinkamus įgaliojimus ir kompetenciją;

- kartu su valstybėmis narėmis padėti parengti suderintą požiūrį, skirtą ES teisėsaugos atsakui į didelio masto kibernetinius incidentus ir krizes, siekiant papildyti atitinkamose sistemose nustatytas procedūras[19];

49. RAGINA ES ir jos valstybes nares tęsti darbą:

- siekiant pašalinti kliūtis, trukdančias tirti nusikaltimus, veiksmingai vykdyti baudžiamąjį teisingumą kibernetinėje erdvėje ir stiprinti tarptautinį bendradarbiavimą bei veiksmų koordinavimą kovojant su nusikaltimais kibernetinėje erdvėje;

- siekiant išspręsti problemas, kurias kelia anonimizavimo technologijos, kartu nepamirštant, jog tvirtas ir patikimas šifravimas yra itin svarbus kibernetiniam saugumui ir pasitikėjimui bendrąja skaitmenine rinka;

- siekiant suformuoti interneto valdymo sprendimus, darančius poveikį teisėsaugos pajėgumams kovoti su nusikaltimais kibernetinėje erdvėje.

[19] Dok. 9916/17 ir C/2017/6100 final.

III skyrius

TARPTAUTINIO BENDRADARBIAVIMO STIPRINIMAS SIEKIANT ATVIROS, LAISVOS, TAIKIOS IR SAUGIOS PASAULINĖS KIBERNETINĖS ERDVĖS

50. PRIPAŽĮSTA, kad kibernetinio saugumo užtikrinimas yra pasaulinis uždavinys, reikalaujantis veiksmingo visuotinio visų subjektų bendradarbiavimo, ir PRIPAŽĮSTA, kad ypač daug dėmesio reikia skirti demokratinių vertybių ir atviros, laisvos, taikios bei saugios pasaulinės kibernetinės erdvės principų apsaugai, ir atsižvelgdama į tai

51. RAGINA ES ir jos valstybes nares propaguoti strateginės sistemos, skirtos konfliktų prevencijai, bendradarbiavimui ir stabilumui kibernetinėje erdvėje, grindžiamos galiojančios tarptautinės teisės, visų pirma JT Chartijos visa jos apimtimi, taikymu, sukūrimą, universalių atsakingo valstybių elgesio normų rengimą bei įgyvendinimą ir regionines valstybių pasitikėjimo stiprinimo priemones;

52. PRIPAŽĮSTA Jungtinių Tautų vaidmenį toliau plėtojant atsakingo valstybių elgesio kibernetinėje erdvėje normas ir primena, kad Jungtinių Tautų Vyriausybių ekspertų grupės diskusijų išvadose jau ne vienus metus yra išdėstomas sutartas normų ir rekomendacijų rinkinys[20], kuriam ne kartą yra pritarusi Generalinė Asamblėja ir kurį valstybės turėtų naudoti kaip atsakingo valstybių elgesio kibernetinėje erdvėje pagrindą;

53. PRIPAŽĮSTA, kad tose atsakingo valstybių elgesio normose nustatyta, jog valstybės neturėtų sąmoningai leisti, kad jų teritorijoje būtų vykdomi tarptautiniu mastu neteisėti veiksmai, turėtų reaguoti į atitinkamus pagalbos prašymus, pateiktus kitos valstybės, kurios ypatingos svarbos infrastruktūros atžvilgiu vykdomi kenkėjiški IRT veiksmai, kylantys iš jų teritorijos, ir kad valstybės turėtų imtis atitinkamų priemonių savo ypatingos svarbos infrastruktūrai apsaugoti nuo IRT grėsmių;

54. PRIPAŽĮSTA bendras kibernetines grėsmes ir pavojus, su kuriais susiduria ES, NATO ir jų atitinkamos valstybės narės, ir PAKARTOJA, kad svarbu tęsti ES ir NATO bendradarbiavimą kibernetinio saugumo ir gynybos srityje, visapusiškai laikantis ES įtraukties, abipusiškumo ir sprendimų priėmimo autonomiškumo principų ir jos 2016 m. gruodžio 6 d. išvadų dėl Europos Vadovų Tarybos pirmininko, Europos Komisijos pirmininko ir Šiaurės Atlanto sutarties organizacijos generalinio sekretoriaus bendro pareiškimo įgyvendinimo[20];

55. RAGINA ES ir jos valstybes nares remti ir skatinti regioninių pasitikėjimo stiprinimo priemonių, kurios yra vienas iš esminių elementų siekiant stiprinti bendradarbiavimą bei skaidrumą ir mažinti konfliktų riziką, plėtojimą. Įgyvendinant kibernetinio saugumo pasitikėjimo stiprinimo priemones ESBO ir kitose regioninėse struktūrose padidės valstybių elgesio nuspėjamumas ir bus toliau prisidedama prie kibernetinės erdvės stabilizavimo;

56. DAR KARTĄ PATVIRTINA, kad ES toliau laikysis savo pagrindinių vertybių gindama žmogaus teises ir pagrindines laisves, remdamasi ES žmogaus teisių gairėmis dėl saviraiškos laisvės internete. ES taip pat pabrėžia, jog svarbu, kad į interneto valdymo procesą būtų įtraukti visi suinteresuotieji subjektai, įskaitant akademinę bendruomenę, pilietinę visuomenę ir privatųjį sektorių;

57. RAGINA ES ir jos valstybes nares propaguoti kibernetinių pajėgumų plėtojimą trečiosiose valstybėse, ypatingą prioritetą teikiant toms ES kaimyninėms ir besivystančioms šalims, kuriose sparčiai plėtojama ryšių infrastruktūra, siekiant kovoti su kibernetiniu nusikalstamumu ir stiprinti kibernetinį atsparumą, vadovaujantis pagrindinėmis ES vertybėmis. Siekiant suintensyvinti ES pastangas šioje srityje, turėtų būti sukurtas ES kibernetinių pajėgumų stiprinimo tinklas ir parengtos ES kibernetinių pajėgumų stiprinimo gairės – jie turėtų papildyti jau esamus mechanizmus ir struktūras;

[20] Dok. 15283/16.

58. PABRĖŽIA pažangą, kurią padarė ES ir NATO bendradarbiaudamos kibernetinės gynybos ir saugumo srityje, plėtodamos mokymą, švietimą ir koncepcijas, vengiant bereikalingo pastangų dubliavimosi tais atvejais, kai reikalavimai iš dalies sutampa, taip pat skatindamos sąveikumą nustatant kibernetinės gynybos reikalavimus bei standartus, ir PRAŠO tęsti bendradarbiavimą vykdant kibernetinės gynybos pratybas (personalo lygmeniu) ir dalytis gerosios patirties pavyzdžiais krizių valdymo srityje, kartu vengiant bereikalingo pastangų dubliavimosi tais atvejais, kai reikalavimai iš dalies sutampa, visapusiškai laikantis ES pratybų politikos ir ES įtraukties, abipusiškumo ir sprendimų priėmimo autonomiškumo principų;

59. PRIPAŽĮSTA, kad Europos Tarybos konvencija dėl elektroninių nusikaltimų (Budapešto konvencija) yra veiksmingas teisinis standartas, kuriuo gali būti grindžiami nacionalinės teisės aktai dėl kibernetinio nusikalstamumo. RAGINA visas šalis parengti tinkamas nacionalines teisines sistemas ir bendradarbiauti naudojantis šia esama tarptautine sistema, sukurta pagal Budapešto konvenciją;

60. PRIMENA rezultatus, pasiektus vedant dvišalius ES dialogus kibernetiniais klausimais, ir ragina toliau dėti pastangas siekiant palengvinti bendradarbiavimą su trečiosiomis valstybėmis kibernetinio saugumo srityje;

61. PRIMENA, kad ES turi tvirtą ir teisiškai privalomą eksporto kontrolės mechanizmą, grindžiamą sprendimais, parengtais pagal tarptautinius ginklų neplatinimo režimus, ir juos taikant įgytos geriausios praktikos pavyzdžiais, ir ATKREIPIA DĖMESĮ į Taryboje vykstančias diskusijas siekiant rasti geriausius tolesnio šių mechanizmų veikimo tobulinimo būdus, ir PRAŠO valstybių narių laikantis atitinkamų tarptautinių eksporto kontrolės režim*ų* (pvz., Vasenaro susitarimo) toliau spręsti klausimus, susijusius su naujoviškų technologijų taikymu ypatingos svarbos kibernetinio saugumo srityse, kad būtų užtikrinta veiksminga būsimų ypatingos svarbos kibernetinio saugumo technologijų kontrolė;

62. Šios išvados, priimtos vadovaujantis 2017 m. spalio 19 d. Europos Vadovų Tarybos išvadomis[21], bus įgyvendinamos pagal veiksmų planą, kurį Taryba turi priimti iki 2017 m. pabaigos. Veiksmų planas turėtų būti dinamiškas dokumentas, kurį Taryba reguliariai peržiūrės ir atnaujins.

[21] Dok. EUCO 14/17.