Europos Sąjungos
Taryba

Briuselis, 2023 m. gegužės 22 d.
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Dalykas:	Tarybos išvados dėl ES kibernetinės gynybos politikos

Delegacijoms pridedamos Tarybos išvados dėl ES kibernetinės gynybos politikos, patvirtintos 2023 m. gegužės 22 d. surengtame Tarybos posėdyje.

Tarybos išvados dėl ES kibernetinės gynybos politikos

1. Remdamasi 2014 m. kibernetinės gynybos politikos metmenimis ir 2018 m. atnaujinta jų redakcija, Taryba palankiai vertina plataus užmojo bendrą komunikatą dėl ES kibernetinės gynybos politikos, kad būtų toliau investuojama į mūsų šiuolaikiškas ir sąveikias ginkluotąsias pajėgas, pažangiąsias technologijas, pažangiausiais metodais grindžiamus kibernetinės gynybos pajėgumus ir stiprinamos partnerystės siekiant įveikti bendrus iššūkius. Didėjant priklausomybei nuo skaitmeninių technologijų, kibernetinė erdvė tapo strateginės konkurencijos sritimi. Taigi, itin svarbu išlaikyti atvirą, laisvą, stabilią ir saugią kibernetinę erdvę. Naudojimasis kibernetinėmis operacijomis, įgalinusiomis ir lydinčiomis neišprovokuotą ir nepateisinamą Rusijos agresijos karą prieš Ukrainą, daro poveikį pasauliniam stabilumui ir saugumui, kelia didelę eskalacijos riziką ir dar labiau padidina ir taip didelį su ginkluotais konfliktais nesusijusios kibernetinės kenkimo veiklos augimą pastaraisiais metais.

2. Dėl karo Ukrainoje atsirado naujas strateginis kontekstas ir pasitvirtino, kad ES, jos valstybėms narėms ir jų partneriams reikia toliau stiprinti ES atsparumą kovojant su kibernetinėmis grėsmėmis ir didinti mūsų bendrą kibernetinį saugumą bei kibernetinę gynybą nuo piktavališko elgesio ir agresijos aktų kibernetinėje erdvėje. Bendras komunikatas dėl ES kibernetinės gynybos politikos yra ženklas, jog esame pasiryžę imtis neatidėliotinų ir ilgalaikių priemonių, kad būtų užtikrina veiksmų laisvė kibernetinėje erdvėje ir duodamas atsakas grėsmę keliantiems subjektams, siekiantiems, bet kita ko, įsilaužti į ES ir jos partnerių tinklus ir informacines sistemas, juo sutrikdyti ar sunaikinti. Šis bendras komunikatas, papildantis ES kibernetinio saugumo strategiją ir atitinkantis Strateginį kelrodį, yra reikšmingas žingsnis kuriant visą spektrą apimantį ES požiūrį į atsparumą, reagavimą, konfliktų prevenciją, bendradarbiavimą ir stabilumą kibernetinėje erdvėje. Atsižvelgdama į tai, Taryba pabrėžia, jog reikia tinkamų ir darnių ES, jos valstybių narių ir jų partnerių reagavimo priemonių, taip pat rengiantis ES kibernetinio saugumo diplomatijos priemonių rinkinio įgyvendinimo gairių peržiūrai, kuri taps dar vienu svarbiu žingsniu pirmyn plėtojant ES kibernetinio saugumo būklę.

3. Taryba pabrėžia, kad neseniai įvykdyti kibernetiniai išpuoliai prieš Europos ypatingos svarbos infrastruktūrą, sparčiai kintanti kibernetinių grėsmių panorama ir spartus technologinės plėtros tempas taip pat rodo, jog reikia stiprinti civilinį ir karinį koordinavimą bei bendradarbiavimą, kartu akcentuodama, kad tarp civilinės ir karinės bendruomenių nėra hierarchijos.

   ES kibernetinės gynybos politika sudaro ES ir jos valstybėms narėms sąlygas stiprinti savo gebėjimą apsaugoti, aptikti, apsiginti ir atgrasyti tinkamai naudojantis visomis civilinei ir karinei bendruomenėms prieinamomis gynybos priemonėmis platesniam ES saugumui ir gynybai užtikrinti laikantis tarptautinės teisės, įskaitant žmogaus teisių teisę ir tarptautinę humanitarinę teisę.

4. Nors kiekviena valstybė narė išlaiko išimtinę atsakomybę už nacionalinį saugumą, be kita ko, kibernetinėje srityje, kaip nurodyta ES sutarties 4 straipsnio 2 dalyje, Taryba pabrėžia, kad reikia individualiai ir kolektyviai daug investuoti į didesnį atsparumą ir viso spektro gynybinių kibernetinės gynybos pajėgumų diegimą ir pasinaudoti ES bendradarbiavimo sistemomis bei finansinėmis paskatomis. Taryba pabrėžia, kad reikia toliau stiprinti valstybių narių ir ES institucijų, įstaigų ir agentūrų veiksmus siekiant kibernetinėje erdvėje apsaugoti Sąjungą, mūsų piliečius, ES institucijas, įstaigas ir agentūras ir BSGP misijas bei operacijas. Be to, ji pabrėžia, kad svarbu užtikrinti ES atsparumą kibernetinėje erdvėje plėtojant kibernetinės gynybos pajėgumus ir stiprinant bendradarbiavimą su patikima privačia ekosistema.

I. **Veikti išvien siekiant užtikrinti tvirtesnę kibernetinę gynybą**

5. Taryba pakartoja, jog norint didinti pasitikėjimą, kuris yra būtinas toliau plėtojant ES kibernetinio saugumo krizių valdymo sistemą vadovaujantis Taryboje parengtomis Kibernetinių krizių valdymo veiksmų gairėms, svarbu, kad procesas būtų laipsniškas, skaidrus ir įtraukus. Taryba pakartoja, kad reikia toliau didinti mūsų gebėjimą apsisaugoti nuo kibernetinių išpuolių, juos aptikti, nuo jų apsiginti ir atgrasyti gerinant informuotumą apie padėtį, stiprinant gebėjimus, plėtojant pajėgumus, vykdant mokymą bei pratybas, didinant atsparumą ir ryžtingai reaguojant į kibernetinius išpuolius prieš ES, jos valstybes nares ir ES institucijas, įstaigas bei agentūras, BSGP misijas ir operacijas naudojantis visomis tinkamomis priemonėmis. Taryba ragina vyriausiąjį įgaliotinį ir Komisiją tai darant mažinti sudėtingumą kibernetinėje srityje, vengti bereikalingo dubliavimo ir užtikrinti bendradarbiavimą bei sinergiją su esamomis iniciatyvomis. Turi būti stiprinamas ES ir valstybėse narėse veikiančių ir joms priklausančių kibernetinės gynybos subjektų vidaus bendradarbiavimas ir koordinavimas, taip pat karinės ir civilinės kibernetinių bendruomenių ir viešosios ir patikimos privačiosios ekosistemų bendradarbiavimas ir koordinavimas. Šiomis aplinkybėmis valstybės narės raginamos toliau nagrinėti ir stiprinti nacionalinius civilinio ir karinio koordinavimo mechanizmus, palengvinti bendrą savanorišką dalijimąsi informacija, dalytis įgyta patirtimi, prisidėti prie sąveikių standartų rengimo ir atlikti rizikos vertinimus bei rengti rizikos scenarijus, taip pat bendras pratybas, ypač Europos lygmeniu, visiškai laikantis Direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2) nuostatų.

6. Pripažindama pastangas toliau didinti Sąjungos atsparumą taikant TIS 2 ir Direktyvą dėl ypatingos svarbos subjektų atsparumo, Taryba pakartoja savo rekomendaciją dėl ES masto suderinto požiūrio į ypatingos svarbos infrastruktūros objektų atsparumo didinimą[1]. Ji ragina imtis priemonių, kuriomis būtų toliau didinamas ypatingos svarbos subjektų, infrastruktūros, skaitmeninių produktų ir paslaugų atsparumas, kartu pažymėdama, kad svarbiausias žingsnis tebėra tinkamas TIS 2 įgyvendinimas. Nors atsakomybė už šias priemones iš esmės yra civilinė, jomis taip pat padedama stiprinti kibernetinę gynybą. Atsižvelgiant į tai, ES institucijos, įstaigos ir agentūros, taip pat valstybės narės raginamos remti tolesnį naujų ir esamų ES koordinavimo mechanizmų, rizikos vertinimų, įvertinimų ir scenarijų, bendro savanoriško dalijimosi informacija ir pratybų plėtojimą bei diegimą tokiu būdu, kad būtų kuriama pridėtinė vertė ir išvengiama bereikalingo dubliavimo su esamomis iniciatyvomis.

7. Kad būtų toliau didinamas pasitikėjimas, stiprinamas bendradarbiavimas ir palengvinamas savalaikis dalijimasis informacija apie reikšmingus ir didelio masto kibernetinius incidentus, darančius poveikį gynybos sistemoms, Taryba palankiai vertina iniciatyvą toliau plėtoti ES kibernetinės gynybos vadų konferenciją, kurią rengs kiekviena ES Tarybai pirmininkaujanti valstybė narė, padedant Europos gynybos agentūrai (EGA) ir dalyvaujant Europos išorės veiksmų tarnybai (EIVT). Taryba ragina visas valstybes nares dalyvauti šiuose susitikimuose. Kad būtų didinamas ES atsparumas didelio masto kibernetinio saugumo incidentams, Taryba prašo ES ryšių palaikymo dėl kibernetinių krizių organizacinio tinklo (EU-CyCLONe) ir ES kibernetinės gynybos vadų konferencijos nustatyti, kokiais būdais būtų galima bendradarbiauti ir pasinaudoti bendra karine ir civiline perspektyva.

[1] Pasiūlymas dėl Tarybos rekomendacijos dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros objektų atsparumo didinimą, COM(2022) 551.

8. Kad būtų skatinamas tvirtesnis ir labiau koordinuotas atsakas ES lygmeniu, Taryba palankiai vertina ES operatyvinio karinių kompiuterinių incidentų tyrimo tarnybų tinklo (MICNET) įsteigimą, ir tikisi, kad iki 2024 m. vidurio bus sukurti pradiniai operatyviniai pajėgumai, kuriais bus stiprinamas dalyvaujančių valstybių narių keitimasis technine informacija apie gynybos sistemas veikiančius kibernetinius incidentus. Taryba ragina visas valstybes nares dalyvauti MICNET veikloje, kad būtų užtikrintas tinklo veiksmingumas. Be to, Taryba prašo valstybių narių remtis patirtimi, įgyta Reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinkle, ir primygtinai ragina tinkamu laiku sukurti veiksmingą abiejų tinklų bendradarbiavimo ir koordinavimo mechanizmą, visapusiškai atsižvelgiant į kiekvieno subjekto valdymo mechanizmus ir naudotojus.

9. Intensyvėjant valstybinių ir nevalstybinių veikėjų vykdomai kibernetinei kenkimo veiklai, nukreiptai prieš ES BSGP misijas ir operacijas, Taryba prašo ES ir jos valstybių narių stiprinti savo pajėgumus ginti ir apsaugoti BSGP misijas ir operacijas. Šiuo atžvilgiu Taryba palankiai vertina tikslus toliau daryti pažangą ES karinių tinklų ir struktūrų apsaugos srityje, laikantis, be kita ko, ES karinės vizijos ir strategijos dėl kibernetinės erdvės kaip operacijų srities[2].

[2] Dok. EIVT(2021) 706 REV4

10. Taryba primena 2022 m. gegužės mėn. Tarybos išvadas[3] ir poreikį investuoti į mūsų savitarpio pagalbą pagal ES sutarties 42 straipsnio 7 dalį, taip pat SESV 222 straipsnyje nustatytą solidarumo sąlygą. Taryba pabrėžia, kad svarbu toliau gilinti ES ir jos valstybių narių bendrą sutarimą dėl 42 straipsnio 7 dalies įgyvendinimo, be kita ko, sudėtingų scenarijų, apimančių kibernetinį išpuolį, atveju, laikantis atitinkamų tarptautinės teisės principų. Ji palankiai vertina galimybę, gavus aiškų atitinkamos (-ų) valstybės (-ių) narės (-ių) prašymą, teikti ES paramą kibernetinio išpuolio atveju, nedarant poveikio specifiniam tam tikrų valstybių narių saugumo ir gynybos politikos pobūdžiui.

11. Taryba akcentuoja pažangą, padarytą vykdant PESCO projektą dėl Greitojo reagavimo į kibernetinius incidentus komandų ir savitarpio pagalbos kibernetinio saugumo srityje (CRRT), ir šių pajėgumų pasirengimą gavus prašymą tenkinti valstybių narių ir ES poreikius, remiant BSGP misijas bei operacijas ir teikiant pagalbą ES partneriams. Taryba palankiai vertina PESCO CRRT pajėgumų, nacionalinių reagavimo į kibernetinius incidentus grupių ir, kai tinkama, papildomų reagavimo į incidentus pajėgumų, tokių kaip Strateginiame kelrodyje numatytos būsimos greitojo reagavimo į hibridines grėsmes grupės, tolesnį plėtojimą, be kita ko, skatinant jų koordinavimą ir bendradarbiavimą ES lygmeniu.

[3] Tarybos išvados dėl Europos Sąjungos pozicijos kibernetiniais klausimais parengimo, 2022 m. gegužės 23 d., dok. 9364/22.

12. Taryba palankiai vertina darbą, atliktą vykdant PESCO projektą dėl Kibernetinės ir informacinės srities koordinavimo centro (CIDCC), kurio tikslas – suteikti karinius pajėgumus, kad būtų galima rinkti ir analizuoti informaciją, susijusią su bendra operatyvine kibernetine padėtimi. Be to, Taryba palankiai vertina pasiūlymą nuo 2025 m. integruoti koncepcijos įrodymą, jei koncepcija pasiteisins kaip informacijos koordinavimo centras, į ES kibernetinės gynybos koordinavimo centrą (EUCDCC), taip gerinant visų pirma ES BSGP misijos ir operacijų vadų veiklos koordinavimą bei informuotumą apie padėtį, taip pat stiprinant platesnę ES vadovavimo ir kontrolės struktūrą. Taryba ragina vyriausiąjį įgaliotinį pateikti EUCDCC įsteigimo koncepciją ir veiksmų gaires, remiantis panašių tarptautinių subjektų patirtimi, nustatant reikiamus išteklius, vengiant bereikalingo dubliavimo ir siekiant papildomumo su platesne ES kibernetinio saugumo sistema.

13. Taryba pabrėžia strateginio bendradarbiavimo žvalgybos srityje, susijusio su kibernetinėmis grėsmėmis ir veikla, svarbą ir prašo valstybių narių per savo kompetentingas institucijas toliau prisidėti prie EU INTCEN, ES karinio štabo žvalgybos direktorato ir valstybių narių darbo Bendro žvalgybinės informacijos analizės centro (SIAC) kontekste. Taryba taip pat pabrėžia, jog svarbu stiprinti mūsų kibernetinės žvalgybos pajėgumus, kad būtų didinamas mūsų kibernetinis atsparumas, gerinamas reagavimas ir būtų teikiama veiksminga parama mūsų civilinėms ir karinėms BSGP misijoms ir operacijoms, taip pat mūsų ginkluotosioms pajėgoms ir SIAC pajėgumams kibernetinėje srityje, remiantis valstybių narių savanoriškai teikiama žvalgybos informacija ir nedarant poveikio jų kompetencijai.

14. Taryba atkreipia dėmesį į Europos Komisijos kibernetinės padėties ir analizės centrą, kurio tikslas – didinti Komisijos informuotumą apie padėtį. Taryba pabrėžia, kad svarbu užmegzti abipusiškai naudingą šio centro ir kitų ES institucijų, įstaigų ir agentūrų, visų pirma ENISA ir CERT-EU, bendradarbiavimą. Taryba akcentuoja, kad plėtojant informuotumą apie padėtį svarbu užtikrinti glaudų bendradarbiavimą su ES bendradarbiavimo tinklais, taip pat laikytis konfidencialumo. Taryba pažymi, kad reikia ES lygmeniu stiprinti bendrą informuotumą apie padėtį ir toliau plėtoti ES kibernetinio saugumo krizių valdymo sistemą, kartu vengiant bereikalingo pastangų dubliavimo.

15. Taryba primena, kad norint užtikrinti parengtį ir veiksmingumą, labai svarbūs yra švietimas, mokymas ir pratybos kibernetinėje srityje, ir palankiai vertina nacionalinę veiklą, taip pat veiklą, kurią ES vykdo per Europos saugumo ir gynybos koledžą (ESGK), EGA, ENISA ir vykdomus PESCO projektus, tokius kaip Kibernetinių poligonų susiejimas ir ES kibernetinis mokslinės kompetencijos ir inovacijų centras (CAIH). Siekdama toliau stiprinti šias pastangas, Taryba laukia, kol bus sukurtas EGA bendrasis projektas *CyDef-X* kibernetinės gynybos pratyboms sinchronizuoti ir remti. Taryba ragina EGA, glaudžiai bendradarbiaujant su valstybėmis narėmis ir EIVT, išnagrinėti, kaip vykdant *CyDef-X* galėtų būti toliau remiamos tokios pratybos kaip CYBER PHALANX, be kita ko, dėl savitarpio pagalbos pagal ES sutarties 42 straipsnio 7 dalį ir SESV 222 straipsnyje nustatytą solidarumo sąlygą, taip pat bendradarbiaujant su Komisija ir ENISA, kiek tai susiję su civilinėmis pratybomis. Be to, Taryba ragina *CyDef-X* kontekste naudoti ir toliau plėtoti esamą kibernetinės gynybos testavimo ir pratybų aplinką, tokią kaip Kibernetinių poligonų susiejimas. Taryba pabrėžia, kad, norint užtikrinti spartų ir veiksmingą sprendimų priėmimo kibernetinių krizių atvejais procesą, svarbu reguliariai rengti teorinio modeliavimo pratybas, skirtas valstybių narių sprendimų priėmimo lygmeniui.

16. Taryba atkreipia dėmesį į pasiūlymą dėl Kibernetinio solidarumo akto ir ketinimą stiprinti pajėgumus nustatyti kibernetines grėsmes ir incidentus ES ir į juos reaguoti. Taryba pabrėžia, kad pasiūlymai šioje srityje gali būti veiksmingi tik juos suderinus su valstybių narių krizių valdymo sistemomis ir poreikiais. Taryba pabrėžia, jog svarbu, kad ypatingos svarbos infrastruktūros galimo pažeidžiamumo testavimas, kai jis laikomas naudingu, pagal nacionalinę kompetenciją būtų vykdomas atsižvelgiant į turimus ES rizikos vertinimus.

17. Taryba atkreipia dėmesį į Komisijos pasiūlymą sukurti Reagavimo į kibernetinio saugumo krizes mechanizmą, kuriuo galėtų būti remiama galimybė naudotis patikimų privačių paslaugų teikėjų kibernetinio saugumo paslaugomis – valstybėms narėms paprašius joms būtų padedama didelio masto kibernetinio saugumo incidentų atveju,– kartu pabrėždama, kad reikia proporcingai plėsti Europos kibernetinio saugumo pramonę padedant ECCC, nes tai yra esminis šio mechanizmo veikimo užtikrinimo ramstis. Taryba pabrėžia, kad kiekviena valstybė narė atlieka pagrindinį vaidmenį stebint ir vertinant jų nacionalinius poreikius.

II. **Apsaugoti ES gynybos ekosistemą**

18. Taryba primena raginanti valstybes nares toliau plėtoti savo pajėgumus vykdyti kibernetinės gynybos operacijas, įskaitant, kai tinkama, proaktyvias gynybos priemones, kurių tikslas yra apsisaugoti nuo kibernetinių išpuolių, juos aptikti, nuo jų gintis ir atgrasyti. Atsižvelgdama į tai, kad TIS 2 netaikoma gynybos srityje veiklą vykdantiems viešojo administravimo subjektams, Taryba prašo EGA, atitinkamai remiant Komisijai ir EIVT, padėti valstybėms narėms parengti TIS 2 įkvėptas teisiškai neprivalomas savanoriškas rekomendacijas siekiant padidinti gynybos bendruomenės kibernetinį saugumą ir prašo visų valstybių narių aktyviai dalyvauti dedant šias pastangas. Šiose rekomendacijose turėtų būti atsižvelgiama į kitose sistemose dedamas panašias pastangas.

19. Kaip pripažinta Strateginiame kelrodyje, ES pajėgumas imtis veiksmų priklauso nuo jos gebėjimo sumažinti savo kibernetinės gynybos pajėgumų ir tiekimo grandinių strateginę priklausomybę, taip pat nuo pažangiųjų kibernetinės gynybos technologijų plėtojimo ir įvaldymo. Tai apima Europos gynybos technologinės ir pramoninės bazės (EGTPB) stiprinimą visoje ES ir jos gebėjimą abipusiškumo pagrindu bendradarbiauti su bendraminčiais partneriais visame pasaulyje, kad būtų užtikrinta abipusė nauda. Todėl Taryba ragina kibernetinio saugumo ir kibernetinės gynybos pramonės atstovus glaudžiai bendradarbiauti, kad būtų sukurta sinergija siekiant plėtoti ir užtikrinti viso spektro kibernetinės gynybos pajėgumus. Taryba prašo Komisijos, kai tinkama, glaudžiai bendradarbiaujant su ECCC, toliau remti stiprios, lanksčios, pasauliniu mastu konkurencingos ir novatoriškos Europos kibernetinės gynybos pramoninės ir technologinės bazės, įskaitant mažąsias ir vidutines įmones (MVĮ), kūrimą, toliau investuojant ir imantis politikos priemonių.

20. Atsižvelgdama į kibernetinės gynybos pajėgumų sąveikumo ir bendrumo svarbą, be kita ko, kiek tai susiję su bendradarbiaujamuoju naujos kartos kibernetinės gynybos pajėgumų plėtojimu, Taryba prašo EGA ir ES karinio štabo parengti ES kibernetinės gynybos sąveikumo reikalavimų rinkinį, kuris būtų grindžiamas esamais principais, procesais ir standartais, visų pirma nustatytais Šiaurės Atlanto sutarties organizacijos (NATO) sistemoje, ir būtų su jais suderinamas. Be to, Taryba prašo valstybių narių, glaudžiai bendradarbiaujant su visais atitinkamais suinteresuotaisiais subjektais, įskaitant atitinkamai Europos standartizacijos organizacijas ir NATO, Europos gynybos standartizacijos komitete išnagrinėti, ar galėtų būti reikalingi konkretūs savanoriški gynybos sistemų standartai.

21. Taryba palankiai vertina Komisijos pastangas pateikti planą, kuriuo siekiama skatinti civilinio kibernetinio saugumo ir kibernetinės gynybos reikmėms naudoti esamus standartus, taip pat parengti naujus savanoriškus standartus. Taryba pabrėžia, kad, kai tinkama, reikia suderinti kibernetinio saugumo ir kibernetinės gynybos standartus. Taryba pripažįsta, kad tokie savanoriški standartai galėtų būti naudingi ES kibernetinio saugumo ir kibernetinės gynybos pramonei, ir ragina civilines ir gynybos standartizacijos įstaigas glaudžiau bendradarbiauti.

22. Taryba ragina skubiai parengti rekomendacijas, grindžiamas esamų saugios komunikacijos kibernetinėje srityje priemonių sąrašu, kurį parengė Komisija ir atitinkamos institucijos. Kai įmanoma, rekomendacijos turėtų būti suderintos su esamomis dalijimosi informacija iniciatyvomis ir jose taip pat turėtų būti atsižvelgiama į besiformuojančių ir perversminių technologijų keliamą riziką dabartiniams šifravimo metodams.

23. Be to, Taryba palankiai vertina atliktą pirminį darbą, susijusį su rizikos vertinimu ir scenarijais, kuriuos Tarybos prašymu rengia Komisija, vyriausiasis įgaliotinis ir TIS bendradarbiavimo grupė, pirmiausia, kiek tai susiję su energetikos ir telekomunikacijų sektoriais. Taryba pripažįsta, kad taip pat rengiami tiksliniai ES ryšių infrastruktūros ir tinklų kibernetinio saugumo rizikos vertinimai. Taryba pakartoja, kad nepaprastai svarbu, jog valstybės narės, taip pat ES institucijos, įstaigos ir agentūros turėtų bendrą supratimą apie galimą kibernetinių incidentų poveikį. Todėl Taryba prašo pirmiau nurodytų subjektų užtikrinti, kad ES ir, kai tinkama, nacionaliniu lygmenimis nustatant priemones bei paramą ir jų prioritetus būtų atsižvelgiama į rizikos vertinimus, scenarijus ir paskesnes rekomendacijas. Be to, Taryba ragina visus atitinkamus subjektus atsižvelgti į rizikos scenarijus rizikos vertinimo procesuose, taip pat rengiant kibernetinio saugumo pratybas.

III. **Investuoti į kibernetinės gynybos pajėgumus**

24. Taryba ragina valstybes nares didinti investicijas į sąveikių kibernetinės gynybos pajėgumų kūrimą, palaikymą ir tolesnį plėtojimą. Taryba pritaria tam, kad būtų rengiami savanoriški įsipareigojimai dėl nacionalinių kibernetinės gynybos pajėgumų tolesnio plėtojimo, atsižvelgiant į kitose sistemose dedamas panašias pastangas.

25. Taryba ragina valstybes nares ir EGA pasinaudoti galimybe peržiūrėti Pajėgumų plėtojimo planą, kad būtų nustatyti aukšto lygio užmojai, susiję su ES lygmens bendradarbiaujamosios kibernetinės gynybos plėtojimu. Taryba taip pat ragina valstybes nares remtis atnaujintu prioritetų rinkiniu ir savo PESCO įsipareigojimais, kad būtų padidintas jų dalyvavimo bendradarbiaujamuosiuose ES kibernetinės gynybos pajėgumų plėtojimo projektuose lygis, pripažindama tiesioginę ES lygmens bendradarbiaujamųjų projektų naudą siekiant remti nacionalinių kibernetinės gynybos pajėgumų plėtojimą.

26. Taryba palankiai vertina ES lygmens pastangas bendradarbiaujamųjų mokslinių tyrimų srityje, siekiant išnagrinėti besiformuojančių ir perversminių technologijų naudojimo su gynyba susijusiose sistemose galimybes, taip pat atkreipdama dėmesį į poreikį užtikrinti, kad tie technologiniai pokyčiai būtų greitai integruojami į esamus ir būsimus pajėgumus. Taryba ragina valstybes nares ir ES pramonę kuo geriau pasinaudoti ES lygmens bendradarbiaujamųjų mokslinių tyrimų galimybėmis, teikiamomis, pavyzdžiui, EGA sistemoje, vykdomais PESCO projektais, pavyzdžiui, ES kibernetiniu mokslinės kompetencijos ir inovacijų centru (CAIH), Europos gynybos fondu ir, kai aktualu, programa „Europos horizontas“ ir Skaitmeninės Europos programa dvejopo naudojimo projektų atveju. Be to, Taryba palankiai vertina tai, kad naudojamasi specialiomis sistemomis, kad pasinaudojant civilinės srities technologijų perėmimo galimybėmis būtų remiamos gynybos inovacijos, visų pirma ES gynybos inovacijų sistema ir Europos gynybos inovacijų centru. Be to, Taryba ragina Europos kibernetinio saugumo kompetencijos centrą (ECCC) ir EGA parengti darbinį susitarimą, kad būtų sudarytos palankesnės sąlygos atitinkamiems darbuotojams dalytis informacija apie atitinkamai civilinių, dvejopo naudojimo ir gynybos technologijų prioritetus, siekiant sukurti sinergiją ir išvengti dubliavimosi.

27. Taryba palankiai vertina Komisijos ketinimą, bendradarbiaujant su EGA ir ECCC, laikantis jų atitinkamų įgaliojimų, su valstybėmis narėmis ir konsultuojantis su atitinkamais suinteresuotaisiais subjektais, pavyzdžiui, pramonės atstovais, parengti ypatingos svarbos kibernetinių technologijų veiksmų gaires, kuriose, nustatant ypatingos svarbos kibernetines technologijas, nustatant technologinius pokyčius ir strateginę priklausomybę, pateikiamos galimybės ją sumažinti, remiant ES strateginį savarankiškumą ir technologinį suverenumą, kartu išsaugant atvirą ekonomiką. Taryba atkreipia dėmesį į tai, kad ypatingos svarbos kibernetinių technologijų veiksmų gairėmis gali būti grindžiami ES finansavimo priemonių strateginiai prioritetai, kartu laikantis atitinkamų joms taikomų sąlygų. Taryba primena, kad ES turėtų vykdyti plataus užmojo ir ryžtingą Europos pramonės politiką, kad būtų sukurta tvari, patraukli ir konkurencinga verslo aplinka, kuri taip pat galėtų sudaryti sąlygas kibernetinėje srityje veikiantiems Europos subjektams plėsti savo veiklą.

28. Taryba palankiai vertina ketinimą spręsti didelio kibernetinio saugumo įgūdžių trūkumo problemą pritraukiant naujų specialistų, įskaitant moteris, keliant kvalifikaciją bei perkvalifikuojant ir investuojant į mokymus bei pratybas ir juos rengiant, kad būtų sukurta įvairi ir įtrauki kibernetinės srities darbo jėga. Pripažindama iššūkius, su kuriais ES susiduria kibernetinio saugumo ir kibernetinės gynybos žmogiškojo kapitalo srityje, Taryba palankiai vertina Kibernetinio saugumo įgūdžių akademijos iniciatyvą, kuri taip pat gali būti naudinga ir kibernetinės gynybos srities darbo jėgai.

29. Taryba prašo valstybių narių keistis informacija apie geriausią patirtį, kad būtų ugdomi kvalifikuoti kibernetinio saugumo specialistai, išnaudojant karinių, civilinių ir teisėsaugos iniciatyvų sinergiją, ir ragina ESGK, remiant EGA bei ENISA ir naudojantis jų ekspertinėmis žiniomis, apsvarstyti galimybes sustiprinti keitimąsi geriausia patirtimi ir skatinti karinės ir civilinės sričių sinergiją, kiek tai susiję su kibernetinei sričiai būdingų gynybos įgūdžių mokymu ir ugdymu.

30. Taryba pabrėžia bendro supratimo apie kibernetinio saugumo srities darbo jėgos sudėtį ir susijusius įgūdžius svarbą siekiant nustatyti ir šalinti kibernetinio saugumo darbo rinkos spragas, taip pat poreikį angažuoti visus suinteresuotuosius subjektus, įskaitant valstybes nares ir pramonę. Taryba pripažįsta, kad nustačius kibernetinio saugumo darbo rinkos stebėsenos rodiklius būtų lengviau nustatyti kibernetinio saugumo įgūdžių poreikius ir tinkamai nukreipti lėšas, o kartu ir įgyvendinti su politika susijusius įsipareigojimus, visų pirma kylančius iš TIS 2. Taryba palankiai vertina pasiūlymą dėl kibernetinės gynybos įgūdžių sertifikavimo sistemos ir prašo vyriausiojo įgaliotinio, veikiančio kaip ESGK vadovas, išnaudojant civilines iniciatyvas, bendradarbiaujant su EIVT, Komisija ir valstybėmis narėmis, ją parengti.

IV. **Partneris bendriems iššūkiams įveikti**

31. Taryba ragina vyriausiąjį įgaliotinį ir Komisiją sustiprinti ir paspartinti savo bendradarbiavimą ir išnagrinėti galimybes pradėti abipusiai naudingas ir pritaikytas partnerystes kibernetinės gynybos politikos srityje, be kita ko, kibernetinės gynybos gebėjimų stiprinimo srityje pasitelkiant Europos taikos priemonę (ETP). Šiuo tikslu į ES dialogus ir konsultacijas kibernetiniais klausimais ir į bendras konsultacijas saugumo ir gynybos klausimais su partneriais turėtų būti įtrauktas kibernetinės gynybos klausimas. Be to, turėtų būti stiprinami dialogai ir bendradarbiavimas su privačiuoju sektoriumi. Taryba pabrėžia, kad tarptautinis bendradarbiavimas kibernetinio saugumo standartų ir sertifikavimo klausimais suteiktų pridėtinės vertės Europos pramonei. Todėl ji palankiai vertina Komisijos pasiryžimą užtikrinti, kad tai taptų esmine ES dialogų kibernetiniais klausimais su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis dalimi.

32. Taryba pabrėžia tarptautinio bendradarbiavimo svarbą siekiant užkirsti kelią konfliktų kibernetinėje erdvėje rizikai arba ją sumažinti, visų pirma toliau plėtojant ir praktiškai įgyvendinant pasitikėjimo stiprinimo priemones regioniniu ir tarptautiniu lygmeniu, be kita ko, Jungtinėse Tautose, ir toliau skatinant naudoti esamas kibernetines pasitikėjimo stiprinimo priemones, tokias, kokios naudojamos Europos saugumo ir bendradarbiavimo organizacijoje (ESBO), be kita ko, vyraujant tarptautinėms įtampoms.
ES ir jos valstybės narės akcentuoja, kad kibernetinėje erdvėje taikoma esama tarptautinė teisė, ir pabrėžia, kad svarbu nuolat dėti pastangas, siekiant puoselėti ir propaguoti JT atsakingo valstybių elgesio sistemą ir dirbti, kad ji būtų įgyvendinta, be kita ko, sukuriant Veiksmų programą dėl atsakingo valstybių elgesio kibernetinėje erdvėje gerinimo.

33. Laikantis bendrų pareiškimų dėl ES ir NATO bendradarbiavimo Taryba prašo vyriausiojo įgaliotinio, taip pat veikiančio kaip EGA vadovas, ir Komisijos toliau stiprinti, gilinti ir plėsti partnerystę su NATO kibernetinėje srityje, visapusiškai laikantis įtraukumo, abipusiškumo, abipusio atvirumo ir skaidrumo principų, taip pat abiejų organizacijų sprendimų priėmimo autonomijos. Atsižvelgdama į tai, kad reikia užtikrinti papildomas ir koordinuotas pastangas kiek įmanoma labiau įtraukiant NATO nepriklausančias valstybes nares ir vengiant bereikalingo dubliavimosi, Taryba ragina atitinkamais lygmenimis nustatyti ES ir NATO sąsajas mokymo, švietimo, informuotumo apie padėtį, pratybų ir mokslinių tyrimų ir plėtros platformų srityse ir siekti užtikrinti galimą sinergiją tarp atitinkamų savanoriškų įsipareigojimų plėtoti nacionalinius kibernetinės gynybos pajėgumus ir krizių valdymo sistemų, ypatingos svarbos infrastruktūros apsaugos, taip pat keitimosi informacija dėl informuotumo apie padėtį stiprinimo, koordinuoto reagavimo į kibernetinę kenkimo veiklą ir pajėgumų stiprinimo pastangų trečiosiose valstybėse. Tai apima NATO reagavimo į kompiuterinius incidentus tarnybos (NCIRC) ir Europos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU) techninį susitarimą ir sustiprintą politinį dialogą kibernetinės gynybos klausimais visais lygmenimis.

V. **Išvada**

34. Remdamasi Tarybos išvadomis dėl ES kibernetinės gynybos politikos, Taryba ragina vyriausiąjį įgaliotinį ir Komisiją ne vėliau kaip 2023 m. antrąjį ketvirtį parengti valstybėms narėms patvirtinti skirtą šios politikos įgyvendinimo planą. Be to, Taryba prašo valstybių narių savanoriškai pareikšti savo užmojus ir veiksmus, susijusius su kibernetine gynyba pagal ES kibernetinės gynybos politiką ir visapusiškai pasinaudoti teisiškai neprivalomomis savanoriškomis rekomendacijomis ir įsipareigojimais paspartinti savo nacionalines ir daugiašales kibernetinės gynybos pastangas, kuriomis siekiama kuo labiau padidinti poveikį ES lygmeniu. Vyriausiojo įgaliotinio, Komisijos ir valstybių narių prašoma pradedant 2024 m. antrąjį ketvirtį pranešti apie bendro komunikato elementų ir jo įgyvendinimo plano įgyvendinimo pažangą ir kasmet ją aptarti.