Europos Sąjungos
Taryba

Briuselis, 2024 m. gruodžio 6 d.
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
kam:	Delegacijoms
Dalykas:	Tarybos išvados dėl ENISA

Delegacijoms priede pateikiamos Tarybos išvados dėl ENISA, kurias Taryba patvirtino 2024 m. gruodžio 6 d. įvykusiame posėdyje.

PRIEDAS

Tarybos išvadų dėl ENISA projektas

EUROPOS SĄJUNGOS TARYBA,

1. PABRĖŽIA, kad dėl besiformuojančių itin sudėtingų kibernetinių grėsmių, nuolat kintančios saugumo aplinkos ir dabartinės geopolitinės įtampos pasaulinėje kibernetinėje erdvėje kylantys iššūkiai dar niekada nebuvo tokie sudėtingi, įvairūs ir rimti kaip dabar. Todėl ES ir jos valstybės narės turėtų toliau dėti pastangų, kad taptų atsparesnės ir galėtų veiksmingai nustatyti esamas ir kylančias grėsmes bei iššūkius ir į juos reaguoti. AKCENTUOJA, kad darbas siekiant didesnio kibernetinio atsparumo turėtų būti tęsiamas laikantis visos visuomenės įtraukimo požiūrio. PABRĖŽIA, kad ateinančiais metais ES ir jos valstybės narės turėtų sutelkti dėmesį į veiksmingą teisėkūros ir ne teisėkūros iniciatyvų, kuriomis grindžiami ir remiami visi veiksmai, kurių iki šiol imtasi šioje srityje, įgyvendinimą;

2. PRIMINDAMA, kad kiekviena valstybė narė ir toliau yra išimtinai atsakinga už savo nacionalinį saugumą, PRIPAŽĮSTA, kad pastaraisiais metais ES ir jos valstybės narės intensyviai dirbo kartu, kad, kiek tai susiję su kibernetine sritimi, tiek nacionaliniu, tiek ES lygmenimis būtų sukurta reikiama institucinė sąranga ir nustatytos bendradarbiavimo formos. PALANKIAI VERTINA įvairias teisėkūros ir ne teisėkūros iniciatyvas, kuriomis ES ir jos valstybėms narėms buvo suteikta tvirta ir patikima sistema šioje srityje ir taip padidintas bendras Sąjungos kibernetinis atsparumas. Ši sistema buvo išplėtota, kad apimtų kelis kibernetinės erdvės aspektus: saugumą, diplomatiją, teisėsaugą ir gynybą. PAŽYMI, kad ES kibernetinio saugumo ekosistemą sudaro daug subjektų, įskaitant valstybių narių kibernetinio saugumo institucijas, TIS bendradarbiavimo grupę (TIS BG), CSIRT tinklą, Europos ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (EU-CyCLONe), Nacionalinių koordinavimo centrų tinklą (NKCT), Europos kibernetinio saugumo sertifikavimo grupę (EKSSG), Komisiją, Europos išorės veiksmų tarnybą (EIVT), Europos Sąjungos kibernetinio saugumo agentūrą (ENISA), Europos kibernetinio saugumo kompetencijos centrą (ECCC), CERT-EU, Europos gynybos agentūrą (EGA) ir Europolo Europos kovos su elektroniniu nusikalstamumu centrą (EC3), ir kiekvienas iš jų atlieka savo vaidmenį įgyvendinant ES masto kibernetinio saugumo sistemą;

3. PRIPAŽĮSTA, kad per pastaruosius du dešimtmečius ENISA įrodė, kad yra neįkainojamas subjektas Europos kibernetinio saugumo ekosistemoje, kuris atlieka itin svarbų vaidmenį aktyviai padėdamas valstybėms narėms ir ES institucijoms, organams, įstaigoms ir agentūroms įgyvendinti ir plėtoti kibernetinio saugumo politiką, stiprinti savo gebėjimus ir parengtį, bendradarbiauti ir skatinti informuotumą apie kibernetinį saugumą ir sertifikavimą.

BENDROSIOS POLITINĖS REKOMENDACIJOS

4. PRAŠO Komisijos pasinaudoti **Kibernetinio saugumo akto vertinimu** kaip galimybe išnagrinėti, kaip juo būtų galima prisidėti prie sudėtingos kibernetinės ekosistemos supaprastinimo ir taip padidinti išteklių naudojimo veiksmingumą ir efektyvumą. Todėl RAGINA Komisiją užtikrinti, kad ENISA įgaliojimai remti valstybes nares ir ES institucijas, organus, įstaigas ir agentūras būtų orientuoti į rezultatus ir aiškiai apibrėžti, kad būtų nustatyti konkretūs strateginiai tikslai ir prioritetinės užduotys, taip pat tiksliau pasidalijamos užduotys ir kompetencijos kitų subjektų atžvilgiu. Šiuo atžvilgiu PRAŠO Komisijos išnagrinėti ir toliau stiprinti ENISA vaidmenį remiant operacinį bendradarbiavimą ES lygmeniu ir tarp valstybių narių kibernetinio atsparumo didinimo srityje, atsižvelgiant į valstybių narių kompetenciją šioje srityje. Be to, RAGINA Komisiją stiprinti ENISA patariamąjį vaidmenį teikiant ekspertų ir įrodymais grindžiamas gaires ir rekomendacijas dėl dabartinių ir būsimų ES teisėkūros ir ne teisėkūros iniciatyvų įgyvendinimo, kartu užtikrinant nuoseklią ES kibernetinio saugumo sistemą;

5. vadovaudamasi tuo pačiu principu RAGINA Komisiją apsvarstyti galimybę racionalizuoti ENISA vaidmenį, susijusį su užduotimis, kurios nėra esminės jos misijai. PABRĖŽIA, kad naujausiomis teisėkūros iniciatyvomis, be kita ko, TIS 2, Kibernetinio atsparumo aktu ir Kibernetinio solidarumo aktu, ENISA **atsakomybė buvo reikšmingai išplėsta**. ATKREIPDAMA DĖMESĮ į tai, kad dėl kai kurių iš šių iniciatyvų ENISA gavo papildomų išteklių, AKCENTUOJA, kad dėl ENISA atsakomybės išplėtimo ir didėjančio kibernetinių grėsmių bei iššūkių sudėtingumo labai padaugėjo jos užduočių, todėl jai turėtų būti suteikti **tinkami ištekliai** – žmogiškieji, finansiniai ir techniniai – kad Agentūra galėtų visapusiškai vykdyti visas jos kompetencijai tenkančias užduotis, nedarant poveikio deryboms dėl daugiametės finansinės programos. Šiuo tikslu RAGINA Komisiją rengiant Sąjungos bendrojo biudžeto projektą prioritetizuoti veiksmus ir teikti pirmenybę užduotims, susijusioms su parama valstybėms narėms didinant jų kibernetinį atsparumą, jų operacinį bendradarbiavimą ir rengiant bei įgyvendinant Sąjungos teisę.

ENISA PARAMA RENGIANT IR ĮGYVENDINANT POLITIKĄ

6. PRIMENA, kad pagal dabartinę kibernetinio saugumo teisinę sistemą ENISA patikėtos kelios pagrindinės pagalbos ir patariamosios užduotys ES. PALANKIAI VERTINA ENISA vaidmenį šioje srityje – **padėti valstybėms narėms** veiksmingai įgyvendinti teisėkūros ir ne teisėkūros iniciatyvas. RAGINA ENISA, glaudžiai bendradarbiaujant su TIS BG ir Komisija, toliau teikti bendras įžvalgas ir analizes apie dabartinę teisinę aplinką kibernetinio saugumo srityje. RAGINA ENISA reguliariai ir struktūrizuotai dalytis techninėmis gairėmis ir geriausios praktikos pavyzdžiais ir aktyviai juos propaguoti, taip padedant valstybėms narėms įgyvendinti kibernetinio saugumo politiką ir teisės aktus;

7. PRIPAŽĮSTA itin svarbų ENISA vaidmenį kuriant **Europos kibernetinio saugumo sertifikavimo schemas**, kuriomis grindžiamas pasitikėjimas IRT produktais, paslaugomis ir procesais, taip pat valdomas saugumo paslaugas, atsižvelgiant į būsimus tikslinius Kibernetinio saugumo akto pakeitimus. PABRĖŽIA, kad valstybės narės ir sektorius yra susirūpinę dėl ilgo kibernetinio saugumo sertifikavimo schemų atrankos, rengimo ir patvirtinimo proceso; todėl RAGINA Komisiją pasinaudoti Kibernetinio saugumo akto vertinimo suteikta galimybe rasti būdų kaip užtikrinti, kad ES kibernetinio saugumo sertifikavimo schemos būtų rengiamos taikant paprastesnį, rizika grindžiamą, skaidresnį ir spartesnį metodą, kartu PABRĖŽDAMA svarbų valstybių narių vaidmenį šiame procese. Be to, AKCENTUOJA, kad svarbu aiškiai priskirti atsakomybę už kiekvienos sertifikavimo schemos priežiūrą. Taip pat PRIMENA, kad ENISA, rengdama potencialias schemas, turėtų laiku konsultuotis su visais atitinkamais suinteresuotaisiais subjektais, pasitelkdama formalų, atvirą, skaidrų ir įtraukų procesą, ir kad Komisija, vertindama patvirtintų schemų veiksmingumą ir naudojimą, turėtų rengti atviras, skaidrias ir įtraukias konsultacijas. Ragina ENISA toliau stiprinti bendradarbiavimą su duomenų apsaugos bendruomene, visų pirma, kai aktualu, su Europos duomenų apsaugos valdyba ir nacionalinėmis kompetentingomis institucijomis, ypatingą dėmesį skirdama sinergijų skatinimui rengiant būsimas Europos kibernetinio saugumo sertifikavimo schemas;

8. RAGINA ENISA, bendradarbiaujant su Komisija, toliau keistis informacija su valstybėmis narėmis dėl pranešimų teikimo procedūros praktinių aspektų, supaprastinimo ir racionalizavimo, kad būtų išvengta nereikalingos administracinės naštos, kuri galėtų atsirasti dėl sudėtingos pranešimų teikimo sistemos. Be to, PRIMENA prašiusi, kad Komisija, padedama ENISA ir kitų atitinkamų ES subjektų, parengtų atitinkamų pareigų pranešti, nustatytų atitinkamuose ES teisės aktuose kibernetiniais ir skaitmeniniais klausimais, apžvalgą. PRIMENA, kad ENISA ir valstybių narių keitimasis informacija remiasi pasitikėjimu grindžiamais santykiais, kai saugumas ir konfidencialumas užtikrinami pagal Kibernetinio saugumo aktą ir atitinkamas taisykles bei protokolus ir turėtų apsiriboti tik tuo, kas aktualu ir proporcinga to keitimosi tikslu. PABRĖŽIA, kad duomenys ir informacija turi būti tvarkomi rūpestingai;

9. PABRĖŽIA, kad ENISA yra atsakinga už **vienos bendros pranešimų teikimo platformos pagal Kibernetinio atsparumo aktą** sukūrimą ir priežiūrą; ši platforma teiks konkrečią operacinę pridėtinę vertę, visų pirma aktyviai išnaudojamų pažeidžiamumų ir rimtų incidentų atvejais, kai daromas poveikis produktų su skaitmeniniais elementais saugumui. Atsižvelgiant į plačią šių horizontaliųjų teisės aktų taikymo sritį, viena bendra pranešimų teikimo platforma turėtų būti veiksminga ir saugi priemonė, padedanti nacionalinėms CSIRT ir ENISA keistis informacija. Todėl RAGINA ENISA ne tik skirti pakankamai žmogiškųjų išteklių, bet ir paspartinti platformos sukūrimą – tai vienas iš svarbiausių prioritetų siekiant užtikrinti platformos parengtį iki Kibernetinio atsparumo akte nustatyto termino;

10. PRIPAŽĮSTA ENISA vaidmenį kuriant **Europos pažeidžiamumų duomenų bazę**, kuria siekiama užtikrinti didesnį skaidrumą, susijusį su pažeidžiamumų atskleidimu, kartu užtikrinant tinkamą neskelbtinų duomenų tvarkymą. Atsižvelgdama į tai, kad baigiasi TIS 2 direktyvos perkėlimo į nacionalinę teisę laikotarpis, RAGINA ENISA paspartinti visą būtiną darbą, kad būtų užtikrintas sklandus šios duomenų bazės veikimas. Kartu PRAŠO TIS BG, padedant ENISA, toliau viešinti pažeidžiamumų atskleidimo gaires, politiką ir procedūras;

11. PRIPAŽĮSTA ENISA vykdomų **kibernetinio saugumo rėmimo veiksmų**, kurie sudaro kibernetinio saugumo paslaugų rezervą, kuriuo valstybės narės gali naudotis norėdamos papildyti savo pastangas, naudą, taip pat ENISA patirtį, įgytą juos įgyvendinant. Šiuo atžvilgiu PABRĖŽIA, kad ENISA turėtų atlikti pagrindinį vaidmenį administruojant ES kibernetinio saugumo rezervą ir užtikrinant jo veikimą. PRAŠO ENISA iš karto po to, kai įsigalios Kibernetinio solidarumo aktas, pradėti rengti reikiamų paslaugų ir jų prieinamumo apžvalgą, kad visose valstybėse narėse ES kibernetinio saugumo rezervas būtų kuo naudingesnis ir kuo labiau pritaikytas naudotojų poreikiams. PRAŠO ENISA, kai tik jai bus pavestos užduotys, įtraukti valstybes nares, visų pirma renkant informaciją apie reikiamus kriterijus ir informuojant apie būsimus konkursus, ankstyvame ES kibernetinio saugumo rezervo kūrimo proceso etape. PRAŠO ENISA, kai tik jai bus pavestos užduotys, užtikrinti, kad patikimų valdomų saugumo paslaugų teikėjų atrankos procesas būtų skaidrus, atviras, sąžiningas ir kad jame galėtų dalyvauti paslaugų teikėjai iš visų valstybių narių, neatsižvelgiant į jų dydį. Be to, PRIMENA, kad ENISA turi nepagrįstai nedelsdama paskelbti tarpvalstybinių kibernetinio saugumo centrų sąveikumo gaires;

12. PABRĖŽIA, kad **tendencijų, susijusių su** sparčiai kintančioje kibernetinėje srityje **besiformuojančiomis technologijomis, stebėsena** yra labai svarbi mūsų kibernetinio saugumo būklei išlaikyti ir toliau stiprinti. PALANKIAI VERTINA darbą, kurį ENISA atliko tam, kad atkreiptų visuomenės dėmesį į tokių technologijų kaip dirbtinis intelektas ir kvantinė kompiuterija keliamą riziką ir teikiamas galimybes, taip padėdama geriau suprasti dabartinius iššūkius. RAGINA ENISA toliau prisidėti vykdant šias užduotis, aktyviai remti jos rekomendacijų įgyvendinimą ir, kai aktualu, patarti ECCC ir su juo bendradarbiauti.

ENISA PARAMA VALSTYBĖMS NARĖMS STIPRINANT KIBERNETINĮ ATSPARUMĄ IR OPERACINĮ BENDRADARBIAVIMĄ

13. AKCENTUOJA, kad ENISA atlieka svarbų vaidmenį, nes yra **dviejų ES lygmens valstybių narių valdomų kibernetinio bendradarbiavimo tinklų – CSIRT tinklo ir EU-CyCLONe – sekretoriatas**. PABRĖŽIA vertingą ENISA dalyvavimą TIS BG, visų pirma jos aktyvų dalyvavimą ir techninį indėlį, susijusius su įvairiomis darbo kryptimis. RAGINA ENISA ateityje toliau remti šių tinklų veikimą ir bendradarbiavimą, nes jie yra itin svarbūs valstybių narių bendradarbiavimo įvairiais lygmenimis kanalai;

14. PAKARTOJA, kad reikia gerinti **bendrą informuotumą apie padėtį** ES lygmeniu – tai padeda gerinti ES kibernetinio saugumo būklę, kiek tai susiję su kibernetinių incidentų aptikimu, prevencija ir reagavimu į juos. Šiuo atžvilgiu AKCENTUOJA ENISA prognozavimo veiklos, reguliaraus ataskaitų teikimo ir grėsmių vertinimų svarbą – visa tai padeda gerinti informuotumą apie padėtį. RAGINA ENISA glaudžiai bendradarbiauti su valstybėmis narėmis ir padėti gerinti informuotumą apie padėtį ES lygmeniu. Šiame kontekste PRIPAŽĮSTA svarbų vaidmenį, kurį ENISA atlieka kartu su CERT-EU ir Europolu, padėdama Tarybai rengti informacinius pranešimus apie padėtį Kibernetinio saugumo diplomatijos priemonių rinkinio kontekste, kuriais papildomas Bendro žvalgybinės informacijos analizės centro (SIAC) indėlis, susijęs su informuotumu apie padėtį, ir AKCENTUOJA, kad reikia parengti išsamią grėsmių apžvalgą remiantis įvairiais šaltiniais, įskaitant privatųjį sektorių. Atsižvelgdama į tai, RAGINA toliau plėtoti ENISA bendradarbiavimą su EIVT, visų pirma su INTCEN, visapusiškai atsižvelgiant į atitinkamus jų įgaliojimus;

15. PABRĖŽIA, kad Komisijos kibernetinės padėties ir analizės centras atlieka vidaus funkciją Komisijoje ir jam yra naudingas bendradarbiavimas su ENISA ir CERT-EU. Siekiant sukurti kuo daugiau galimybių sinergijoms ir sumažinti ES kibernetinės ekosistemos sudėtingumą, PRAŠO Komisijos atsižvelgti į Kibernetinio saugumo akto vertinimo rezultatus ir diskusijas dėl Kibernetinio saugumo plano vertinimo, kad būtų racionalizuotos Komisijos Kibernetinės padėties ir analizės centro užduotys ir susijusios ENISA užduotys. RAGINA Komisiją vengti nereikalingo užduočių dubliavimo, kartu išsaugant pagrindinį ENISA vaidmenį – padėti gerinti bendrą informuotumą apie padėtį Sąjungos lygmeniu, remiant valstybes nares, tinkamai atsižvelgiant į jų nacionalinę kompetenciją;

16. AKCENTUOJA, kad bendro informuotumo apie padėtį gerinimas yra būtina sąlyga norint laiku ir veiksmingai valdyti krizes Sąjungos mastu. PABRĖŽIA, kad **reaguojant į didelio masto kibernetinio saugumo incidentus** ES lygmeniu dalyvauja įvairūs svarbūs subjektai ir kad tokių incidentų atveju veiksmingas valstybių narių bendradarbiavimas daugiausia grindžiamas CSIRT tinklu ir EU-CyCLONe. ENISA atlieka svarbų vaidmenį valdant kibernetines krizes, nes yra CSIRT tinklo ir EU-CyCLONe sekretoriatas. PRAŠO Komisijos pasinaudoti Kibernetinio saugumo plano vertinimu, kad būtų tinkamai atspindimos papildomos užduotys ir pareigos, padedančios plėtoti bendradarbiavimu grindžiamą atsaką į didelio masto tarpvalstybinius kibernetinius incidentus ar krizes, taip pat vaidmuo, tenkantis ENISA kaip CSIRT tinklo ir EU-CyCLONe sekretoriatui ir pagal neseniai priimtus kibernetinio saugumo teisės aktus;

17. PABRĖŽIA, kad svarbu reguliariai organizuoti **kibernetinio saugumo pratybas**, kurios labai pagerina ES pasirengimą reaguoti į incidentus ir krizes. PRIPAŽĮSTA, kad ENISA sukaupė vertingos ir didelės patirties šioje srityje, padėdama valstybėms narėms. PRIPAŽĮSTA svarbų ENISA vaidmenį kibernetinio saugumo pratybų planavimo, rengimo, vykdymo ir vertinimo etapuose ir PABRĖŽIA, kad ji ir toliau turėtų būti vienu iš pagrindinių subjektų ES lygmeniu, atsižvelgiant į tai, kad tokios pratybos turėtų būti vykdomos remiantis struktūrizuotomis sistemomis ir bendra terminologija. PRAŠO ENISA, CSIRT tinklo ir EU-CyCLONe kuo veiksmingiau naudotis esamomis reguliariomis pratybomis, kad būtų išbandomos ir tobulinamos ES reagavimo į krizes sistemos, ir užtikrinti kuo geresnį įgytos patirties panaudojimą.

ENISA BENDRADARBIAVIMAS SU KITAIS KIBERNETINĖS EKOSISTEMOS SUBJEKTAIS

18. PAKARTOJA, kad dėl horizontalaus kibernetinio saugumo pobūdžio itin svarbus **visų valstybių narių ir Sąjungos lygmens subjektų bendradarbiavimas**, todėl PABRĖŽIA, kad bendram kibernetiniam atsparumui didinti Europos lygmeniu taip pat reikalingas bendras ENISA ir kitų atitinkamų kibernetinės srities subjektų darbas;

19. PABRĖŽIA, kad institucijų, organų, įstaigų ir agentūrų gebėjimas užsitikrinti kibernetinį saugumą yra svarbus bendram ES lygmens kibernetiniam atsparumui, kurį užtikrinant CERT-EU vaidmuo yra neįkainojamas. Šiuo atžvilgiu PALANKIAI VERTINA nustatytą CERT-EU ir ENISA struktūrizuotą bendradarbiavimą ir RAGINA juos toliau glaudžiai bendradarbiauti ateityje;

20. pasiekęs finansinį savarankiškumą, ECCC pagal savo įgaliojimus labai prisidės plėtojant stiprią Europos kibernetinę mokslinių tyrimų, pramonės ir technologijų ekosistemą, apimančią darbo jėgos ugdymo įgūdžius. RAGINA ENISA ir ECCC toliau glaudžiai bendradarbiauti, visų pirma kiek tai susiję su mokslinių tyrimų ir inovacijų poreikiais ir prioritetais, taip pat kibernetiniais įgūdžiais, kad būtų didinamas Sąjungos kibernetinio saugumo pramonės konkurencingumas. PRAŠO Komisijos išnagrinėti, kaip būtų galima dar labiau optimizuoti ENISA ir ECCC veiklos sinergiją ir kaip geriau racionalizuoti veiklą pagal atitinkamus jų įgaliojimus;

21. PABRĖŽIA, kad reguliarus naujausios informacijos apie grėsmių padėtį teikimas padeda geriau nustatyti, kokių priemonių reikia tam, kad būtų veiksmingai kovojama su kibernetiniais nusikaltimais. PABRĖŽIA ES bendro kibernetinio saugumo vertinimo ataskaitų, kurios yra ENISA, Europolo EC3 ir CERT-EU bendradarbiavimo rezultatas ir jau suteikė vertingos informacijos reaguojant į įvairius iššūkius, įskaitant kovą su kibernetiniais nusikaltimais, pridėtinę vertę. PRAŠO ENISA ir Europolo ateityje toliau struktūrizuotai bendradarbiauti;

22. AKCENTUOJA, kad kibernetinė gynyba yra svarbi ir nuolat tobulinama kovos su kibernetinėje erdvėje kylančiomis grėsmėmis dalis. PABRĖŽIA, kad ENISA turi bendradarbiauti su EIVT ir Komisija tais atvejais, kai ENISA atlieka tam tikrą vaidmenį padėdama įgyvendinti ES kibernetinės gynybos politiką, glaudžiai bendradarbiaudama su EGA, ECCC ir kibernetinės gynybos bendruomene. Pabrėžia ENISA, kaip civilinės agentūros, vaidmenį. PABRĖŽIA, kad svarbu stiprinti ir racionalizuoti civilinį ir karinį bendradarbiavimą kibernetinėje srityje ES, įskaitant aiškų vaidmenų ir atsakomybės pasidalijimą tarp dviejų bendruomenių ir tarp ES ir NATO, visapusiškai laikantis įtraukumo, abipusiškumo, abipusio atvirumo ir skaidrumo principų, taip pat abiejų organizacijų sprendimų priėmimo autonomiškumo. RAGINA ENISA toliau sudarinėti darbo susitarimus su NATO ryšių ir informacijos agentūra;

23. RAGINA ES toliau propaguoti mūsų bendras vertybes ir bendras pastangas pasauliniuose forumuose, kad būtų apsaugota laisva, visuotinė, atvira ir saugi kibernetinė erdvė. AKCENTUOJA, kad dėl tarpvalstybinio kibernetinių grėsmių ir incidentų pobūdžio būtinas tvirtas ir veiksmingas bendradarbiavimas ne tik ES lygmeniu, bet ir **su tarptautinėmis organizacijomis ir partneriais**. PAŽYMI, kad ENISA tarptautinis dalyvavimas turėtų būti sutelktas į strateginius partnerius ir ES šalis kandidates, laikantis ES bendros užsienio ir saugumo politikos. AKCENTUOJA, kad tarptautinio dalyvavimo kontekste ENISA turėtų veikti pagal savo įgaliojimus ir atitinkamas Kibernetinio saugumo akto nuostatas. PRIPAŽĮSTA, kad būtina paaiškinti, laikantis atitinkamų procedūrų, ENISA tarptautinį dalyvavimą, visų pirma užtikrinant, kad jos Valdančioji taryba būtų tinkamai ir laiku informuojama apie susijusią veiklą. RAGINA ENISA dalyvauti atitinkamose tarptautinėse kibernetinio saugumo srities bendradarbiavimo sistemose, įskaitant tokias organizacijas kaip NATO ir ESBO;

24. PAKARTOJA, kad ES ir jos valstybės narės dažnai akcentuoja **kibernetinio saugumo įgūdžių** trūkumą. PRIMENA, kad Komisija ir ENISA nustatė plačią ir visa apimančią sistemą, skirtą teikti gaires visiems suinteresuotiesiems subjektams, pavyzdžiui, Europos kibernetinio saugumo įgūdžių sistemą, Komunikatą dėl Kibernetinio saugumo įgūdžių akademijos ir kasmet organizuojamą Europos kibernetinio saugumo įgūdžių konferenciją, ir RAGINA Komisiją ir ENISA remtis šiomis iniciatyvomis, daug dėmesio skiriant vykstančioms diskusijoms dėl Europos skaitmeninės infrastruktūros konsorciumo (ESIK). Todėl PRAŠO Komisijos palaikyti ryšius su valstybėmis narėmis, suinteresuotomis įsteigti ESIK. PRIPAŽĮSTA, kad ir ENISA, ir ECCC yra įgalioti skatinti įgūdžius visoje Sąjungoje. PRAŠO ENISA pirmenybę teikti valstybių narių įgūdžių ir švietimo pastangų rėmimui, plačiosios visuomenės informuotumo didinimui ir, kai tinkama, bendradarbiavimui su ECCC;

25. PRIPAŽĮSTA, kad pastaraisiais metais ENISA plėtojo **bendradarbiavimą su privačiuoju sektoriumi**. PRIMENA, kad privatusis sektorius nuolat stebi kibernetinių grėsmių padėtį, todėl šio sektoriaus surinkta informacija galėtų padėti pagerinti bendrą informuotumą apie padėtį. Todėl RAGINA ENISA, glaudžiai bendradarbiaujant su valstybėmis narėmis ir subjektais visoje ES, skatinti bendradarbiavimą su privačiuoju sektoriumi;

26. RAGINA Komisiją ir ENISA apsvarstyti būdus, kaip sustiprinti ENISA ir Europos **standartizacijos** institucijų bendradarbiavimą. AKCENTUOJA, kad ENISA turi gilinti savo ekspertines žinias Europos kibernetinio saugumo standartizacijos srityje, be kita ko, stebėdama standartizacijos veiklą ir joje dalyvaudama;

27. PRIMYGTINAI RAGINA Komisiją ir ENISA išnagrinėti, kaip geriau optimizuoti ES kibernetinio saugumo sistemos veikimą, atsižvelgiant į šiose išvadose pateiktas rekomendacijas ir pasiūlymus. Nuolatinis bendradarbiavimas, užduočių ir išteklių prioritetizavimas, taip pat sudėtingos kibernetinės aplinkos supaprastinimas bus pagrindiniai elementai, padėsiantys įveikti dabartinius ir būsimus iššūkius.