Europos ekonomikos ir socialinių reikalų komiteto nuomonė „Bendras komunikatas Europos Parlamentui ir Tarybai „ES kibernetinės gynybos politika““

(nuomonė savo iniciatyva)

(2023/C 293/04)

Pranešėjas **Anastasis YIAPANIS**

Bendrapranešėjis **Alberto MAZZOLA**

Plenarinės asamblėjos sprendimas	2022 9 20
Teisinis pagrindas	Darbo tvarkos taisyklių 52 straipsnis 2 dalis
	Nuomonė savo iniciatyva
Atsakingas skyrius	Pramonės permainų konsultacinė komisija (CCMI)
Priimta skyriuje	2023 3 27
Priimta plenarinėje sesijoje	2023 6 14
Plenarinė sesija Nr.	579
Balsavimo rezultatai	
(už / prieš / susilaikė)	208 / 1 / 2

1. **Išvados ir rekomendacijos**

1.1. Europos ekonomikos ir socialinių reikalų komitetas (EESRK) pritaria siūlomai ES kibernetinės gynybos politikai, tačiau tikėjosi, kad rengiant šiuos pasiūlymus organizuotai pilietinei visuomenei bus suteiktas svarbesnis vaidmuo. Komitetas mano, kad šiuo metu sunku įvertinti, ar bus įgyvendintos bendrame komunikate nurodytos būsimos iniciatyvos ir ar bus pasiekti numatyti jų rezultatai. Jis ragina ES institucijas ir valstybes nares teikti pirmenybę paskelbtoms iniciatyvoms ir skubiai jas įgyvendinti.

1.2. EESRK pabrėžia, jog reikia papildomų priemonių, kad ES turėtų geresnes galimybes nustatyti kibernetines grėsmes, ir ragina moksliniams tyrimams ir plėtrai skiriamą finansavimą nukreipti į pažangiųjų ES pajėgumų kūrimą. Privačiojo ir viešojo sektorių bendradarbiavimas yra labai svarbus ir neturi būti vienkryptis. EESRK mano, kad ES koordinavimas yra būtinas siekiant spręsti susiskaidymo problemą ir užtikrinti valstybių narių bendradarbiavimą ir bendras investicijas.

1.3. EESRK pritaria ES kibernetinės gynybos koordinavimo centro įkūrimui ir rekomenduoja valstybėms narėms įsipareigoti kasdien visą parą užtikrinti greitąjį reagavimą, įvertinti ES reagavimo į kibernetines krizes mechanizmų parengtį ir veiksmingumą, daugiausia dėmesio skiriant tiek kariniams pajėgumams, tiek ypatingos svarbos sektoriams, kaip nustatyta Europos Parlamento ir Tarybos direktyvoje (ES) 2022/2555 ([1]) (toliau – TIS 2 direktyva). Komitetas pritaria, kad būtų išplėsti Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro (ECCC) įgaliojimai siekiant padėti ES kibernetinės gynybos koordinavimo centrui vykdyti veiklą.

1.4. EESRK mano, kad siekiant padidinti Sąjungos kibernetinio saugumo strateginį savarankiškumą ir suverenumą, reikėtų sukurti arba iš privačiojo sektoriaus perimti dinamišką testavimo ir dalijimosi informacija tikruoju laiku platformą, kad būtų galima nustatyti esamas turimų pajėgumų spragas. Platforma taip pat gali būti naudojama keitimuisi geriausios praktikos pavyzdžiais, pranešimams apie kibernetinius incidentus ir visų kibernetinių nusikaltėlių ES sąrašo sudarymui.

([1]) 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva) (OL L 333, 2022 12 27, p. 80).

1.5. EESRK pabrėžia, kad reikia geriau pasirengti tokiems kibernetiniams išpuoliams kaip Rusijos išpuoliai Ukrainoje, kurie visų pirma yra nukreipti prieš ypatingos svarbos infrastruktūros objektus. Civilinių ir karinių ekosistemų bendradarbiavimas yra labai svarbus siekiant veiksmingai valdyti krizes, užtikrinti sąveikumą ir išvengti pastangų bei investicijų dubliavimo. Pavyzdžiui, būtų galima imituoti bandomuosius kibernetinius išpuolius.

1.6. EESRK mano, kad investicijomis į kibernetinę gynybą pirmenybė turėtų būti teikiama ES piliečių ir ypatingos svarbos infrastruktūros objektų apsaugai, be kita ko, pasirenkant patikimus aparatinės ir programinės įrangos tiekėjus. Komitetas primygtinai ragina laiku atnaujinti prioritetus ir investicijas, dėl kurių turi susitarti ES ir valstybės narės, dalyvaujant atitinkamiems privatiems suinteresuotiesiems subjektams.

1.7. ES turi išlaikyti ir plėtoti būtinus pajėgumus, kad apsaugotų savo skaitmeninę ekonomiką, visuomenę, demokratiją bei ypatingos svarbos technologijas ir teiktų pagrindines kibernetinio saugumo paslaugas. Siekiant ES strateginio savarankiškumo gyvybiškai svarbu mažinti priklausomybę nuo trečiųjų šalių. EESRK nuomone, labai svarbu, kad ES vidutinės trukmės laikotarpiu siektų savarankiškumo pagrindinių technologijų srityje, ir tvirtai pasisako už tai, kad ES įsisteigusios įmonės kurtų moksliniams tyrimams ir gamybai skirtus įrenginius, o atitinkama Europos pramonės politika būtų orientuota į savarankišką kibernetinę ekosistemą.

1.8. MVĮ turėtų gauti tikslinę paramą ir turėti prieigą prie finansavimo programų, kuriomis didinamas jų atsparumas kibernetiniams išpuoliams, taip pat suteikti joms pagalbą, galimybes mokytis ir šviestis apie kibernetinę riziką ir apie tai, kaip nuo jos apsisaugoti. ES turėtų numatyti paskatų mechanizmą, kuriuo būtų skatinamas laipsniškas MVĮ supažindinimas su kibernetinio saugumo klausimais ir novatoriškų MVĮ plėtra.

1.9. EESRK pritaria planui įsteigti Kibernetinio saugumo įgūdžių akademiją ir prašo Europos Komisijos koordinuoti bei finansuoti didelio masto mokymo ir profesinio rengimo programas, kuriose dalyvautų visos valstybės narės ir kuriomis būtų siekiama rengti kvalifikuotą darbo jėgą visoms kibernetinės gynybos srityje veikiančioms agentūroms bei organizacijoms, taip pat privatiems civiliniams tinklams.

1.10. Komitetas mano, kad piliečių informuotumo apie kibernetinį saugumą didinimas yra labai svarbus mažinant susidūrimo su kibernetiniais išpuoliais riziką, ir ragina parengti kibernetinio saugumo mokymo programas bei visą gyvenimą trunkančio mokymo programas, kuriose daugiausia dėmesio būtų skiriama kibernetinių įgūdžių lavinimui ir žinių gilinimui. EESRK pritaria tam, kad kibernetinis saugumas būtų įtrauktas į visas būsimas ES viešosios politikos sritis, o plačioji visuomenė būtų informuojama apie kibernetines grėsmes.

1.11. EESRK mano, kad glaudžiai bendradarbiaujant su NATO sąjungininkais karinėse srityse daugiausia dėmesio turi būti skiriama visapusiškam koordinavimui ir abipusiškumui, bendriems mokslinių tyrimų, plėtros ir inovacijų projektams, dalijimuisi geriausia patirtimi, didelio masto mokymo programoms ir kibernetinių išpuolių imitavimui, siekiant pagrindinio tikslo – išplėsti bendrus reagavimo pajėgumus.

1.12. Komitetas ragina vyriausiąjį įgaliotinį peržiūrėti dabartinius dvišalius dialogus kibernetinio saugumo srityje ir pradėti papildomas diskusijas su kitomis šalimis bei atitinkamomis tarptautinėmis organizacijomis, siekiant sukurti pasaulinę tarptautinės teisės kibernetinėje erdvėje laikymosi sistemą, ypač daug dėmesio skiriant abipusiškumui. Komitetas mano, kad ES yra tinkamai pasirengusi imtis vadovaujamo vaidmens tarptautinėse diskusijose dėl kibernetinio saugumo ateities, ypač Jungtinėse Tautose, nes turi tvirtą pagrindinių demokratinių laisvių pagrindą.

1.13. ES turėtų griežtai pasisakyti prieš bet kokią piliečių socialinio vertinimo sistemą. EESRK aiškiai nurodo, kad tikra demokratija negali egzistuoti be veiksmingos asmens duomenų apsaugos, ir mano, kad atsakingas ir veiksmingas duomenų valdymas yra labai svarbus siekiant, kad hipersusietumas taptų konkurenciniu pranašumu.

2. **Įžanga ir bendrosios pastabos**

2.1. Skaitmeninės visuomenės plėtra atneša daugybę kibernetinio saugumo grėsmių, kylančių dėl technologijų pažangos. Per pastaruosius kelerius metus kibernetinių išpuolių skaičius ir sudėtingumas labai išaugo, o tai kenkia tiek viešųjų, tiek privačiųjų subjektų saugumui. Nesvarbu, ar kalbame apie išpirkos reikalavimo programinę įrangą, kenkimo programinę įrangą, išpuolius el. paštu, duomenų saugumo pažeidimus, dezinformaciją, paskirstytojo paslaugos trikdymo atakas (DDoS atakas) ar kitų formų išpuolius – visi jie nuosekliai ir nuolat kelia grėsmę visos ES saugumui.

2.2. EESRK palankiai vertina bendrą komunikatą „ES kibernetinės gynybos politika“ ([2]) ir mano, kad dabar tinkamas metas skubiai ir koordinuotai veikti ES lygmeniu, įtraukiant civilines ir karines kibernetinės erdvės ekosistemas ir užtikrinant tinkamą investicijų į kibernetinės gynybos pajėgumus sistemą. Vis dėlto Komitetas atkreipia dėmesį į tai, kad komunikate tik deklaruojamas pasiryžimas veikti ir išvardijamos būsimos ES iniciatyvos, kurios turėtų padėti pasiekti rezultatų, ir mano, kad neįmanoma įvertinti, ar šie būsimi įsipareigojimai iš tikrųjų bus vykdomi, nes būsimos teisėkūros institucijų derybos, savaime suprantama, turės įtakos galutiniams ES kibernetinio saugumo veiksmų plano rezultatams.

2.3. Dėl Rusijos išpuolio prieš KA-SAT palydovinį tinklą, sutrikdžiusio Ukrainos karinių pajėgų ryšius, ir neseniai kilusio skandalo, kai kelios gynybos bendrovės pasamdė Éric Léandri kibernetiniam šnipinėjimui jų vardu vykdyti, kibernetinis saugumas ES atsidūrė pirmoje grėsmių saugumui sąrašo vietoje. Nors BDAR yra patikimas ES teisės aktas ir jau galioja kelerius metus, akivaizdu, kad vis daugiau prieinamų duomenų yra nesaugūs, o rizika, kad trečiosios šalys peržengs teisėtumo ribas, kasdien didėja.

2.4. Atsižvelgiant į tarpvalstybinį kibernetinių išpuolių pobūdį, ES lygmens koordinavimas yra būtinas siekiant sumažinti dabartinį susiskaidymą ir užtikrinti, kad valstybės narės būtų pasirengusios bendradarbiauti ir bendrai investuoti. Tai ypač svarbu būsimiems atvejams, kad vienai valstybei narei patyrus išpuolį visos kitos turėtų turėti galimybę nedelsiant suteikti paramą.

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

3.1. Komitetas atkreipia dėmesį į paskelbtas plataus užmojo iniciatyvas įsteigti ES kibernetinės gynybos koordinavimo centrą, plėtoti projektą „CyDEf-X“, sukurti greitojo reagavimo į kibernetines grėsmes komandas, parengti ES kibernetinės gynybos solidarumo iniciatyvą ir išnagrinėti IRT produktams, paslaugoms ir procesams skirtų kibernetinio saugumo sertifikavimo schemų kūrimo galimybes. EESRK rekomenduoja visoms valstybėms narėms įsipareigoti pasirengti kasdien bet kuriuo paros metu užtikrinti greitąjį reagavimą, o ES koordinavimo centrui dalyvauti vertinant ir rengiant reguliarias ataskaitas apie valstybių narių pasirengimą kibernetiniams išpuoliams ir Europos reagavimo į kibernetines krizes mechanizmo veiksmingumą, daugiausia dėmesio skiriant tiek kariniams pajėgumams, tiek TIS 2 direktyvoje nustatytiems ypatingos svarbos sektoriams. Kiekviena valstybė narė turėtų turėti specialiai parengtus specialistus, kurie galėtų imtis intervencinių priemonių kibernetinių incidentų atveju, ir turėtų reguliariai tikrinti savo gebėjimą imtis tokių priemonių kitose valstybėse narėse.

3.2. Nors komunikate pateikiamas ilgas laipsniškai vykdytinų patobulinimų sąrašas, EESRK tikėjosi, kad bus parengtas išsamus šių iniciatyvų įgyvendinimo planas su aiškiu valdymu ir pateikimo bei priėmimo terminais. Be to, Komitetas tikėjosi, kad organizuotai pilietinei visuomenei bus suteiktas svarbesnis vaidmuo rengiant šiuos pasiūlymus.

3.3. EESRK mano, kad valstybės narės turi stiprinti savo vidaus pajėgumus, kad galėtų kovoti su kibernetinėmis grėsmėmis ir kartu dalyvauti bendradarbiavimo projektuose bei dalytis informacija ir geriausia patirtimi su partneriais iš kitų valstybių narių. Reikia skubiai investuoti į visų valstybių narių kibernetinės gynybos pajėgumus, spartų technologijų diegimą ([3]) ir bendrą pasirengimą nustatyti kibernetinius išpuolius, po jų atsigauti ir apsisaugoti. Komitetas mano, kad siekiant remti Sąjungos kibernetinio saugumo savarankiškumą reikia sukurti arba iš privačiojo sektoriaus perimti dinamišką testavimo ir dalijimosi informacija tikruoju laiku platformą, kurioje daugiausia dėmesio būtų skiriama šiuo metu trūkstamų pajėgumų nustatymui.

3.4. EESRK pritaria nuomonei, kad šiame etape karinės kibernetinės erdvės operacijos turėtų ir toliau griežtai priklausyti valstybių narių kompetencijai; Komitetas remia paskelbtą ES karinių kompiuterinių incidentų tyrimo tarnybų (*milCERT*), reagavimo į kompiuterinius saugumo incidentus tarnybų (CSIRT) ir EUIBA kompiuterinių incidentų tyrimo tarnybos (CERT-EU) bendradarbiavimą.

3.5. Neseniai priimtoje TIS 2 direktyvoje ir Direktyvoje dėl ypatingos svarbos subjektų atsparumo ([4]) jau nustatytos konkrečios nacionalinės ir sektorių pareigos ES kibernetinės gynybos sistemoje. Reikia imtis tolesnių veiksmų ES kolektyvinio nustatymo pajėgumams pagerinti, todėl EESRK ragina investuoti į mokslinius tyrimus ir plėtrą, kad būtų plėtojami pažangieji ES pajėgumai.

([2]) Komisijos komunikatas „ES kibernetinės gynybos politika“.
([3]) Pvz., NATO iniciatyva „Accelerator for the North Atlantic“ (DIANA).
([4]) Direktyva dėl ypatingos svarbos subjektų atsparumo.

4. **Apsaugoti ES gynybos ekosistemą**

4.1. EESRK mano, kad dėl savo sudėtingumo ir sparčiai kintančių technologinių iššūkių pasikeitė gynybos ekosistema ir kad kibernetinis saugumas tapo bendra tema tiek kariniam, tiek civiliniam sektoriams, taip pat – ES piliečiams. Civilinių ir karinių ekosistemų bendradarbiavimas šiuo metu yra svarbesnis nei kada nors anksčiau ir turėtų prisidėti prie veiksmingesnio krizių valdymo, taip pat prie nuolatinės pažangos ir sąveikumo, siekiant išvengti nereikalingo pastangų ir investicijų dubliavimo ar dauginimo. Valstybės narės turėtų būti pasirengusios atlikti nacionalinių ypatingos svarbos infrastruktūros objektų testavimą nepalankiausiomis sąlygomis, kad įvertintų ir padidintų atsparumą būsimiems kibernetiniams išpuoliams.

4.2. EESRK mano, kad investuojant į kibernetinę gynybą pirmenybė turėtų būti teikiama ES piliečių ir ypatingos svarbos infrastruktūros objektų apsaugai. Atsižvelgdamas į spartų skaitmeninės pertvarkos tempą ir sparčią grėsmių pobūdžio raidą, Komitetas primygtinai ragina ES ir valstybes nares laiku susitarti dėl prioritetų ir investicijų atnaujinimo, išsamiai konsultuojantis su atitinkamais privačiais suinteresuotaisiais subjektais. Daiktų interneto prietaisai dažnai būna ne taip gerai apsaugoti kaip tradiciniai, todėl EESRK ragina užtikrinti minimalų saugumo lygį panaudojant tapatybės ir prieigos valdymo (angl. *identity and access management*, IDAM) platformas. Kadangi sertifikavimas yra pagrindinis būdas užtikrinti aukštesnį saugumo lygį, Komitetas ragina taikant naują ES sertifikavimo metodą daugiau dėmesio skirti daiktų interneto saugumui.

4.3. ES turi didinti atsparumą kibernetiniams išpuoliams ir sukurti veiksmingas atgrasymo nuo jų priemones. Ypatingos svarbos infrastruktūros objektai turi būti apsaugoti nuo bet kokios rūšies kibernetinių išpuolių, be kita ko, pasitelkiant ES gynybos sistemas. Komitetas mano, kad ES strateginis interesas yra išsaugoti ir plėtoti Sąjungos esminius pajėgumus užtikrinti savo skaitmeninės ekonomikos, visuomenės ir demokratijos saugumą, pasiekti visišką skaitmeninį suverenumą, nes tai vienintelis būdas apsaugoti ypatingos svarbos technologijas ir teikti veiksmingas pagrindines kibernetinio saugumo paslaugas. Priklausomybės nuo trečiųjų šalių mažinimas taip pat yra gyvybiškai svarbus ES strateginiam savarankiškumui. EESRK mano, kad sektorinės ES agentūros (ENISA, EASA, ESGA, EMA, EBI, EKA, HADEA ir kt.) turėtų dalyvauti šiame procese ir teikti rekomendacijas rengiant kibernetinio saugumo schemas.

4.4. COVID-19 pandemija paspartino skaitmeninę pertvarką ir tradicines darbo formas pakeitė mišrios ir (arba) nuotolinio darbo formos, todėl atsirado naujų darbo santykių bei lūkesčių, taip pat nauja ir vis gausėjanti skaitmeninių klajoklių klasė. EESRK atkreipia dėmesį į sparčius darbo rinkos pokyčius, dėl kurių įmonės, naudodamos tapatybės ir prieigos valdymo (IAM) ir privilegijuotos prieigos valdymo (PAM) sprendimus, ėmė taikyti nulinio pasitikėjimo architektūrą. Komitetas mano, kad toks įmonių išteklių valdymas kelia naujų iššūkių, susijusių su kibernetinėmis grėsmėmis, ir mano, kad būtina remti privatųjį sektorių didinant jų novatoriškų skaitmeninių sprendimų saugumo lygį.

4.5. EESRK yra gana nusivylęs Komisijos teiginiu, kad „[į]gyvendinimo planas galėtų būti parengtas bendradarbiaujant su valstybėmis narėmis“, ir mano, kad toks įgyvendinimo planas yra privalomas. Jis mano, kad jis turėtų būti parengtas drauge su valstybėmis narėmis ir kuo skubiau įgyvendintas. Komitetas yra susirūpinęs dėl negriežtos Komisijos pozicijos ir ragina ES institucijas bei valstybes nares sudaryti palankesnes sąlygas sparčiai pažangai įgyvendinant paskelbtas iniciatyvas.

5. **Investuoti į kibernetinės gynybos pajėgumus**

5.1. Sparčiai vystantis technologijoms, kibernetinė erdvė tapo naujausia karo veiksmų sritimi po sausumos, jūrų, oro ir kosmoso. Ji taip pat suteikia daug galimybių vykdyti nusikalstamą veiklą piktavaliams kibernetiniams subjektams, pradedant nepriklausomais įsilaužėliais ir baigiant profesionaliais nusikaltėliais ir net valstybiniais subjektais.

5.2. Investicijos į mokslinius tyrimus ir plėtrą yra gyvybiškai svarbios, todėl EESRK pritaria tiksliniam finansavimui pagal Skaitmeninės Europos programą, Europos gynybos fondą, programą „Europos horizontas“ ir nacionalinius ekonomikos gaivinimo ir atsparumo didinimo planus. Tačiau Komitetas pageidautų, kad būtų daugiau tarpvalstybinių projektų, kuriuose daugiausia dėmesio būtų skiriama kibernetinės gynybos sistemų bendradarbiavimui ir sąveikumui visose valstybėse narėse, taip pat didesnės finansavimo priemonių, ypač susijusių su novatoriškomis MVĮ, sinergijos siekiui.

5.3. Kaip paskelbta dar 2020 m. ES kibernetinio saugumo strategijoje, Komitetas pažymi, kad Jungtinis kibernetinio saugumo padalinys turi būti įsteigtas šiais metais, ir laukia naujienų apie šio proceso užbaigimą bei ES pasirengimą reaguoti į didelio masto kibernetinius incidentus. EESRK tikisi, kad dėl to padidės ES informuotumas apie kibernetinės gynybos padėtį ir sustiprės bendras gebėjimas reaguoti į kibernetines grėsmes ir po jų atsigauti.

5.4. EESRK pritaria tam, kad būtų pratęsti ECCC įgaliojimai padėti ES kibernetinės gynybos koordinavimo centro veiklai. Be to, šis tinklas galėtų remti Europos skaitmeninį suverenumą sukuriant konkurencingą Europos pramoninę bazę, skirtą pagrindiniams technologiniams pajėgumams ir iš dalies grindžiamą sutartinės viešojo ir privačiojo sektorių partnerystės pagrindu atliktais darbais. Paaiškėjo, kad viešojo ir privačiojo sektorių partnerystė yra veiksmingiausias visos skaitmeninės ekosistemos kibernetinio saugumo didinimo būdas, tačiau ji negali būti vienkryptė: viešosios institucijos taip pat turi dalytis savo žvalgybos informacija su privačiuoju sektoriumi.

5.5. EESRK pažymi, kad siekdama reaguoti į būsimus kvantinių kompiuterių mėginimus įsilaužti ES turi nedelsdama investuoti į pažangiąsias technologijas, pavyzdžiui, postkvantinę kriptografiją. Komitetas mano, kad vidutinės trukmės laikotarpiu Europa būtinai turi siekti savarankiškumo ir tvirtai pasisako už tai, kad ES įsisteigusios įmonės kurtų moksliniams tyrimams ir gamybai skirtus įrenginius. EESRK mano, kad svarbu padidinti ES išteklius skaitmeniniams moksliniams tyrimams ir inovacijoms bei remti operatorių ir tiekėjų investicijas į naujas technines saugumo funkcijas, taip pat susijusias su naujomis tendencijomis, pavyzdžiui, išplėstine realybe ir metavisata. Visų pirma labai svarbu sukurti Europos paskirstytąją debesijos infrastruktūrą, grindžiamą Europos taisyklėmis, reglamentuojančiomis tokius klausimus kaip duomenų saugojimas ir tvarkymas ([5]).

5.6. MVĮ turėtų būti skiriamas ypatingas dėmesys ir sudaromos sąlygos naudotis finansavimo programomis, kurios padėtų joms geriau pasirengti kibernetiniams išpuoliams, taip pat pagalba, mokymo ir švietimo programomis, kurios padėtų joms suprasti kibernetinę riziką ir išmokytų apsisaugoti. ES turėtų numatyti paskatų mechanizmą, kuriuo būtų skatinamas laipsniškas MVĮ supažindinimas su kibernetinio saugumo klausimais.

5.7. Komisija apskaičiavo, kad šiuo metu kibernetinio saugumo sektoriuje trūksta pusės milijono žmonių, todėl EESRK palankiai vertina pasiūlymą įsteigti Kibernetinių įgūdžių akademiją. Akivaizdu, kad valstybių narių lygmens pastangų nepakanka įgūdžių trūkumui sumažinti, todėl Komitetas siūlo, kad kartu su akademijos įsteigimu Komisija pasinaudotų ir Europos įgūdžių metų galimybėmis ir koordinuotų bei finansuotų didelio masto mokymo programas ir profesinio rengimo bei mokymo programas ES lygmeniu, kuriose dalyvautų visos valstybės narės ir kuriose daugiausia dėmesio būtų skiriama visų kibernetinės gynybos srityje veikiančių agentūrų bei įstaigų, taip pat privačių civilinių tinklų aprūpinimui kvalifikuota darbo jėga. Ypatingas dėmesys turi būti skiriamas darbuotojų mokymui, ypač gamtos mokslų, technologijos, inžinerijos ir matematikos (STEM) srityse.

5.8. Be to, EESRK mano, kad labai svarbu didinti piliečių informuotumą apie kibernetinį saugumą, kad būtų sumažintas kibernetinių išpuolių poveikis, ypač kalbant apie pagrindinius, prieš plačiąją visuomenę nukreiptus kibernetinius nusikaltimus. Komitetas ragina parengti kibernetinio saugumo mokymo programas ir visą gyvenimą trunkančio kibernetinio saugumo mokymo programas, kuriose daugiausia dėmesio būtų skiriama kibernetinių įgūdžių lavinimui ir platesniam piliečių, ypač jaunosios kartos, supažindinimui su kibernetiniu saugumu bei susidomėjimo juo skatinimui. EESRK pasisako už tai, kad kibernetinio saugumo klausimai būtų įtraukti į visas būsimas ES viešosios politikos sritis ir kad visuomenė būtų informuojama apie kibernetines grėsmes, be kita ko, rengiant nemokamas mokymo programas visiems gyventojams, nemokamas informacines mobiliųjų telefonų programėles arba skelbiant informaciją geriausiu televizijos eterio laiku. Kartu su šiais veiksmais turi būti siekiama plataus masto kultūrinių pokyčių visais visuomenės lygmenimis, kad būtų ugdomas į „kibernetinį saugumą orientuotas“ požiūris.

5.9. EESRK mano, kad ypač svarbu vertinti tiekėjų rizikos profilį ir taikyti atitinkamus apribojimus tiems tiekėjams, kurie laikomi labai pavojingais, be kita ko, taikant būtinus draudimus pagrindiniams objektams ir taikomosioms programoms, kurie ES koordinuotame rizikos vertinime laikomi ypatingos svarbos ir konfidencialūs, taip pat sertifikuojant patikimus aparatinės ir programinės įrangos tiekėjus.

6. **Partneris bendriems uždaviniams spręsti**

6.1. Pasirengimo būsimiems kibernetiniams išpuoliams lygis valstybėse narėse labai skiriasi. EESRK mano, kad pirmas neatidėliotinas žingsnis – sukurti ES vidaus geriausios patirties komunikacijos platformą, kurioje kibernetinio saugumo srityje didžiausią pažangą padariusios valstybės narės galėtų dalytis savo žiniomis su kitomis šalimis ir sudaryti joms palankesnes sąlygas jomis naudotis. Tai padėtų padidinti nacionalinių subjektų tarpusavio pasitikėjimą. Antra, Komitetas mano, kad, siekiant padidinti produktų ir paslaugų kibernetinį saugumą visoje ES, reikia glaudesnio valstybinių ir nevalstybinių subjektų bendradarbiavimo vidaus rinkoje. EESRK taip pat siūlo sukurti bendrą ES platformą, skirtą pranešti apie kibernetinius incidentus, taip pat joje paskelbti ES visų kibernetinių nusikaltimų vykdytojų juodąjį sąrašą.

([5]) Pvz., Prancūzijos ir Vokietijos iniciatyva „Gaia-X“.

6.2. EESRK nuomone, glaudus bendradarbiavimas su NATO sąjungininkais karinėje srityje turi būti sutelktas ne tik į gebėjimų stiprinimą ir ankstyvą nustatymą, bet ir į bendrus mokslinių tyrimų, plėtros ir inovacijų projektus, ekspertų keitimąsi geriausia patirtimi ir nuomonėmis, plačias mokymo programas ir kibernetinių išpuolių imitavimą. Pagrindinis tikslas turėtų būti išplėsti bendrus reagavimo pajėgumus ir sukurti sinergiją kovai su būsimomis hibridinėmis grėsmėmis, atsižvelgiant į 2016 m. Varšuvoje ir 2018 m. Briuselyje priimtas bendras deklaracijas. Dar yra neišnaudotų ES ir NATO bendradarbiavimo galimybių, o sparti pažanga gali realiai padėti užtikrinti mūsų piliečių ir visuomenės saugumą.

6.3. Komitetas mano, kad turi vykti diskusijos pasauliniu lygmeniu ir su mūsų tarptautiniais partneriais ir turėtų būti sudarytos sąlygos skatinti atvirą pasaulinę kibernetinę erdvę, kurioje ginamos žmogaus teisės, pagrindinės laisvės ir teisinės valstybės principas, ir daugiausia dėmesio skiriama privalomų tarptautinių standartų rengimui sektoriuose, kuriuose sparčiai vyksta skaitmeninė plėtra. EESRK rekomenduoja vyriausiajam įgaliotiniui peržiūrėti esamus dvišalius dialogus kibernetinio saugumo srityje ir pradėti tolesnes derybas su kitomis šalimis bei atitinkamomis tarptautinėmis organizacijomis, siekiant sukurti pasaulinę tarptautinės teisės taikymo kibernetinėje erdvėje sistemą, grindžiamą griežta abipusiškumo sąlyga.

6.4. Galiausiai Komitetas mano, kad ES gali geriausiai vadovauti tarptautinėms diskusijoms dėl kibernetinio saugumo ateities, ypač diskusijoms JT, nes turi tvirtą pagrindinių demokratinių laisvių pagrindą. ES taip pat turi dalyvauti kovoje su totalitariniais režimais, kurie vykdo piliečių duomenų stebėseną ir pažeidžia jų teises bei laisves, taip pat turėtų ryžtingai pasisakyti prieš bet kokią socialinio vertinimo sistemą, nukreiptą prieš piliečius. EESRK aiškiai nurodo, kad tikros demokratijos negalima sukurti be tikros asmens duomenų apsaugos, ir mano, kad atsakingas ir veiksmingas duomenų valdymas yra gyvybiškai svarbus siekiant hipersusietumą paversti pranašumu.

2023 m. birželio 14 d., Briuselis

Europos ekonomikos ir socialinių reikalų komiteto pirmininkas
Oliver RÖPKE