Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl Pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl ES kibernetinio saugumo agentūros ENISA ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas)

(COM(2017) 477 final/2–2017/0225 (COD))

(2018/C 227/13)

Pranešėjas: **Alberto MAZZOLA**

Bendrapranešėjis: **Antonio LONGO**

Konsultavimasis	Europos Parlamentas, 2017 10 23
	Europos Sąjungos Taryba, 2017 10 25
Teisinis pagrindas	Sutarties dėl Europos Sąjungos veikimo 114 straipsnis
Atsakingas skyrius	Transporto, energetikos, infrastruktūros ir informacinės visuomenės skyrius
Priimta skyriuje	2018 2 5
Priimta plenarinėje sesijoje	2018 2 14
Plenarinė sesija Nr.	532
Balsavimo rezultatai	206/1/2
(už/prieš/susilaikė)	

1. **Išvados ir rekomendacijos**

1.1. EESRK mano, kad naujas nuolatinis Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA) įgaliojimas, kurį siūlo Komisija, labai prisidės prie Europos sistemų atsparumo didinimo. Tačiau pridedamo preliminaraus biudžeto ir išteklių, skirtų ENISA, nepakaks, kad agentūra galėtų vykdyti savo įgaliojimus.

1.2. EESRK rekomenduoja visoms valstybėms narėms sukurti instituciją, kuri būtų aiškus ir lygiavertis ENISA atitikmuo, nes daugelis jų to dar nepadarė.

1.3. Be to, EESRK mano, kad pajėgumų stiprinimo srityje ENISA turėtų pirmenybę teikti veiksmams, kuriais remiama e. valdžia ([1]). ES ir visame pasaulyje asmenų, organizacijų ir objektų skaitmeninė tapatybė yra labai svarbi ir užkirsti kelią tapatybės vagystėms ir sukčiavimui internete ir su jais kovoti turėtų būti prioritetas.

1.4. EESRK rekomenduoja, kad ENISA turėtų teikti reguliarias ataskaitas apie valstybių narių kibernetinį pasirengimą, visų pirma dėmesį skirdama Kibernetinio saugumo direktyvos (TIS direktyvos) II priede nurodytiems sektoriams. Kasmetinėse Europos kibernetinio saugumo pratybose turėtų būti įvertinamas valstybių narių pasirengimas ir Europos kibernetinio saugumo reagavimo į krizes mechanizmo veiksmingumas ir parengiamos rekomendacijos.

1.5. EESRK remia pasiūlymą sukurti kibernetinio saugumo kompetencijos tinklą. Šį tinklą remtų Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centras. Šis tinklas prisidėtų prie Europos skaitmeninio suvereniteto sukuriant konkurencingą Europos pramoninę bazę pagrindiniams technologijų pajėgumams, grindžiamiems sutartinės viešojo ir privačiojo sektorių partnerystės (SVPSP) darbu; ši partnerystė turėtų išsiplėtoti į trišalę bendrąją įmonę.

1.6. Žmogiškasis veiksnys yra viena svarbiausių kibernetinių incidentų priežasčių. EESRK nuomone, reikia sukurti tvirtą kibernetinių įgūdžių bazę, gerinti kibernetinę higieną didinant asmenų ir įmonių informuotumą. EESRK remia ES sertifikuotos aukštųjų mokyklų ir specialistų mokymo programos kūrimą.

([1]) Bendroji skaitmeninė rinka. Laikotarpio vidurio peržiūra.

1.7. EESRK mano, kad Europos bendrajai skaitmeninei rinkai taip pat reikalingas vienodas kibernetinio saugumo taisyklių aiškinimas, įskaitant valstybių narių tarpusavio pripažinimą; be to, sertifikavimo sistema ir skirtingų sektorių sertifikavimo schemomis galėtų būti sukurtas bendras pagrindas. Vis dėlto skirtingiems sektoriams turi būti taikomi skirtingi metodai atsižvelgiant į tai, kaip tie sektoriai veikia. Todėl EESRK mano, kad į šį procesą reikėtų įtraukti sektorines ES agentūras (EASA, EGA, EMA ir kt.) ir kai kuriais atvejais, pritariant ENISA, kad būtų užtikrintas nuoseklumas, įgalioti jas rengti kibernetinio saugumo schemas. Minimalūs Europos IT saugumo standartai turėtų būti priimti bendradarbiaujant su Europos standartizacijos komitetu (CEN), Europos elektrotechnikos standartizacijos komitetu (Cenelec) ir Europos telekomunikacijų standartų institutu (ETSI).

1.8. Europos kibernetinio saugumo sertifikavimo grupę, kurią numatoma įsteigti ir kurią remia ENISA, turėtų sudaryti nacionalinės sertifikavimo priežiūros įstaigos, privačiojo sektoriaus suinteresuotieji subjektai, įskaitant įvairių taikymo sričių operatorius ir mokslo bei pilietinės visuomenės subjektus.

1.9. EESRK laikosi nuomonės, kad agentūra, Komisijos vardu vykdydama auditus ir patikrinimus, turėtų stebėti nacionalinių sertifikavimo priežiūros institucijų veiklos rezultatus ir sprendimų priėmimą. Reglamente turėtų būti apibrėžta atsakomybė ir sankcijos už standartų nesilaikymą.

1.10. EESRK mano, kad sertifikavimo veikla turi apimti tinkamą ženklinimo sistemą, kurią reikia taikyti ir importuojamiems produktams, siekiant didinti vartotojų pasitikėjimą.

1.11. Europa, sutelkdama įvairius ES fondus, nacionalines lėšas ir privačiojo sektoriaus investicijas, turėtų didinti investicijas į strateginius tikslus, kurių turėtų būti siekiama vykdant glaudų viešojo ir privačiojo sektorių bendradarbiavimą, taip pat dabartinėje ir būsimoje mokslinių tyrimų bendrojoje programoje sukuriant ES kibernetinio saugumo fondą inovacijoms, moksliniams tyrimams ir technologinei plėtrai. Be to, Europa turėtų sukurti kibernetinio saugumo priemonių įgyvendinimo fondą atverdama naują galimybę dabartinėje ir būsimoje Europos infrastruktūros tinklų priemonėje ir būsimoje ESIF 3.0.

1.12. EESRK mano, kad būtina nustatyti minimalųjį saugumo lygį „įprastiems“ „žmonių interneto“ prietaisams. Tokiu atveju sertifikavimas yra vienas iš svarbiausių būdų užtikrinti aukštesnį saugumo lygį. Daiktų interneto saugumas turėtų būti prioritetas.

2. **Dabartinė kibernetinio saugumo sistema**

2.1. Kibernetinis saugumas yra labai svarbus tiek siekiant užtikrinti klestėjimą ir nacionalinį saugumą, tiek ir pačiam mūsų demokratijos, laisvių ir vertybių sistemos veikimui. JT visuotinio kibernetinio saugumo indekso (angl. *UN Global Cybersecurity Index*) ataskaitoje teigiama, kad „kibernetinis saugumas yra ekosistema, kurioje įstatymai, organizacijos, įgūdžiai, bendradarbiavimas ir techninis įgyvendinimas turi derėti tarpusavyje, nes tik tada ši sistema bus efektyviausia“, ir priduriama, kad kibernetinis saugumas „užima vis svarbesnę vietą šalių sprendimus priimančių asmenų mintyse“.

2.2. Dėl interneto revoliucijos poreikis užtikrinti saugią ekosistemą tampa itin svarbus. Ši revoliucija ne tik iš naujo apibrėžė tuos sektorius, kurie veikia pagal modelį verslas vartotojui (B2C), pavyzdžiui, medijų, mažmeninės prekybos ir finansinių paslaugų sektorius, bet ir keičia apdirbamosios pramonės, energetikos, žemės ūkio, transporto ir kitus ekonomikos pramonės sektorius, kurie kartu sudaro beveik du trečdalius pasaulio bendrojo vidaus produkto, taip pat paslaugų infrastruktūrą ir žmonių sąveiką su viešojo administravimo institucijomis.

2.3. Bendrosios skaitmeninės rinkos strategija yra paremta prieigos prie prekių, paslaugų ir turinio gerinimu, tinkamos teisinės sistemos skaitmeniniams tinklams ir paslaugoms kūrimu ir duomenimis grindžiamos ekonomikos privalumų išnaudojimu. Apskaičiuota, kad įgyvendinus šią strategiją ES ekonomika kasmet būtų papildyta 415 mlrd. EUR. Prognozuojama, kad iki 2022 m. kvalifikuotų kibernetinio saugumo srities darbuotojų trūkumas Europos privačiajame sektoriuje pasieks 350 000 ([2]).

([2]) OL JOIN/2017/0450 final.

2.4. 2014 m. atliktus tyrimą buvo apskaičiuota, kad kibernetinių nusikaltimų ekonominis poveikis Sąjungoje 2013 m. sudarė 0,41 % ES BVP (t. y. apie 55 mlrd. EUR) ([3]).

2.5. Remiantis specialiąja „Eurobarometro“ apklausa Nr. 464a „Europiečių požiūris į kibernetinį saugumą“, 73 % interneto naudotojų yra susirūpinę, kad jų asmens duomenys gali būti nesaugiai laikomi interneto svetainėse, ir 65 % naudotojų baiminasi, kad jų asmens duomenys gali būti nesaugiai laikomi valdžios institucijų. Dauguma respondentų yra susirūpinę, kad gali tapti įvairių rūšių kibernetinių nusikaltimų aukomis, ypač dėl kenkimo programinės įrangos jų įrenginiuose (69 %), tapatybės vagystės (69 %) ir su banko kortele ir elektronine bankininkyste susijusio sukčiavimo (66 %) ([4]).

2.6. Iki šiol jokiai teisinei sistemai nepavyko prisitaikyti prie skaitmeninių inovacijų tempo ir įvairūs teisiniai tekstai padeda po truputį kurti tinkamą sistemą: Telekomunikacijų kodekso peržiūra, Bendrasis duomenų apsaugos reglamentas (BDAR), Tinklų ir informacinių sistemų saugumo direktyva (TIS direktyva), reglamentas dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje (e-IDAS reglamentas), ES ir JAV „privatumo skydas“, direktyva dėl sukčiavimo negrynosiomis mokėjimo priemonėmis ir kt.

2.7. Be ES kibernetinio saugumo agentūros ENISA, kibernetinio saugumo klausimus sprendžia daugelis įvairių organizacijų: Europolas, CERT-ES (Europos institucijų, įstaigų ir agentūrų Kompiuterinių incidentų tyrimo tarnyba), ES žvalgybos ir situacijų centras (ES INTCEN), Europos didelės apimties IT sistemų laisvės, saugumo ir teisingumo erdvėje operacijų valdymo Europos agentūra („eu-LISA“), keitimosi informacija ir jos analizės centrai (ISAC), Europos kibernetinio saugumo organizacija (ECSO), Europos gynybos agentūra (EGA), NATO bendros kibernetinės gynybos kompetencijos centras, Jungtinių Tautų Vyriausybių ekspertų grupė pažangos informacijos ir telekomunikacijų srityje tarptautinio saugumo aspektų klausimais).

2.8. Integruotasis saugumas labai svarbus norint teikti aukštos kokybės prekes ir paslaugas: išmanieji įrenginiai nėra tokie išmanūs, jeigu jie nesaugūs; tas pats pasakytina apie pažangius automobilius, pažangiuosius miestus ir ligonines – visiems jiems reikalingas integruotasis įrenginių, sistemų, struktūrų ir paslaugų saugumas.

2.9. 2017 m. spalio 19–20 d. Europos Vadovų Taryba paragino laikytis bendro požiūrio į ES kibernetinį saugumą vadovaujantis pasiūlytu reformos dokumentų rinkiniu, kuriame raginama laikytis „bendro požiūrio į kibernetinį saugumą: skaitmeniniame pasaulyje reikia pasitikėjimo, o pasitikėjimas gali būti užtikrintas tik tada, jei garantuosime labiau iniciatyvų integruotąjį saugumo užtikrinimą visose skaitmeninės politikos srityse, vykdysime tinkamą gaminių ir paslaugų saugumo sertifikavimą ir padidinsime savo pajėgumus užkirsti kelią kibernetiniams išpuoliams, atgrasyti nuo jų, juos aptikti ir į juos reaguoti“ ([5]).

2.10. Savo 2017 m. gegužės 17 d. rezoliucijoje Europos Parlamentas „pabrėžia, kad reikia užtikrinti ištisinį saugumą visoje finansinių paslaugų vertės grandinėje; atkreipia dėmesį į didelę ir įvairią riziką, keliamą kibernetinių išpuolių, nukreiptų prieš mūsų finansų rinkų infrastruktūrą, daiktų internetą, valiutas ir duomenis; […] ragina Europos priežiūros institucijas, reguliariai peržiūrėti galiojančius veiklos standartus, susijusius su finansų įstaigų IRT rizika; be to, ragina priimti Europos priežiūros institucijų gaires dėl valstybių narių kibernetinės rizikos priežiūros; pabrėžia Europos priežiūros institucijų turimų technologinių praktinių žinių svarbą“ ([6]).

2.11. EESRK jau keletą kartų turėjo galimybę iškelti šį klausimą ([7]), įskaitant Talino aukščiausiojo lygio susitikimo metu konferencijoje „Tolesnis e. valdžios gerinimas“ ([8]), ir sukūrė nuolatinę tyrimo grupę dėl skaitmeninės darbotvarkės.

([3]) Komisijos tarnybų darbinis dokumentas „Poveikio vertinimas“, pridedamas prie pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, 1/6 dalis, p. 21, Briuselis, 2017 m. rugsėjo 13 d..

([4]) Specialioji „Eurobarometro“ apklausa Nr. 464a, Wave EB87.4 – *Europeans' attitudes towards cyber security* („Europiečių požiūris į kibernetinį saugumą“), 2017 m. rugsėjo mėn.

([5]) 2017 m. spalio 19 d. Europos Vadovų Tarybos išvados.

([6]) EP rezoliucija A8–0176/2017, 2017 5 17.

([7]) Bendroji skaitmeninė rinka. Laikotarpio vidurio peržiūra.OL C 75, 2017 3 10, p. 124, OL C 246, 2017 7 28, p. 8, OL C 345, 2017 10 13, p. 52, OL C 288, 2017 8 31, p. 62, OL C 271, 2013 9 19, p. 133.

([8]) EESRK pranešimas spaudai Nr. 31/2017, Pilietinės visuomenės diskusija su Tarybai pirmininkausiančia Estija tema „E. valdžia ir kibernetinis saugumas: https://www.eesc.europa.eu/en/news-media/press-releases/civil-society-debates-e-government-and-cybersecurity-incomingestonian-presidency.

3. **Komisijos pasiūlymai**

3.1. Kibernetinio saugumo dokumentų rinkinį sudaro bendras komunikatas, kuriame peržiūrima ankstesnė Europos kibernetinio saugumo strategija (2013 m.), taip pat Kibernetinio saugumo aktas, kuriame daugiausia dėmesio skiriama naujiems ES tinklų ir informacijos apsaugos agentūros (ENISA) įgaliojimams ir siūlomai sertifikavimo sistemai.

3.2. Strategiją sudaro trys pagrindinės dalys: atsparumas, atgrasymas ir tarptautinis bendradarbiavimas. Atgrasymo dalyje daugiausia dėmesio skiriama kibernetinių nusikaltimų klausimams, įskaitant Budapešto konvenciją, o tarptautinio bendradarbiavimo dalyje aptariama kibernetinė gynyba, kibernetinė diplomatija ir bendradarbiavimas su NATO.

3.3. Pasiūlyme numatytos šios naujos iniciatyvos:

— stipresnės ES kibernetinio saugumo agentūros sukūrimas,

— ES masto kibernetinio saugumo sertifikavimo sistemos įdiegimas,

— spartus TIS direktyvos įgyvendinimas.

3.4. Atsparumui skirtoje dalyje siūlomi kibernetinio saugumo užtikrinimo veiksmai, susiję visų pirma su rinkos klausimais, TIS direktyva, greitu reagavimu į krizes, ES kompetencijos vystymu, švietimo ir mokymo kibernetinių įgūdžių ir kibernetinės higienos srityje skatinimu ir informuotumo didinimu.

3.5. Be to, Kibernetinio saugumo akte siūloma sukurti IRT produktų ir paslaugų Europos kibernetinio saugumo sertifikavimo sistemą.

3.6. Kibernetinio saugumo akte taip pat siūloma sustiprinti ENISA, kaip ES kibernetinio saugumo agentūros, vaidmenį suteikiant jai nuolatinį įgaliojimą. Be dabartinių pareigų, ENISA turėtų prisiimti naujas rėmimo ir koordinavimo užduotis šiose srityse: TIS direktyvos įgyvendinimo rėmimo, ES kibernetinio saugumo strategijos, ES kibernetinio saugumo projekto, pajėgumų stiprinimo, žinių ir informacijos, informuotumo didinimo, su rinka susijusių užduočių, pavyzdžiui, paramos standartizacijos ir sertifikavimo sistemoms, mokslinių tyrimų ir inovacijų, visos Europos kibernetinio saugumo pratybų, ir veikti kaip reagavimo į kompiuterių saugumo incidentus tarnybos (CSIRT) tinklo sekretoriatas.

4. **Bendrosios pastabos. Apžvalga**

4.1. ***Aplinkybės. Atsparumas***

4.1.1. *Bendroji kibernetinio saugumo rinka*

Rūpestingumo pareiga. Bendrame komunikate paminėtas rūpestingumo pareigos principo plėtojimas siekiant saugių kūrimo ciklo procesų taikymo yra įdomi sąvoka, kurią reikėtų plėtoti su ES pramone ir kuri padėtų suformuoti visapusišką požiūrį į ES teisės aktų laikymąsi. Ateityje kuriant bet kokį produktą saugumas turėtų tapti savaime suprantamu standartu.

Atsakomybė. Dėl sertifikavimo bus lengviau nustatyti atsakomybę kilus ginčui.

4.1.2. TIS direktyva. Energetika, transportas, bankininkystė ir finansai, sveikata, vanduo, skaitmeninė infrastruktūra, e. prekyba.

EESRK mano, kad labai svarbu visapusiškai ir veiksmingai įgyvendinti TIS direktyvą siekiant užtikrinti ypatingos svarbos nacionalinių sektorių atsparumą.

EESRK mano, kad keitimąsi informacija tarp viešojo ir privataus sektorių subjektų reikėtų sustiprinti pasitelkiant keitimosi informacija ir jos analizės centrus (ISAC). Remiantis šiuo metu naudojamo mechanizmo vertinimu ir (arba) analize, reikėtų sukurti tinkamą mechanizmą, kuris leistų saugiai keistis patikima informacija keitimosi informacija ir jos analizės centruose (ISAC) ir tarp ISAC ir CSIRT.

4.1.3. *Greitas reagavimas į krizes*

Projektu bus užtikrintas veiksmingas operatyvinis reagavimas ES ir valstybių narių lygmenimis į didelio masto incidentą. Komitetas pabrėžia, kad būtina įtraukti privatųjį sektorių; kuriant operatyvinio reagavimo mechanizmą reikėtų atsižvelgti ir į esminių paslaugų operatorius, kadangi jie gali suteikti vertingos informacijos apie grėsmes ir (arba) padėti nustatyti grėsmes ir didelio masto krizes ir į jas reaguoti.

Bendrame komunikate siūloma kibernetinius incidentus įtraukti į ES krizių valdymo mechanizmus. Nors EESRK supranta, kad išpuolio atveju reikalingas bendras atsakas ir solidarumas, būtina geriau suprasti, kaip tai galėtų būti taikoma turint omenyje, kad kibernetinės grėsmės paprastai pasklinda įvairiose šalyse. Nacionalinės ekstremaliosios situacijos atveju naudojamomis priemonėmis būtų galima dalytis tik iš dalies, jei to prireiktų vietos lygmeniu.

4.1.4. *ES kompetencijos didinimas*

Kad ES būtų iš tiesų konkurencinga pasauliniu mastu ir siekiant sukurti tvirtą technologinį pagrindą, labai svarbu sukurti nuoseklią, ilgalaikę sistemą, kuri apimtų visus kibernetinio saugumo vertės grandinės etapus. Šiuo požiūriu, siekiant sukurti ES kibernetinio saugumo vertės grandinę, labai svarbu skatinti Europos regioninių ekosistemų bendradarbiavimą. EESRK palankiai vertina pasiūlymą sukurti kibernetinio saugumo kompetencijos tinklą.

Šiuo tinklu būtų galima prisidėti prie Europos skaitmeninio suvereniteto sukuriant konkurencingą Europos pramoninę bazę ir pagrindinių technologijų pajėgumų atveju sumažinant priklausomybę nuo už ES ribų sukauptos praktinės patirties, padėti rengti technines pratybas, praktinius seminarus ir netgi organizuoti būtiniausios kibernetinės higienos mokymą specialistams ir ne specialistams, taip pat, remiantis SVPSP darbu, skatinti sukurti nacionalinių viešojo ir privataus sektorių organizacijų tinklą, kuris remtų rinkos plėtrą Europoje. „Tobulinant SVPSP turėtų pavykti ją optimizuoti, pritaikyti ar išplėsti“, (Estijos, Bulgarijos ir Austrijos trijų valstybių narių kibernetinio saugumo darbo programa) įsteigiant trišalę (Komisijos, valstybių narių ir bendrovių) bendrąją įmonę.

Kad šis tinklas efektyviai veiktų ir pasiektų Europos lygmeniu siūlomus tikslus, jis turėtų būti grindžiamas aiškiai apibrėžta valdymo sistema.

Šis tinklas Europos lygmeniu turėtų būti remiamas Kibernetinio saugumo mokslinių tyrimų ir kompetencijos centro (CRCC) ir sujungti visoje ES veikiančius nacionalinius kompetencijos centrus. CRCC ne tik koordinuotų ir valdytų mokslinius tyrimus, kaip kitose bendrosiose įmonėse, bet ir leistų veiksmingai kurti Europos kibernetinio saugumo ekosistemą, kuri remtų ES inovacijų diegimą ir įgyvendinimą.

4.2. ***Aplinkybės. Atgrasymas***

4.2.1. Kova su kibernetiniais nusikaltimais yra vienas iš svarbiausių prioritetų nacionaliniu ir Europos lygmenimis ir jai reikalingas tvirtas politinis įsipareigojimas. Atgrasymo veikla turėtų būti vykdoma remiantis tvirta viešojo ir privačiojo sektorių partneryste, užtikrinant veiksmingą keitimąsi informacija ir patirtimi tiek nacionaliniu, tiek Europos lygmeniu. Būtų galima numatyti galimybę išplėsti Europolo veiklą įtraukiant kibernetinę kriminalistiką ir stebėjimą.

4.3. ***Aplinkybės. Tarptautinis bendradarbiavimas***

4.3.1. Siekiant sustiprinti Europos gebėjimą užkirsti kelią didelio masto kibernetiniams išpuoliams, nuo jų atgrasyti ir į juos reaguoti, labai svarbu užmegzti ir išlaikyti patikimą bendradarbiavimą su trečiosiomis šalimis plėtojant kibernetinio saugumo diplomatiją ir įmonių partnerystes. Europa turėtų stiprinti savo bendradarbiavimą su JAV, Kinija, Izraeliu, Indija ir Japonija. Modernizuojant ES eksporto kontrolę, turėtų būti užkirstas kelias žmogaus teisių pažeidimams ar netinkamam technologijų naudojimui kenkiant pačios ES saugumui, taip pat turėtų būti užtikrinama, kad ES pramonė nenukentėtų dėl trečiosios šalies pasiūlymų. Reikėtų numatyti *ad hoc* strategiją narystės siekiančioms šalims, kad būtų galima pasiruošti keitimuisi neskelbtinais tarpvalstybiniais duomenimis, įskaitant galimybę stebėtojų teisėmis dalyvauti kai kuriuose ENISA priklausančių šalių veiksmuose – šios narystės siekiančios šalys turėtų būti išdėstytos eiliškumo tvarka priklausomai nuo jų pasiryžimo kovoti su kibernetiniais nusikaltimais ir gali būti numatoma sudaryti „juodąjį sąrašą“.

4.3.2. EESRK palankiai vertina tai, kad į antrąjį galimo būsimo ES kibernetinio saugumo kompetencijos centro kūrimo etapą numatoma įtraukti kibernetinę gynybą. Todėl Europa tuo tarpu galėtų apsvarstyti galimybę plėtoti dvejopos paskirties gebėjimus, be kita ko, pasinaudojant Europos gynybos fondu ir kibernetinės gynybos mokymo ir švietimo platforma, kurią numatoma sukurti iki 2018 m. Atsižvelgdamas į abipusiai pripažįstamą potencialą ir grėsmes, EESRK mano, kad būtina plėtoti ES ir NATO bendradarbiavimą; be to, Europos pramonės subjektai turėtų atidžiai stebėti ES ir NATO bendradarbiavimo dėl didesnio kibernetinio saugumo standartų sąveikumo ir kitų formų bendradarbiavimo raidą formuojant ES požiūrį į kibernetinę gynybą.

4.4. ***ES sertifikavimo sistema***

4.4.1. EESRK yra įsitikinęs, kad Europa turi įveikti kibernetinio saugumo susiskaidymo iššūkį užtikrindama vienodą taisyklių aiškinimą, įskaitant valstybių narių savitarpio pripažinimą bendroje sistemoje, kad būtų sudarytos palankios sąlygos bendrosios skaitmeninės rinkos apsaugai. Sertifikavimo sistema galėtų suteikti būtiną bendrą pagrindą (jei reikia, su konkrečiomis nuostatomis aukštesniems lygmenims), kuris užtikrintų vertikaliųjų sektorių sinergiją ir sumažintų dabartinį susiskaidymą.

4.4.2. EESRK palankiai vertina tai, kad sukurta ES kibernetinio saugumo sertifikavimo sistema ir įvairių sektorių sertifikavimo schemos, paremtos pakankamais reikalavimais ir parengtos bendradarbiaujant su pagrindiniais suinteresuotaisiais subjektais. Tačiau patekimo į rinką laikas ir sertifikavimo išlaidos, taip pat kokybė ir saugumas yra svarbiausi veiksniai, į kuriuos turi būti atsižvelgta. Sertifikavimo schemomis siekiama didinti saugumą atsižvelgiant į dabartinius poreikius ir informaciją apie grėsmes; jos turi būti lanksčios ir nebaigtinės, kad prireikus jas būtų galima atnaujinti. Skirtingiems sektoriams turi būti taikomi skirtingi metodai atsižvelgiant į tai, kaip tie sektoriai veikia. Todėl EESRK mano, kad į procesą reikėtų įtraukti sektorines ES agentūras (EASA, EBI, EGA, EMA ir kitas) ir kai kuriais atvejais, pritariant ENISA, kad būtų išvengta dubliavimosi ir nuoseklumo trūkumo, įgalioti jas tobulinti kibernetinio saugumo schemas.

4.4.3. Komitetui svarbu, kad sertifikavimo sistema būtų paremta bendra Europos kibernetinio saugumo apibrėžtimi ir IRT standartais, kurie būtų kiek įmanoma pripažįstami tarptautiniu mastu. Atsižvelgiant į laiką ir nacionalines prerogatyvas, minimalūs Europos IT saugumo standartai turėtų būti priimti bendradarbiaujant su Europos standartizacijos komitetu (CEN), Europos elektrotechnikos standartizacijos komitetu (Cenelec) ir Europos telekomunikacijų standartų institutu (ETSI). Profesiniai standartai turėtų būti vertinami teigiamai, tačiau neturėtų būti teisiškai privalomi ar kliudyti konkurencijai.

4.4.4. Akivaizdu, kad remiantis grėsmių poveikiu įsipareigojimus reikia susieti su skirtingais saugumo užtikrinimo lygiais. Priimant veiksmingus kibernetinio saugumo užtikrinimo pagal sektorius reikalavimus, būtų naudinga užmegzti dialogą su draudimo bendrovėmis. EESRK mano, kad įmonės, siekiančios „aukšto saugumo užtikrinimo lygio“, turėtų būti remiamos ir skatinamos, ypač diegiant gyvybinės svarbos prietaisus ir sistemas.

4.4.5. Atsižvelgdamas į tai, kiek laiko praėjo nuo tada, kai buvo priimta Direktyva 85/374/EEB ([9]), ir į dabartinę technologijų pažangą, EESRK ragina Komisiją apsvarstyti, ar nevertėtų į direktyvos taikymo sritį įtraukti keletą šiame pasiūlyme dėl reglamento pateiktų scenarijų, siekiant užtikrinti saugesnius produktus, kuriems taikoma aukšto lygio apsauga.

4.4.6. EESRK mano, kad Europos kibernetinio saugumo sertifikavimo grupę, kurią numatoma įsteigti ir kurią remia ENISA, turėtų sudaryti nacionalinės sertifikavimo priežiūros įstaigos, privačiojo sektoriaus suinteresuotieji subjektai ir įvairių taikymo sričių operatoriai, kad būtų sukurtos išsamios sertifikavimo schemos. Be to, turėtų būti numatytas šios grupės ir sektoriams atstovaujančių asociacijų iš ES (EEE) (pvz., SVPSP, bankų, transporto, energetikos, federacijų ir kt.) bendradarbiavimas skiriant ekspertus. Ši grupė turėtų galėti atsižvelgti į Europos laimėjimus sertifikavimo srityje (daugiausia remdamasi SO-GIS savitarpio pripažinimo susitarimu, nacionalinėmis ir patentuotomis schemomis) ir siekti išsaugoti Europos konkurencinius pranašumus.

([9]) OL L 210, 1985 8 7 p. 29.

4.4.7. EESRK siūlo šiai suinteresuotųjų subjektų grupei kartu su Europos Komisija suteikti atsakomybę už bendrą sertifikavimo schemų rengimą. Su sektoriais susiję reikalavimai taip pat turėtų būti nustatyti viešojo ir privataus sektorių suinteresuotųjų subjektų (naudotojų ir tiekėjų) bendru sutarimu.

4.4.8. Be to, grupė turėtų reguliariai peržiūrėti sertifikavimo schemas atsižvelgdama į kiekvieno sektoriaus reikalavimus ir prireikus jas pritaikyti.

4.4.9. EESRK pritaria laipsniškam nacionalinių sertifikavimo schemų atsisakymui, kai bus įdiegta Europos sistema, kaip siūloma Reglamento 49 straipsnyje. Bendroji rinka negali veikti esant skirtingoms ir konkuruojančioms nacionalinėms taisyklėms. Todėl EESRK siūlo surašyti visas nacionalines schemas.

4.4.10. EESRK siūlo Komisijai imtis veiksmų skatinti kibernetinio saugumo sertifikavimą ir sertifikatų išdavimą ES bei remti jų pripažinimą visuose tarptautiniuose prekybos susitarimuose.

4.5. ***ENISA***

4.5.1. EESRK mano, kad naujas nuolatinis Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA) įgaliojimas, kurį siūlo Komisija, labai prisidės prie Europos sistemų atsparumo didinimo. Tačiau pridedamo preliminaraus biudžeto ir išteklių, skirtų pertvarkytai ENISA, gali nepakakti, kad agentūra galėtų vykdyti savo įgaliojimus.

4.5.2. EESRK ragina visas valstybes nares sukurti instituciją, kuri būtų aiškus ir panašus ENISA atitikmuo, nes daugelis jų to dar nepadarė. Turėtų būti remiama struktūruota programa, skirta deleguoti į ENISA nacionalinius ekspertus siekiant skatinti keistis geriausia praktika ir stiprinti pasitikėjimą. Komitetas taip pat rekomenduoja Komisijai užtikrinti valstybėse narėse esančios geriausios praktikos pavyzdžių ir veiksmingų priemonių rinkimą ir sklaidą.

4.5.3. Be to, EESRK mano, kad pajėgumų stiprinimo srityje ENISA turėtų pirmenybę teikti veiksmams, kuriais remiama e. valdžia ([10]). Asmenų, organizacijų, bendrovių ir objektų ES ir pasaulinė skaitmeninė tapatybė yra labai svarbi ir užkirsti kelią tapatybės vagystėms ir sukčiavimui internete ir su jais kovoti, taip pat užkirsti kelią pramoninės intelektinės nuosavybės vagystei turėtų būti prioritetas.

4.5.4. ENISA taip pat turėtų teikti reguliarias ataskaitas apie valstybių narių kibernetinį pasirengimą, visų pirma dėmesį skirdama TIS direktyvos II priede nurodytiems sektoriams. Kasmetinėse Europos kibernetinio saugumo pratybose turėtų būti įvertinamas valstybių narių pasirengimas ir Europos kibernetinio saugumo reagavimo į krizes mechanizmo veiksmingumas ir parengiamos rekomendacijos.

4.5.5. EESRK yra susirūpinęs, kad operatyviniam bendradarbiavimui, įskaitant CSIRT tinklo veiklą, numatyta per mažai išteklių.

4.5.6. Dėl užduočių, susijusių su rinka, EESRK mano, kad bendradarbiavimo su valstybėmis narėmis skatinimas ir oficialaus kibernetinio saugumo agentūrų tinklo sukūrimas padėtų sustiprinti suinteresuotųjų subjektų bendradarbiavimą ([11]). Laikas iki produkto pateikimo į rinką yra labai trumpas, o ES bendrovėms labai svarbu pajėgti konkuruoti šioje srityje, todėl ENISA turi turėti galimybę reaguoti į tai atsižvelgdama. EESRK mano, kad ENISA, kaip ir kitos ES agentūros, ateityje galėtų taikyti mokesčių ir rinkliavų sistemą. EESRK yra susirūpinęs, kad dėl ES ir nacionalinių agentūrų konkurencijos dėl kompetencijos sričių gali užtrukti tinkamas ES reguliavimo sistemos sukūrimas ir nukentėti ES bendroji rinka, kaip tai atsitiko kitose srityse.

4.5.7. EESRK pažymi, kad su mokslinių tyrimų ir inovacijų ir tarptautiniu bendradarbiavimu susiję uždaviniai šiuo metu yra labai nedideli.

([10]) Bendroji skaitmeninė rinka. Laikotarpio vidurio peržiūra.
([11]) OL C 75, 2017 3 10, p. 124.

4.5.8. EESRK mano, kad reguliariai vykstančiuose bendruose teisingumo ir vidaus reikalų (TVR) agentūrų posėdžiuose kibernetinis saugumas turėtų būti įprastas diskusijų klausimas, o ENISA ir Europolas turėtų reguliariai bendradarbiauti.

4.5.9. Kadangi kibernetinis pasaulis yra labai inovatyvus, standartai turi būti atidžiai apsvarstomi, kad būtų išvengta kliūčių inovacijoms, o tam būtina sukurti dinamišką sistemą; reikėtų kuo labiau užtikrinti tiek išankstinį, tiek atgalinį suderinamumą siekiant apsaugoti piliečių ir bendrovių investicijas.

4.5.10. Dėl nacionalinių sertifikavimo priežiūros institucijų svarbos EESRK siūlo šiuo reglamentu jau sukurti oficialų valdžios institucijų, įgaliotų su ENISA pagalba spręsti tarpvalstybines problemas, tinklą. Šis tinklas vėliau galėtų tapti atskira agentūra.

4.5.11. Pasitikėjimas yra labai svarbus, tačiau ENISA negali priimti sprendimų ar teikti audito ataskaitų. EESRK laikosi nuomonės, kad agentūra, Komisijos vardu vykdydama auditą ir patikrinimus, turėtų stebėti nacionalinių sertifikavimo priežiūros institucijų veiklos rezultatus ir sprendimų priėmimą.

4.5.12. Pramonės ir vartotojų organizacijoms turėtų būti sudaryta galimybė stebėtojų teisėmis dalyvauti ENISA valdančiosios tarybos veikloje.

4.6. ***Pramonė, MVĮ, finansavimas ir (arba) investicijos ir novatoriški verslo modeliai***

4.6.1. *Pramonė ir investicijos*

Siekiant didinti IRT srityje veikiančių ES bendrovių pasaulinį konkurencingumą, veiksmai šiuo tikslu turi būti orientuoti į geresnį IRT pramonės įmonių, įskaitant MVĮ, augimo ir konkurencingumo rėmimą.

Europa, sutelkdama įvairius ES fondus, nacionalines lėšas ir privačiojo sektoriaus investicijas, turėtų didinti investicijas į strateginius tikslus, kurių turėtų būti siekiama vykdant glaudų viešojo ir privačiojo sektorių bendradarbiavimą. Investicijos į svarbiausias sritis turėtų būti didinamos ir remiamos dabartinėje ir būsimoje mokslinių tyrimų bendrojoje programoje sukuriant ES kibernetinio saugumo fondą inovacijoms, moksliniams tyrimams ir technologinei plėtrai. Be to, Europa turėtų sukurti kibernetinio saugumo priemonių įgyvendinimo fondą atverdama naują galimybę dabartinėje ir būsimoje Europos infrastruktūros tinklų priemonėje ir būsimoje ESIF 3.0.

Reikėtų numatyti paskatas ES valstybėms narėms, jei įmanoma, pirkti Europos sprendimus ir pasirinkti Europos tiekėjus, jei tokių yra, ypač dėl neskelbtino pobūdžio prietaikų. Europa turėtų remti pirmaujančių Europos kibernetinių įmonių, galinčių konkuruoti pasaulio rinkoje, augimą.

4.6.2. *MVĮ*

Dėl rinkos susiskaidymo reikia aiškiau nustatyti klientų poreikius siekiant geriau spręsti rinkos klausimus. Be struktūruotos paklausos MVĮ ir startuoliai negali sparčiai augti. Atsižvelgiant į tai, būtų naudinga įsteigti Europos kibernetinio saugumo srityje veikiančių MVĮ centrą.

Kibernetinio saugumo technologijos sparčiai kinta ir MVĮ dėl savo gyvybingumo gali pasiūlyti pažangių sprendimų, kurių reikia, kad jos išliktų konkurencingos. Palyginti su trečiosiomis šalimis, ES vis dar ieško tinkamo MVĮ verslo modelio.

Galėtų būti parengtos specialios pradedančiosioms ir MVĮ skirtos schemos siekiant padėti joms padengti sertifikavimo išlaidas ir taip padėti sumažinti labai didelius sunkumus, kuriuos jos patiria norėdamos sukaupti savo technologinei ir komercinei plėtrai būtinas lėšas.

4.7. ***Žmogiškasis veiksnys. Švietimas ir apsauga***

4.7.1. EESRK atkreipia dėmesį į tai, kad Komisijos pasiūlyme nepakankamai atsižvelgiama į žmones, kaip svarbią skaitmeninių procesų varomąją jėgą, kuri naudojasi šiais procesais arba sukelia didelius kibernetinius incidentus.

4.7.2. Reikia sukurti tvirtą kibernetinių įgūdžių bazę, gerinti kibernetinę higieną ir didinti asmenų ir įmonių informuotumą. Kad būtų pasiektas šis rezultatas, reikėtų numatyti tam skirtas investicijas, laiką aukšto lygio instruktorių parengimui ir veiksmingas informuotumo didinimo kampanijas. Įgyvendinant šias tris veiksmų kryptis reikalingi bendri nacionalinių ir regionų valdžios institucijų (atsakingų už veiksmingų švietimo programų parengimą ir investavimą į jas) ir įmonių bei MVĮ veiksmai.

4.7.3. Reikėtų numatyti galimybę sukurti ES sertifikuotą aukštųjų mokyklų ir specialistų mokymo programą, į kurios kūrimą aktyviai įsitrauktų ENISA ir analogiškos nacionalinės institucijos. Be to, rengiant švietimo programas turi būti atsižvelgiama į lyčių lygybę, kad būtų pakeltas užimtumo lygis kibernetinio saugumo srityje.

4.7.4. EESRK mano, kad sertifikavimo procesas turi apimti tinkamą techninės ir programinės įrangos ženklinimo sistemą, kuri jau taikoma daugeliui kitų produktų (pavyzdžiui, energijos sektoriuje naudojamiems produktams). Ši priemonė duos trejopos naudos – sumažins įmonių sąnaudas, pašalins esamą rinkos susiskaidymą, sukeltą nacionaliniu lygmeniu jau priimtų skirtingų sertifikavimo sistemų, ir padės vartotojams suprasti įsigyto daikto kokybę ir savybes. Todėl svarbu, kad ir iš trečiųjų šalių importuojamiems produktams būtų taikomi minėti sertifikavimo ir ženklinimo mechanizmai. Galiausiai EESRK mano, kad sukūrus *ad hoc* ženklą būtų galima nedelsiant informuoti vartotojus ir naudotojus apie įsigytų prekių arba svetainių, kuriose jie vykdo pirkimus arba kurios gali perduoti neskelbtinus duomenis, patikimumą.

4.7.5. ENISA turėtų imtis labai svarbios daugiapakopio informavimo ir informuotumo didinimo veiklos, kad padidintų visuomenės sąmoningumą apie „saugų“ kibernetinį elgesį ir naudotojų pasitikėjimą internetu. Šiuo tikslu reikia įtraukti verslo asociacijas, vartotojų asociacijas ir kitas skaitmeninių paslaugų sektoriuje veikiančias organizacijas.

4.7.6. Kaip jau nurodyta nuomonėje INT/828, EESRK mano, kad siekiant papildyti Kibernetinio saugumo aktą labai svarbu kuo greičiau pradėti įgyvendinti plataus masto skaitmeniniam švietimui ir mokymui skirtą Europos programą ir taip užtikrinti visiems piliečiams priemones siekiant sklandesnio perėjimo. EESRK žino, kad ši sritis konkrečiai priklauso nacionalinei kompetencijai, tačiau tikisi, kad tokia programa bus skirta mokykloms, kad bus stiprinamos mokytojų žinios, prie skaitmeninių technologijų (įskaitant e. mokymąsi) pritaikomos mokymo programos ir metodika ir visiems besimokantiesiems suteikiamas aukštos kokybės mokslas. Šioje programoje natūraliai bus numatytas mokymasis visą gyvenimą siekiant keisti visų darbuotojų įgūdžius arba juos atnaujinti ([12]).

5. **Konkrečios pastabos**

5.1. ***Naujos technologijos ir sprendimai. Daiktų internetas***

Dėl komponentų, sistemų ir sprendimų skaitmeninimo ir geresnio ryšio susietųjų įrenginių skaičius vis didėja ir manoma, kad šių prietaisų netrukus bus keliskart daugiau nei Žemės gyventojų. Ši tendencija suteikia naujų galimybių kibernetiniams nusikaltėliams, visų pirma todėl, kad naudojami daiktų interneto prietaisai dažnai ne taip gerai apsaugoti kaip tradiciniai įrenginiai.

Europos saugumo standartai įvairiuose daiktų interneto įrenginius naudojančiose vertikaliosiose pramonės šakose gali sumažinti visų susietųjų produktų vertės grandinėje veikiančių pramonės dalyvių kūrimui skiriamas pastangas, laiką ir biudžetą.

Panašu, kad „įprastiems“ „žmonių interneto“ prietaisams bus reikalingas tam tikras minimalus saugumo lygis, užtikrinamas valdant tapatybę ir prieigą (angl. *Identity & Access Management*), atliekant pataisas (angl. *patching*) ir valdant prietaisus. Sertifikavimas yra vienas iš svarbiausių būdų užtikrinti aukštesnį saugumo lygį, todėl pagal naująją ES sertifikavimo strategiją daugiau dėmesio turėtų būti skiriama daiktų interneto saugumui.

Briuselis, 2018 m. vasario 14 d.

Europos ekonomikos ir socialinių reikalų komiteto pirmininkas
Georges DASSIS

([12]) Bendroji skaitmeninė rinka. Laikotarpio vidurio peržiūra.