Europos ekonomikos ir socialinių reikalų komiteto nuomonė „Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Europos kibernetinio atsparumo sistemos stiprinimo ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimas“

(COM(2016) 410 final)

(2017/C 075/21)

Pranešėjas **Thomas McDONOGH**

Konsultavimasis	Europos Komisija, 2016 8 18
Teisinis pagrindas	Sutarties dėl Europos Sąjungos veikimo 304 straipsnis
Atsakingas skyrius	Transporto, energetikos, infrastruktūros ir informacinės visuomenės skyrius
Priimta skyriuje	2016 11 15
Priimta plenarinėje sesijoje	2016 12 14
Plenarinė sesija Nr.	521
Balsavimo rezultatai (už/prieš/susilaikė)	148/0/1

1. **Išvados ir pasiūlymai**

1.1. Komitetas palankiai vertina Komisijos komunikatą dėl Europos kibernetinio atsparumo sistemos stiprinimo ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimo. Komitetas, kaip ir Komisija, yra susirūpinęs, kad Europa ir toliau išlieka neatspari kibernetiniams išpuoliams, ir pažymi, kad per pastaruosius metus ne mažiau kaip 80 % Europos įmonių yra patyrusios bent vieną kibernetinį išpuolį, o kibernetinių incidentų skaičius visose pramonės šakose visame pasaulyje 2015 m. padidėjo 38 % (The Global State of Information Security Survey (Pasaulinės informacijos saugumo padėties tyrimas) 2016 m., PWC). Pritariame Komisijai, kad reikia imtis priemonių, siekiant sustiprinti Europos kibernetinio atsparumo sistemą ir skatinti Europos kibernetinio saugumo pramonės konkurencingumą ir novatoriškumą.

1.2. Komitetas ypač pritaria šiam pasiūlymui, atsižvelgdamas į neseniai priimtą Tinklų ir informacijos saugumo direktyvą (TIS direktyva) ([1]), kuria reikalaujama labiau suderinto požiūrio į kibernetinį saugumą Europos Sąjungoje ir platesnės ES kibernetinio saugumo strategijos ([2]), kurioje išdėstyta dabartinė vizija, kaip geriausiai užkirsti kelią kibernetiniams trikdžiams ir išpuoliams bei į juos reaguoti, kaip remti Europos laisvės ir demokratijos vertybes ir kaip užtikrinti saugų skaitmeninės ekonomikos augimą.

1.3. EESRK sutinka, kad reikia imtis visuotinių priemonių, siekiant labiau apsaugoti Europai gyvybiškai svarbią skaitmeninę infrastruktūrą ir paslaugas nuo grėsmių jų saugumui, ir džiaugiasi matydamas, kad dabartinės pasiūlytos priemonės turės didelę reikšmę įgyvendinant daugelį Komiteto rekomendacijų, išdėstytų ankstesnėse nuomonėse ([3]) dėl kibernetinio saugumo didinimo visoje Europos Sąjungoje.

([1]) OL L 194, 2016 7 19, p. 1.
([2]) JOIN(2013) 1.
([3]) OL C 97, 2007 4 28, p. 21.
OL C 175, 2009 7 28, p. 92;
OL C 255, 2010 9 22, p. 98;
OL C 54, 2011 2 19, p. 58;
OL C 107, 2011 4 6, p. 58;
OL C 229, 2012 7 31, p. 90;
OL C 218, 2011 7 23, p. 130;
OL C 24, 2012 1 28, p. 40;
OL C 229, 2012 7 31, p. 1;
OL C 351, 2012 11 15, p. 73;
OL C 76, 2013 3 14, p. 59;
OL C 271, 2013 9 19, p. 127;
OL C 271, 2013 9 19, p. 133;
OL C 451, 2014 12 16, p. 31.

1.4. EESRK palankiai vertina Komisijos pasirašytą kibernetinio saugumo sutartinę viešojo ir privataus sektorių partnerystę (VPSP), kuria, tikimasi, į ES kibernetinio saugumo pramonę bus pritraukta 1,8 mlrd. EUR investicijų, skirtų bendradarbiavimui ankstyvuoju mokslinių tyrimų ir inovacijų proceso etapu skatinti ir įvairiems, pavyzdžiui, energetikos, sveikatos priežiūros, transporto ir finansų sektoriams skirtiems kibernetinio saugumo sprendimams kurti. Ypač tikimės, kad šia sutartine VPSP bus remiamas ankstyvame veiklos etape esančių kibernetinio saugumo įmonių plėtojimas.

1.5. Komitetas pritaria Komisijos ketinimui iki 2017 m. pabaigos įvertinti poreikį pakeisti arba atnaujinti Europos tinklų ir informacijos apsaugos agentūros (ENISA) įgaliojimus ir tikisi, kad Komisija konsultuosis su Komitetu šiuo klausimu. EESRK įsitikinęs, kad bet koks ENISA įgaliojimų atnaujinimas turėtų apimti didesnį agentūros operatyvinį vaidmenį, siekiant, kad visoje Sąjungoje būtų geriau žinoma apie kibernetinių išpuolių pavojų ir geriau į šiuos išpuolius reaguojama, taip pat ji turėtų prisiimti daugiau tiesioginės atsakomybės už su kibernetiniu saugumu susijusio švietimo ir informavimo programas, pirmiausia skirtas piliečiams ir mažosioms bei vidutinėms įmonėms (MVĮ).

1.6. Siekiant užtikrinti ryžtingą vadovavimą ir integraciją, kurių reikia ES lygmeniu norint atremti efektyvios Europos kibernetinio saugumo politikos įgyvendinimo iššūkius, Komitetas ragina Komisiją įvertinti galimybę pakeisti ENISA statusą ir įsteigti ES lygmens už kibernetinį saugumą atsakingą įstaigą, panašią į centrinę aviacijos pramonės agentūrą – Europos aviacijos saugos agentūrą (EASA). Jei šis ENISA įgaliojimų pakeitimas nėra įmanomas, EESRK siūlo įsteigti naują tokio pobūdžio instituciją.

1.7. EESRK ragina Komisiją pagalvoti apie nacionalinio kibernetinio saugumo modelio ir reitingų sistemos sukūrimą, analogišką brandžiajam programavimui IT sistemoje, kad būtų galima objektyviai įvertinti kiekvienos valstybės narės kibernetinio saugumo atsparumą.

1.8. Komitetas pažymi, kad Komisija artimiausiu metu svarstys, ar reikia atnaujinti 2013 m. ES kibernetinio saugumo strategiją, ir mes tikimės, kad Komisija laiku pradės konsultuotis su mumis šiuo klausimu.

1.9. Atsižvelgdamas į kibernetinio saugumo svarbą ir vis didėjančią kibernetinių nusikaltimų grėsmę, EESRK ragina skirti pakankamą finansavimą ir išteklius Europole įsteigtam Europos kovos su elektroniniu nusikalstamumu centrui ir Europos gynybos agentūrai.

1.10. Atsižvelgiant į tai, kad labai svarbu apsaugoti piliečių asmeninę informaciją, kurią saugo viešojo administravimo institucijos ir įstaigos, Komitetas ragina organizuoti viešojo administravimo įstaigų darbuotojams specialius mokymus informacijos valdymo, duomenų apsaugos ir kibernetinio saugumo srityse.

1.11. Siekiant visapusiškai apsaugoti ES nuo kibernetinių nusikaltimų ir išpuolių bei sukurti stiprią ES kibernetinio saugumo pramonę, EESRK manymu, ES kibernetinio saugumo strategija ir politika turi būti orientuojamos šiomis kryptimis: ES turi ryžtingai imtis lyderės vaidmens; reikia kibernetinio saugumo politikos priemonių, kurios didintų saugumą kartu išsaugodamos privatumą ir kitas pagrindines teises; reikia didinti piliečių informuotumą ir skatinti imtis iniciatyvos įgyvendinant apsaugos priemones; valstybėse narėse reikia visapusiškų valdymo priemonių; įmonės turi imtis informacija ir atsakomybe paremtų veiksmų; šalių Vyriausybės, privatus sektorius ir piliečiai turi tapti tikrais partneriais; reikia pakankamai investicijų; turi būti taikomi aukšti techniniai standartai ir pakankamai investuojama į mokslinius tyrimus ir technologijų plėtrą; būtini tarptautiniai veiksmai.

2. **Svarbiausios Komisijos komunikato nuostatos**

2.1. Šiame komunikate pristatomos priemonės, kuriomis siekiama sustiprinti Europos kibernetinio atsparumo sistemą ir skatinti Europos kibernetinio saugumo pramonės konkurencingumą ir novatoriškumą, kaip paskelbta ES kibernetinio saugumo strategijoje ir Bendrosios skaitmeninės rinkos strategijoje.

2.2. Kad būtų pasiekti šie tikslai, Komisijos pasiūlytomis priemonėmis subalansuojamos TIS direktyvos nuostatos, siekiant stiprinti bendradarbiavimą kibernetinio saugumo srityje, keitimąsi informacija, mokymus ir saugumo užtikrinimo organizavimą visoje Sąjungoje. Be to, Komisija iki 2017 m. pabaigos baigs vertinti ENISA veiklą ir apsvarstys, ar reikia pakeisti arba atnaujinti ENISA įgaliojimus.

2.2.1. Komisija, glaudžiai bendradarbiaudama su valstybėmis narėmis, ENISA, EIVS ir kitomis susijusiomis ES įstaigomis, sieks sukurti kibernetinio saugumo mokymo platformą.

2.2.2. Siūloma nemažai priemonių, kuriomis siekiama spręsti problemas, susijusias su sektorių tarpusavio priklausomybe, bei didinti pagrindinės viešųjų tinklų infrastruktūros atsparumą, tarp šių priemonių – Europos sektorinių keitimosi informacija ir jos analizės centrų plėtra ir jų bendradarbiavimas su Reagavimo į kompiuterinius saugumo incidentus tarnybomis (CSIRT). Komisija taip pat siūlo, kad nacionalinės valdžios institucijos galėtų prašyti CSIRT atlikti reguliarias pagrindinės tinklų infrastruktūros patikras.

2.3. Komisijos siūlomomis priemonėmis siekiama atkreipti dėmesį į būtinybę didinti paramą stiprios Europos kibernetinio saugumo pramonės augimui ir plėtrai, pasitelkiant mokymus, investicijas, bendrosios rinkos reikalavimus bei sukuriant naują kibernetinio saugumo viešojo ir privataus sektorių partnerystę, kuria iki 2020 m. tikimasi pritraukti 1,8 mlrd. EUR investicijų.

2.3.1. Taip pat siūloma parengti ir iki 2017 m. pabaigos pateikti pasiūlymą dėl europinės IRT saugumo sertifikavimo sistemos ir įvertinti paprastos europinės kibernetinio saugumo ženklinimo sistemos įgyvendinamumą ir poveikį.

2.3.2. Siekdama padidinti investicijas į kibernetinį saugumą Europoje ir paramą MVĮ, Komisija didins kibernetinės bendruomenės informuotumą apie esamus finansavimo mechanizmus; skatins daugiau naudotis ES priemonėmis ir mechanizmais, kad būtų remiamos novatoriškų MVĮ pastangos išnagrinėti civilinio ir gynybos sektorių kibernetinio saugumo rinkų sinergijos galimybes (pavyzdžiui, Europos įmonių tinklas ir Europos su gynyba susijusių regionų tinklas suteiks naujų galimybių regionams išnagrinėti tarpvalstybinio bendradarbiavimo dvejopo naudojimo produktų, įskaitant kibernetinio saugumo produktus, srityje galimybes ir naujų galimybių MVĮ megzti ryšius); išnagrinės galimybes lengviau gauti lėšų investicijoms, pavyzdžiui, naudojantis specialios paskirties Investavimo į kibernetinį saugumą platforma arba kitomis priemonėmis); sukurs Kibernetinio saugumo pažangiosios specializacijos platformą (RIS3), kad padėtų valstybėms narėms ir regionams, suinteresuotiems investuoti į kibernetinio saugumo sektorių.

2.3.3. Be to, siekdama skatinti ir puoselėti Europos kibernetinio saugumo pramonę diegiant inovacijas, Komisija sudarys kibernetinio saugumo sutartinę viešojo ir privataus sektorių partnerystę (VPSP); paskelbs su kibernetinio saugumo sutartine VPSP susijusius kvietimus teikti pasiūlymus pagal programą „Horizontas 2020“; užtikrins, kad kibernetinio saugumo sutartinės VPSP veikla būtų derinama su susijusiomis sektorinėms strategijomis, programos „Horizontas 2020“ priemonėmis ir sektorių sutartinių VPSP veikla.

3. **Bendrosios pastabos**

3.1. Skaitmeninei ekonomikai tenka penktadalis ES BVP augimo, kasmet internetu perka daugelis europiečių. Internetas ir sujungtos skaitmeninės technologijos būtinos mūsų gyvybiškai svarbioms energetikos, sveikatos priežiūros, valdžios ir finansinėms paslaugoms. Tačiau ypatingos svarbos skaitmeninė infrastruktūra ir paslaugos, kurios atlieka tokį svarbų vaidmenį ekonominiame ir socialiniame gyvenime, yra pažeidžiamos – kibernetinių nusikaltimų ir išpuolių pavojus stiprėja ir kelia grėsmę mūsų klestėjimui ir gyvenimo kokybei.

3.2. Dabartiniu metu valdžios ir viešojo administravimo institucijos bei įstaigos saugo daug asmeninės informacijos apie visus piliečius elektronine forma. Todėl geras informacijos valdymas, kibernetinis saugumas ir duomenų apsauga yra labai svarbu piliečiams visoje Sąjungoje, ir jie turi būti užtikrinti, kad jų asmeninė informacija ir privatumas yra saugomi pagal ES direktyvas ir reglamentus. Tai pirmiausia pasakytina apie duomenis, susijusius su sveikata, finansais, teisiniais ir kitais dalykais, kuriais galėtų būti pasinaudota norint pavogti tapatybės duomenis arba juos netinkamai atskleisti trečiosioms šalims. Gyvybiškai svarbu, kad visi viešojo sektoriaus darbuotojai būtų gerai apmokyti informacijos valdymo, kibernetinio saugumo ir duomenų apsaugos srityse.

3.3. Piliečių švietimas asmeninio kibernetinio saugumo, taip pat duomenų apsaugos klausimais turėtų būti esminė visų skaitmeninio raštingumo programų dalis. ES remiama švietimo programa galėtų būti paremtos mažiau aktyvių valstybių narių pastangos ir kartu būti užtikrinta, kad strategija yra tinkamai suprantama, taip sumažinant baiminimąsi dėl privatumo ir didinant pasitikėjimą skaitmenine ekonomika. Ši programa galėtų būti įgyvendinama kartu su vartotojų asociacijomis ir pilietinės visuomenės organizacijomis visoje Sąjungoje, įskaitant švietimo įstaigas, teikiančias paslaugas vyresnio amžiaus žmonėms.

3.4. Kiekviena valstybė narė turėtų įgalinti savo dabartines pramonės vystymo organizacijas, kurios informuotų MVĮ sektorių, jį šviestų ir jam padėtų spręsti su kibernetiniu saugumu susijusias problemas. Stambios įmonės gali lengvai gauti joms reikiamų žinių, tačiau MVĮ reikia paramos.

3.5. Būtų labai naudinga turėti objektyvų kiekvienos valstybės narės kibernetinio saugumo atsparumo lygio įvertį, kad būtų galima daryti palyginimus, kuriais remiantis būtų galima šalinti trūkumus ar tobulinti priemones. Būtų galima sukurti nacionalinį kibernetinio saugumo ir reitingų sistemos modelį, analogišką brandžiajam programavimui IT sistemoje, nacionalinio kibernetinio saugumo apsaugai ir atsparumui įvertinti.

3.6. Visapusiška kibernetinio saugumo strategija turėtų apimti šiuos veiksmus:

— ES turi tapti lydere, įgyvendinančia tokią politiką, teisės aktus ir kuriančia tokias institucijas, kurios užtikrintų aukštą kibernetinio saugumo lygį visoje Sąjungoje,

— reikia vykdyti kibernetinio saugumo politiką, kuria būtų padidintas individualus ir kolektyvinis saugumas ir išsaugomos piliečių teisės į privatumą ir kitos pagrindinės vertybės ir laisvės,

— visi piliečiai turi būti gerai informuoti apie naudojimosi internetu riziką ir skatinami patys imtis iniciatyvos apsaugoti savo skaitmeninius prietaisus, asmens duomenis, privatumą ir internetu vykdomus sandorius,

— visos valstybės narės turi imtis visapusiškų valdymo priemonių, kad užtikrintų ypatingos svarbos informacinės infrastruktūros saugumą ir atsparumą,

— visos verslo įmonės turi imtis informacija ir atsakomybe paremtų veiksmų, kad užtikrintų savo IRT sistemų saugumą ir atsparumą, apsaugotų savo veiklą ir savo klientų interesus,

— interneto paslaugų teikėjai turi imtis iniciatyvos, kad apsaugotų savo klientus nuo kibernetinių išpuolių,

— visoje ES Vyriausybės, privatus sektorius ir piliečiai strateginiu ir praktiniu lygmenimis turi įgyvendinti gilia partneryste pagrįstą kibernetinio saugumo strategiją,

— reikia laikytis požiūrio, pagrįsto koncepcija, kad kibernetinis saugumas būtų integruotas į interneto technologijas ir paslaugas jų kūrimo metu,

— reikia pakankamai investuoti į informaciją apie kibernetinį saugumą ir įgūdžių ugdymą šioje srityje, siekiant išugdyti gerai kibernetinio saugumo klausimus išmanančius darbuotojus,

— reikia taikyti aukštus techninius kibernetinio saugumo standartus ir pakankamai investuoti į mokslinius tyrimus, technologinę plėtrą ir inovacijas, prisidedant prie stiprios kibernetinio saugumo pramonės ir pasaulinio lygio sprendimų kūrimo,

— reikia aktyviai įsitraukti į veiklą tarptautiniu lygmeniu, kartu su ES nepriklausančiomis valstybėmis kuriant suderintą pasaulinę politiką ir reagavimo į grėsmes kibernetiniam saugumui priemones.

4. **Konkrečios pastabos**

4.1. Remdamasi TIS direktyvoje išdėstyta kibernetinio saugumo valdymo sistema ir tolesnėmis šiame komunikate pateiktomis priemonėmis, ES turėtų apsvarstyti galimybę sukurti stiprią centralizuotą kibernetinio saugumo instituciją, panašią į Europos aviacijos saugos agentūrą (EASA) arba neseniai JAV įsteigtą vyriausiojo federalinio informacijos saugumo pareigūno pareigybę (Kibernetinio saugumo nacionalinis veiksmų planas, Baltieji Rūmai, 2016 m. vasario 9 d.), kuri būtų atsakinga už kibernetinio saugumo politikos įgyvendinimo ES lygmeniu priežiūrą ir sujungtų į visumą įvairių šioje srityje dirbančių agentūrų pastangas.

4.2. Komitetui didelį įspūdį padarė per daugelį metų įgyta ENISA kompetencija, todėl, Komiteto manymu, ji galėtų dar labiau prisidėti prie Europos kibernetinio atsparumo ir saugumo užtikrinimo. Reikėtų sustiprinti ENISA veiklos įgaliojimus, siekiant, kad visoje Sąjungoje būtų geriau žinoma apie kibernetinių išpuolių pavojų ir geriau į šiuos išpuolius reaguojama. Įgaliojimų peržiūra yra savalaikė, atsižvelgiant į tai, kaip nuo ENISA įkūrimo pasikeitė kibernetinio saugumo aplinka. Remiantis TIS direktyva, galbūt būtų galima išplėsti operatyvinį ENISA vaidmenį, kad ji, derindama turimą kompetenciją bei sinergiją su kitų ES ir valstybių narių institucijų, agentūrų bei įstaigų, tokių kaip Kompiuterinių incidentų tyrimo tarnyba (CERT), Europos kovos su elektroniniu nusikalstamumu centras ir Europos gynybos agentūra, veikla, galėtų teikti didesnę naudą ES, valstybėms narėms, piliečiams ir įmonėms. ENISA turėtų būti suteikta daugiau tiesioginės atsakomybės už kibernetinio saugumo švietimo ir informavimo programas, pirmiausia skirtas piliečiams ir MVĮ.

4.3. Kai 2013 m. buvo įkurtas Europos kovos su kibernetiniu nusikalstamumu centras (EC3), jo veiklos biudžetą tesudarė 7 mln. EUR, t. y. mažiau nei 10 % viso Europolo biudžeto (2012 m. sausio 9 d. Europos Komisijos informacinis pranešimas/13/6). 2014 m. EC3 vadovas teigė, kad išlaidų mažinimas labai apribojo jo įstaigos išteklius ir kad jiems yra labai sunku spėti reaguoti į sparčiai kintančias kibernetinių nusikaltimų grėsmes (Security Magazine, 2014 11 1). EESRK įsitikinęs, kad siekiant reaguoti į kintančias grėsmes, Europolui skirti ištekliai kovai su kibernetiniais nusikaltimais turi būti gerokai padidinti. 2016 m. Europolo biudžetas vis dar yra tik 100 mln. EUR ([4]).

4.4. Komitetas palankiai vertina TIS direktyvos nuostatas ir komunikate pasiūlytus veiksmus, kuriais siekiama pagerinti valstybių narių bendradarbiavimą kibernetinio saugumo srityje. Siekiant užtikrinti visų piliečių saugumą ir sustiprinti kibernetinį atsparumą Europos Sąjungoje, kur ypatingos svarbos informacinės infrastruktūros sistemos dažnai yra tarpusavyje sujungtos, labai svarbu numatyti bendradarbiavimo priemones, skirtas mažinti didėjantį atotrūkį tarp labiausiai kibernetinio saugumo srityje pažengusių šalių ir tų valstybių narių, kurių kompetencija šioje srityje yra žemesnio lygio.

2016 m. gruodžio 14 d., Briuselis

Europos ekonomikos ir socialinių reikalų komiteto pirmininkas
Georges DASSIS

([4]) OL C 113, 2016 3 30, p. 144.