EUROPOS KOMISIJA

EUROPOS SĄJUNGOS VYRIAUSIASIS ĮGALIOTINIS UŽSIENIO REIKALAMS IR SAUGUMO POLITIKAI

Briuselis, 2013 02 07
JOIN(2013) 1 final

BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

Europos Sąjungos kibernetinio saugumo strategija.

Atvira, saugi ir patikima kibernetinė erdvė

BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

Europos Sąjungos kibernetinio saugumo strategija.

Atvira, saugi ir patikima kibernetinė erdvė

1. ĮŽANGA

1.1. Kontekstas

Per pastaruosius du dešimtmečius internetas ir apskritai kibernetinė erdvė padarė didžiulį poveikį visoms visuomenės gyvenimo sritims. Mūsų kasdienis gyvenimas, pagrindinės teisės, socialinė sąveika ir ekonomika priklauso nuo sklandaus informacinės ir ryšių technologijos veikimo. Atvira ir laisva kibernetinė erdvė tapo politinės ir socialinės įtraukties paskata visame pasaulyje; ji sugriovė valstybes, bendrijas ir piliečius skyrusias sienas sudarydama sąlygas bendrauti ir dalytis informacija bei idėjomis nepaisant atstumo; ji tapo žodžio laisvės ir pagrindinių teisių įgyvendinimo erdve, sudarė sąlygas žmonėms siekti visuomenės demokratėjimo ir netgi daugiau, kaip ryškiausiai parodė Arabų pavasaris.

Kad kibernetinė erdvė liktų atvira ir laisva, jai turėtų galioti tie patys principai, normos ir vertybės, kuriuos ES taiko tradicinei aplinkai. Kibernetinėje erdvėje pagrindinės teisės, demokratija, teisinės valstybės principai turi būti saugomi. Mūsų laisvė ir gerovė vis labiau priklauso nuo patikimo ir novatoriško interneto, kuris klestės toliau, jeigu jo augimą skatins privačiojo sektoriaus inovacijos ir pilietinė visuomenė. Tačiau laisvei internete reikia saugos ir saugumo. Kibernetinė erdvė turi būti saugoma nuo incidentų, piktavališkos veiklos ir piktnaudžiavimo; vyriausybėms tenka reikšmingas vaidmuo – užtikrinti laisvę ir saugą kibernetinėje erdvėje. Vyriausybėms tenka kelios užduotys: išsaugoti prieigą ir atvirumą, gerbti ir saugoti pagrindines teises internete, užtikrinti interneto patikimumą ir sąveikumą. Tačiau didelę kibernetinės erdvės dalį valdo ir eksploatuoja privatusis sektorius, todėl norint, kad bet kuri šios srities iniciatyva susilauktų sėkmės, reikia pripažinti jo vadovaujamąjį vaidmenį.

Informacijos ir ryšių technologija tapo mūsų ekonomikos augimo pamatu ir yra ypač svarbus išteklius, nuo kurio priklauso visi ūkio sektoriai. Dabar ji palaiko sudėtingas sistemas, kurios užtikrina mūsų ūkių funkcionavimą pagrindiniuose sektoriuose, kaip antai finansų, sveikatos, energetikos ir transporto; nuolatinė prieiga prie interneto ir sklandus informacinių sistemų veikimas yra daugelio verslo modelių pagrindas.

Įgyvendinusi bendrąją skaitmeninę rinką Europa galėtų padidinti BVP beveik 500 mlrd. EUR per metus[1]; arba vidutiniškai 1 000 EUR vienam gyventojui. Kad rinkoje išpopuliarėtų naujos sujungtosios technologijos, įskaitant e. mokėjimus, nuotolinę kompiuteriją arba tiesioginius ryšius tarp įrenginių[2], piliečiams reikia užtikrintumo ir pasitikėjimo. Deja, 2012 m.

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] Pavyzdžiui, augalai su įdiegtais jutikliais, kurie perduoda laistymo sistemai informaciją, kada laikas laistyti.

„Eurobarometro“ apklausos duomenimis[3], beveik trečdalis europiečių nepasitiki savo gebėjimu naudotis internetu elektroninės bankininkystės ar apsipirkimo tikslais. Absoliuti dauguma taip pat teigė, kad saugumo sumetimais jie vengia atskleisti asmeninę informaciją internete. Visoje ES daugiau nei vienas iš dešimties interneto naudotojų jau yra tapęs internetinio sukčiavimo auka.

Pastaraisiais metais paaiškėjo, kad skaitmeninis pasaulis ne tik nepaprastai naudingas, bet ir pažeidžiamas. Tyčiniai ar atsitiktiniai kibernetinio saugumo[4] incidentai dažnėja nerimą keliančiu greičiu; jie gali sutrikdyti pagrindinių savaime suprantamomis laikomų paslaugų teikimą (vandens, elektros energijos tiekimą, sveikatos priežiūros ar judriojo ryšio paslaugų teikimą). Grėsmės kyla dėl įvairių priežasčių, įskaitant kriminalines, politinę motyvaciją, terorizmą ar valstybės remiamus išpuolius, taip pat dėl gaivalinių nelaimių ar atsitiktinių klaidų.

ES ekonomika jau kenčia nuo elektroninių nusikaltimų[5] prieš privatųjį sektorių ir individualius asmenis. Kibernetiniai nusikaltėliai vis išmoningiau braunasi į informacines sistemas, vagia labai svarbius duomenis ir reikalauja iš bendrovių išpirkos. Augantys ekonominio šnipinėjimo ir valstybės remiamos veiklos mastai kibernetinėje erdvėje kelia naujos rūšies grėsmes ES vyriausybėms ir bendrovėms.

Valstybėse, kurios nėra ES narės, vyriausybės taip pat gali piktnaudžiauti kibernetine erdve, kad stebėtų ir kontroliuotų savo piliečius. ES gali tam duoti atkirtį remdama laisvę internete ir internete užtikrindama pagarbą pagrindinėms teisėms.

Visi šie veiksniai paaiškina, kodėl vyriausybės visame pasaulyje pradėjo rengti kibernetinio saugumo strategijas ir kibernetinę erdvę vertinti kaip vis aktualesnį tarptautinį klausimą. Imtis veiksmų šioje srityje atėjo laikas ir Europos Sąjungai. Šiame Komisijos ir Sąjungos Vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai pateiktame Europos Sąjungos kibernetinio saugumo strategijos pasiūlyme išdėstoma šios srities ES vizija, paaiškinamos užduotys ir kompetencija, nurodomi veiksmai, kurių reikia imtis norint tvirtai bei veiksmingai apsaugoti ir stiprinti piliečių teises, kad ES internetinė aplinka taptų saugiausia pasaulyje.

1.2. Kibernetinio saugumo principai

Sienų nepaisantis ir daugiasluoksnis internetas be vyriausybių priežiūros ar reguliavimo tapo viena galingiausių pasaulinės pažangos priemonių. Privačiajam sektoriui ir toliau turėtų tekti vadovaujamasis vaidmuo kuriant internetą ir vykdant kasdienį jo valdymą, tačiau vis ryškėja poreikis nustatyti skaidrumo, atskaitomybės ir saugumo reikalavimus. Šioje strategijoje

---

[3] 2012 m. speciali „Eurobarometro“ apklausa Nr. 390 dėl kibernetinio saugumo.

[4] Kibernetinis saugumas paprastai reiškia saugumo priemones ir veiksmus, kurie gali būti panaudoti kibernetinei erdvei saugoti (ir civilinėje, ir karinėje srityje) nuo grėsmių, kurios siejasi su žala vienas nuo kito priklausomiems kibernetinės erdvės tinklams ir informacinei infrastruktūrai arba gali jiems pakenkti. Kibernetinio saugumo tikslas – išsaugoti tinklų ir infrastruktūros prieinamumą bei vientisumą ir juose saugomos informacijos konfidencialumą.

[5] Elektroniniai nusikaltimai reiškia įvairaus pobūdžio nusikalstamą veiką, kuriai kaip pirminės priemonės ar pirminis tikslas naudojami kompiuteriai ir informacinės sistemos. Elektroniniai nusikaltimai paprastai apima įprastas nusikaltimų rūšis, pavyzdžiui, sukčiavimą, klastojimą ir tapatybės vagystę; su turiniu susijusius nusikaltimus, pavyzdžiui, vaikų pornografijos platinimą internete arba rasinės neapykantos kurstymą; ir specifinius kompiuterių bei informacinių sistemų nusikaltimus, pavyzdžiui, išpuolius prieš informacines sistemas, siekimą nutraukti sistemos veiklą ir kenkimo programinę įrangą.

paaiškinami principai, pagal kuriuos reikėtų orientuoti kibernetinio saugumo politiką Europos Sąjungoje ir pasaulyje.

ES pagrindinės vertybės galioja ir skaitmeniniame, ir fiziniame pasaulyje

Tie patys įstatymai ir normos, kurie taikomi kitose mūsų kasdienio gyvenimo srityse, galioja ir kibernetinėje erdvėje.

Pagrindinių teisių, žodžio laisvės, asmens duomenų ir privatumo apsauga

Kibernetinis saugumas gali būti patikimas ir veiksmingas tik tuo atveju, kai jo pagrindas – pagrindinės teisės ir laisvės, kaip įtvirtinta Europos Sąjungos pagrindinių teisių chartijoje, ir ES pagrindinės vertybės. Kita vertus, individų teisės negali būti užtikrintos be saugių tinklų ir sistemų. Bet koks su asmens duomenimis susijęs dalijimasis informacija kibernetinio saugumo tikslais turėtų atitikti ES duomenų apsaugos teisės nuostatas ir jį vykdant reikia paisyti individo teisių toje srityje.

Prieiga visiems

Žinant, kaip skaitmeninis pasaulis persmelkia gyvenimą visuomenėje, piliečiai, kurių prieiga prie interneto ribota arba kurie neturi jokios prieigos ir neturi skaitmeninių įgūdžių, atsiduria nepalankioje padėtyje. Kiekvienas turėtų turėti galimybę naudotis internetu ir netrukdomai gauti informaciją. Norint užtikrinti visų žmonių saugią prieigą prie interneto, turi būti užtikrintas interneto vientisumas ir saugumas.

Demokratiškas ir veiksmingas daugelio suinteresuotųjų šalių dalyvavimu grindžiamas valdymas

Skaitmeninio pasaulio nekontroliuoja kuris nors vienas subjektas. Šiuo metu interneto išteklius, protokolus ir standartus visą laiką valdo ir jo ateities plėtrą vykdo daug suinteresuotųjų šalių, tarp kurių nemažai komercinių ir nevyriausybinių subjektų. ES nuolat tvirtina, kad dabartiniam interneto valdymo modeliui svarbus visų suinteresuotųjų šalių dalyvavimas, ir remia plataus suinteresuotųjų šalių rato dalyvavimu grindžiamo valdymo modelį[6].

Bendra atsakomybė siekiant užtikrinti saugumą

Augant priklausomybei nuo informacinių ir ryšių technologijų visose žmogaus gyvenimo srityse, atsirado pažeidžiamumas, kurį reikia tinkamai apibrėžti, nuodugniai išnagrinėti, pašalinti arba sumažinti. Norint didinti kibernetinį saugumą, visi subjektai, kuriems tai aktualu – valdžios institucijos, privatusis sektorius ar pavieniai piliečiai – turi pripažinti, kad atsakomybė yra bendra, imtis savisaugos veiksmų ir prireikus užtikrinti koordinuotai sureaguoti.

[6] Žr. taip pat COM(2009) 277, Komisijos komunikatą Europos Parlamentui ir Tarybai „Tolesni interneto valdymo etapai“.

2. STRATEGINIAI PRIORITETAI IR VEIKSMAI

ES turėtų visiems užtikrinti saugią internetinę aplinką suteikdama didžiausią įmanomą laisvę ir saugumą. Pripažįstant, kad spręsti saugumo užduotis kibernetinėje erdvėje didžia dalimi yra valstybių narių užduotis, šioje strategijoje siūlomi konkretūs veiksmai, kuriais galima padidinti bendrus ES pasiektus rezultatus. Vieni veiksmai yra artimiausio laikotarpio, kiti – tolimos perspektyvos; numatyta įvairių politikos priemonių[7] ir jos siejamos su įvairiais subjektų tipais: ES institucijomis, valstybėmis narėmis ar pramone.

Šioje strategijoje pateikta ES vizija yra orientuota į penkis aptartiesiems uždaviniams spręsti skirtus strateginius prioritetus:

- pasiekti kibernetinį atsparumą
- radikaliai sumažinti elektroninių nusikaltimų skaičių
- sukurti kibernetinės gynybos politiką ir pajėgumus, susijusius su bendra saugumo ir gynybos politika
- plėtoti pramoninius ir technologinius išteklius kibernetiniam saugumui užtikrinti
- sukurti nuoseklią tarptautinę Europos Sąjungos kibernetinės erdvės politiką ir remti pagrindines ES vertybes.

2.1. Kibernetinio atsparumo pasiekimas

Remiant kibernetinį atsparumą Europos Sąjungoje, plėtoti pajėgumus ir veiksmingai bendradarbiauti turi ir valdžios įstaigos, ir privatusis sektorius. Naudojantis teigiamais iki šiol atliktų veiksmų rezultatais[8], tolesnė ES veikla gali ypač padėti pašalinti tarpvalstybinio pobūdžio kibernetinius pavojus bei grėsmes ir koordinuotai reaguoti ekstremaliose situacijose. Tai labai padėtų pagerinti vidaus rinkos veikimo sklandumą ir padidintų vidaus saugumą Europos Sąjungoje.

Nedėdama didelių pastangų gerinti viešojo ir privačiojo sektorių pajėgumų, išteklių ir procesų, kurie padėtų vykdyti kibernetinių incidentų prevenciją, juos aptikti ir įveikti, Europa liks pažeidžiama. Todėl Komisija suformavo tinklų ir informacijos saugumo politiką[9]. 2004 m. įsteigta **Europos tinklų ir informacijos apsaugos agentūra ENISA[10]** ir šiuo metu Taryba ir Parlamentas tariasi dėl naujo reglamento, kuriuo būtų sustiprinta ENISA ir modernizuotos jos kompetencijos[11]. Be to, Elektroninių ryšių pagrindų direktyvoje[12] elektroninių ryšių paslaugų teikėjai įpareigojami tinkamai valdyti jų tinklams kylančias

---

7 Veiksmai, siejami su keitimusi informacija, kurioje yra asmens duomenų, turėtų atitikti ES duomenų apsaugos teisės aktus.

8 Žr. nuorodas šiame komunikate ir su Komisijos pasiūlymu dėl direktyvos dėl tinklų ir informacijos saugumo pateikiamame Komisijos tarnybų darbiniame dokumente (poveikio vertinime), ypač 4.1.4 ir 5.2 skirsniuose, 2, 6 ir 8 prieduose.

9 2001 m. Komisija priėmė komunikatą „Tinklų ir informacijos apsauga: pasiūlymas dėl Europos politikos požiūrio“ (COM(2001) 298); 2006 m. – „Saugios informacinės visuomenės strategiją – „Dialogas, partnerystė ir teisių suteikimas“ (COM(2006) 251). Nuo 2009 m. Komisija taip pat priėmė veiksmų planą ir komunikatą dėl ypatingos svarbos informacinės infrastruktūros apsaugos: COM(2009) 149, kuriam pritarta Tarybos rezoliucija 2009/C 321/01; ir COM(2011)163, kuriam pritarta Tarybos išvadomis 10299/11).

10 Reglamentas (EB) Nr. 460/2004

11 COM(2010) 521. Šioje strategijoje siūlomi veiksmai nereiškia galiojančių ar būsimų ENISA kompetencijų pakeitimo.

12 Direktyvos 2002/21/EB 13a ir 13b straipsniai

grėsmes ir pranešti apie svarbius saugumo pažeidimus. Taip pat ES duomenų apsaugos teisės aktuose[13] reikalaujama, kad duomenų valdytojai užtikrintų duomenų apsaugos reikalavimus ir apsaugos priemones, įskaitant su saugumu susijusias priemones, o viešai prieinamų e. ryšių paslaugų srityje duomenų valdytojai privalo apie asmens duomenų saugumo pažeidimą pranešti kompetentingoms nacionalinėms institucijoms.

Nepaisant pažangos, kuriai akstiną davė savanoriški įsipareigojimai, visoje ES iki šiol likę spragų, kurios konkrečiai susijusios su nacionaliniais pajėgumais, koordinavimu kilus kelias valstybes apimantiems incidentams, privačiojo sektoriaus dalyvavimu ir parengtimi. Ši strategija pateikiama su **teisės akto** pasiūlymu, kuriuo siekiama:

- nustatyti mažiausius bendrus nacionalinio lygmens tinklų ir informacijos saugumo reikalavimus, kuriais valstybės narės būtų įpareigotos: paskirti tinklų ir informacijos saugumo (TIS) kompetentingą nacionalinę instituciją; sukurti sklandžiai veikiančią kompiuterinių incidentų tyrimo tarnybą; priimti nacionalinę TIS strategiją ir nacionalinį TIS bendradarbiavimo planą. ES institucijoms taip pat svarbus pajėgumų stiprinimas ir koordinavimas: 2012 m. buvo įsteigta nuolatinė už ES institucijų, agentūrų ir įstaigų IT sistemų saugumą atsakinga kompiuterinių incidentų tyrimo tarnyba (CERT-EU);
- parengti koordinuotos prevencijos, aptikimo, pasekmių švelninimo ir reagavimo mechanizmus, kurie sudarytų sąlygas TIS kompetentingoms nacionalinėms institucijoms keistis informacija ir viena kitai padėti. TIS kompetentingų nacionalinių institucijų bus prašoma užtikrinti tinkamą ES masto bendradarbiavimą, konkrečiai – remiantis Sąjungos TIS bendradarbiavimo planu, kuris parengiamas siekiant reaguoti į kibernetinius incidentus, darančius poveikį ne vienai valstybei narei. Tas bendradarbiavimas taip pat bus grindžiamas pažanga, pasiekta Valstybių narių Europos forumo (angl. *EFMS*)[14], kuris surengė vaisingų diskusijų ir kuriame keistasi informacija su TIS susijusios viešosios politikos klausimais; tas forumas gali būti integruotas į bendradarbiavimo mechanizmą, kai pastarasis bus sukurtas;
- stiprinti privačiojo sektoriaus parengtį ir dalyvavimą. Kadangi didžioji dauguma tinklų ir informacinių sistemų priklauso privatiems savininkams ir yra jų valdoma, sąsajų su privačiuoju sektoriumi gerinimas siekiant kibernetinio saugumo yra nepaprastai svarbus. Privatusis sektorius turėtų techniniu lygmeniu plėtoti savus kibernetinio atsparumo pajėgumus ir dalintis geriausia skirtingų sektorių patirtimi. Pramonės išplėtotos priemonės, skirtos reaguoti į incidentus, nustatyti priežastis ir atlikti teisminius tyrimus, turėtų būti naudingos ir viešajam sektoriui.

Tačiau privatiems subjektams dažnai trūksta veiksmingų paskatų teikti patikimus TIS incidentų ir jų poveikio duomenis, puoselėti rizikos valdymo kultūrą ar investuoti į saugumo sprendimus. Todėl siūlomais teisės aktais siekiama užtikrinti, kad kai kurių svarbiausių sričių – energetikos, transporto, bankininkystės, biržų ir pagrindinių interneto paslaugų teikimą užtikrinančių priemonių, taip pat viešojo administravimo – subjektai įvertintų galimą kibernetinio saugumo riziką, užtikrintų tinklų ir informacinių sistemų patikimumą ir atsparumą tinkamai valdydami riziką, dalytųsi nustatyta informacija su TIS nacionalinėmis kompetentingomis institucijomis. Kibernetinio saugumo kultūros puoselėjimas galėtų praplėsti verslo galimybes ir padidinti konkurencingumą privačiajame sektoriuje, kuris kibernetinį saugumą galėtų pabrėžti kaip savo prekės privalumą.

---

13 Direktyvos 95/46/EB 17 straipsnis; Direktyvos 2002/58/EB 4 straipsnis.

14 Valstybių narių Europos forumas buvo įkurtas remiantis dokumentu COM(2009) 149 kaip platforma, kuri palaikytų valstybių narių viešųjų institucijų diskusijas apie gerąją patirtį, susijusią su ypatingos svarbos informacinės infrastruktūros objektų saugumu ir atsparumu.

Tie subjektai turėtų teikti ataskaitas TIS kompetentingomis nacionalinėmis institucijomis apie incidentus, darančius didelį poveikį nuo tinklų ir informacinių sistemų priklausančiam pagrindinių paslaugų tęstinumui ir prekių tiekimui.

TIS nacionalinės kompetentingos institucijos turėtų bendradarbiauti ir keistis informacija su kitomis reguliavimo įstaigomis, ypač su asmens duomenų apsaugos institucijomis. Savo ruožtu TIS kompetentingos nacionalinės institucijos apie įtariamus sunkius nusikalstamo pobūdžio incidentus turėtų pranešti teisėsaugos institucijoms. Kompetentingos nacionalinės institucijos taip pat turėtų tam skirtoje svetainėje reguliariai skelbti neįslaptintą informaciją apie paskelbtus išankstinius perspėjimus dėl incidentų bei rizikos ir dėl koordinuoto reagavimo. Teisiniai įpareigojimai neturėtų nei pakeisti, nei trukdyti neoficialaus ir savanoriško bendradarbiavimo plėtros, įskaitant tarp viešojo ir privačiojo sektorių, siekiant padidinti saugumo lygį ir pasikeisti informacija bei geriausia patirtimi. Ypač patikima ir tinkama ES lygmens platforma yra Europos viešojo ir privačiojo sektorių partnerystė atsparumui užtikrinti (EP3R[15]), ir ji turi būti plėtojama toliau.

Europos infrastruktūros tinklų priemonė (EITP)[16] suteiktų finansinę paramą pagrindinei infrastruktūrai, jungiančiai valstybių narių TIS pajėgumus, ir taip palengvintų bendradarbiavimą Europos Sąjungoje.

Be to, norint išbandyti valstybių narių ir privačiojo sektoriaus bendradarbiavimą būtinos kibernetinių incidentų pratybos ES lygmeniu. Pirmosios pratybos, kuriose dalyvavo valstybės narės, įvykdytos 2010 m. (*Cyber Europe 2010*), o antrosios, į kurias įsijungė ir privatusis sektorius, vyko 2012 m. spalio mėn. (*Cyber Europe 2012*). ES ir JAV teorinio modeliavimo pratybos atliktos 2011 m. lapkričio mėn. (*Cyber Atlantic 2011*). Artimiausiais metais planuojama kitų pratybų, kai kuriose jų dalyvaus tarptautiniai partneriai.

Komisija:

- tęs Jungtinio tyrimų centro vykdomą veiklą glaudžiai bendradarbiaudama su valstybių narių institucijomis ir itin svarbios infrastruktūros savininkais ir operatoriais, kad nustatytų TIS pažeidžiamumą itin svarbioje Europos infrastruktūroje ir paskatintų atsparių sistemų kūrimą;
- 2013 m. pradžioje inicijuos ES finansuojamą bandomąjį projektą[17] dėl **kovos su kenksmingu programiniu kodu apkrėstų kompiuterių tinklais ir kenkimo programine įranga**, kad būtų sukurta ES valstybių narių, privačiojo sektoriaus organizacijų (tokių kaip interneto paslaugų teikėjai) ir tarptautinių partnerių koordinavimo ir bendradarbiavimo sistema.

---

15 Europos viešojo ir privačiojo sektorių partnerystė atsparumui užtikrinti (EP3R) buvo sukurta remiantis COM(2009) 149. Ši platforma inicijavo darbą ir skatino viešojo ir privačiojo sektorių bendradarbiavimą nustatant atsparumui reikalingus pagrindinius išteklius, priemones, funkcijas ir pagrindinius reikalavimus, taip pat bendradarbiavimo poreikius ir mechanizmus, kuriais būtų reaguojama į didelio masto sutrikimus, kurie paveikia elektroninius ryšius.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. EITP biudžeto eilutė 09.03.02 – Telekomunikacijų tinklai (skatinti nacionalinių internetu teikiamų viešųjų paslaugų sujungimą bei sąveiką ir prieigą prie tokių tinklų).

17 CIP-ICT PSP-2012-6, 325188. Jo bendras biudžetas yra 15 mln. EUR, o ES finansavimas siekia 7,7 mln. EUR.

Komisija prašo ENISA:

- padėti valstybėms narėms stiprinti **nacionalinius kibernetinio atsparumo pajėgumus**, konkrečiai – sukaupti technines žinias apie pramonės kontrolės sistemų, transporto ir energetikos infrastruktūros saugumą ir atsparumą;
- 2013 m. išnagrinėti pramonės kontrolės sistemoms skirtų reagavimo į kompiuterinius saugumo incidentus tarnybų įsteigimo galimybę Europos Sąjungoje;
- toliau remti valstybių narių ir ES institucijų pastangas vykdyti reguliarias **visos Europos kibernetinių incidentų pratybas**, kurios taip pat būtų veiklos bazė Europos Sąjungai dalyvaujant tarptautinėse kibernetinių incidentų pratybose.

Komisija Europos Parlamentą ir Tarybą kviečia:

- sparčiai priimti direktyvos dėl **bendro aukšto lygio tinklų ir informacijos saugumo** visoje Sąjungoje pasiūlymą; spręsti nacionalinių pajėgumų ir parengties, ES lygmens bendradarbiavimo klausimus; vykdyti su TIS susijusios rizikos valdymo patirties ir informacijos sklaidą ir mainus.

Komisija ragina pramonę:

- siekti lyderystės **investuojant** į aukšto lygio kibernetinį saugumą, formuoti geriausią patirtį ir dalytis informacija sektoriniu lygmeniu ir su viešojo sektoriaus institucijomis, kad būtų užtikrinta stipri ir veiksminga turto ir asmenų apsauga, ypač vykdant viešojo ir privačiojo sektoriaus partnerystes, kaip antai EP3R ir „Pasitikėjimą skaitmeniniu gyvenimu“ (TDL)[18].
-

Informuotumo didinimas

Kibernetinio saugumo užtikrinimas yra bendra atsakomybė. Galutiniams vartotojams tenka itin svarbus vaidmuo užtikrinant tinklų ir informacinių sistemų saugumą – jie turi suvokti internete slypinčią riziką ir įgyti galimybių nesudėtingais veiksmais nuo jos apsisaugoti.

Pastaraisiais metais imtasi keleto iniciatyvų ir jas reikėtų tęsti. Pavyzdžiui, ENISA didino informuotumą skelbdama ataskaitas, rengdama ekspertų seminarus ir puoselėdama viešojo ir privačiojo sektorių partnerystes. Didinant informuotumą taip pat prisideda Europolas, Eurojustas ir nacionalinės duomenų apsaugos institucijos. 2012 m. spalio mėn. ENISA su keliomis valstybėmis narėmis pradėjo bandomąjį projektą „Europos kibernetinio saugumo mėnuo“. Informuotumo didinimas yra vienas ES ir JAV kibernetinio saugumo ir kovos su

[18] http://www.trustindigitallife.eu/

elektroniniais nusikaltimais darbo grupės[19] veiklos barų ir svarbi Saugesnio interneto programos[20] (orientuotos į vaikų saugą internete) dalis.

Komisija prašo ENISA:

- 2013 m. pasiūlyti planą dėl vartotojų raštingumo tinklų ir informacijos saugumo srityje – savanoriškos sertifikavimo programos, kuri IT profesionalams, pavyzdžiui, svetainių administratoriams, padėtų gerinti įgūdžius ir kompetencijas.

Komisija:

- 2014 m. su ENISA parama organizuos kibernetinio saugumo **čempionatą**, kuriame universitetų studentai varžysis dėl geriausių TIS sprendimų.

Komisija kviečia valstybes nares[21]:

- siekiant pagerinti galutinių naudotojų informuotumą nuo 2013 m. kasmet rengti „**kibernetinio saugumo mėnesį**“, naudojantis ENISA parama ir dalyvaujant privačiajam sektoriui. Nuo 2014 m. ES ir JAV bus tuo pačiu metu rengiamas „kibernetinio saugumo mėnuo“;

- **padidinti nacionalines pastangas vykdyti švietimą ir profesinį mokymą TIS klausimais** įdiegiant: švietimą TIS klausimais mokyklose iki 2014 m.; TIS, saugios programinės įrangos plėtros ir asmens duomenų apsaugos mokymą kompiuterijos studentams; bazinį mokymą TIS klausimais viešojo administravimo įstaigų darbuotojams.

Komisija ragina pramonę:

- siekti didinti suvokimą apie kibernetinį saugumą **visais lygmenimis**: ir verslo procesuose, ir bendraujant su klientais. Svarbu, kad pramonė svarstytų, kaip generaliniams direktoriams ir valdyboms pavesti didesnę atskaitomybę už kibernetinio saugumo užtikrinimą.

2.2. Radikalus elektroninių nusikaltimų skaičiaus sumažinimas

Kuo labiau pasineriame į skaitmeninį pasaulį, tuo daugiau progų piktnaudžiauti įgyja kibernetiniai nusikaltėliai. Elektroniniai nusikaltimai yra viena sparčiausiai dažnėjančių

[19] Tai darbo grupei, įkurtai 2010 m. lapkričio mėn. ES ir JAV viršūnių susitikime (MEMO/10/597), pavesta formuoti bendradarbiavimo modelius įvairiais kibernetinio saugumo ir elektroninių nusikaltimų klausimais.

[20] Pagal Saugesnio interneto programą finansuojamas nevyriausybinių organizacijų, siekiančių užtikrinti vaikų gerovę internete, tinklas, teisėsaugos institucijų, kurios dalijasi informacija ir geriausia patirtimi, susijusia su interneto naudojimu nusikalstamiems tikslams (seksualinės prievartos prieš vaikus medžiagos platinimu), tinklas ir tyrėjų, kurie kaupia informaciją apie interneto technologijų naudojimo, rizikos ir pasekmių vaikų gyvenimui, tinklas.

[21] Įtraukiant atitinkamas nacionalines institucijas, įskaitant TIS kompetentingas institucijas ir duomenų apsaugos institucijas.

nusikaltimo formų: kasdien jų aukomis tampa daugiau nei milijonas žmonių. Kibernetiniai nusikaltėliai ir elektroninių nusikaltimų tinklai tampa vis sudėtingesni; kovojant su jais mums reikia apsirūpinti tinkamomis veiklos priemonėmis ir pajėgumais. Elektroniniai nusikaltimai labai pelningi ir kelia mažą grėsmę piktadariams, kurie paprastai pasinaudoja svetainių domenų anonimiškumu. Elektroninių nusikaltimų sienos nesulaiko: pasaulinė interneto skvarba reiškia, kad norėdamos duoti atkirtį šiai augančiai grėsmei teisėsaugos institucijos turi veikti koordinuotai ir bendradarbiaudamos.

Griežti ir veiksmingi teisės aktai

Kovoje su elektroniniais nusikaltimais ES ir valstybėms narėms reikia griežtų ir veiksmingų teisės aktų. Europos Tarybos konvencija dėl elektroninių nusikaltimų, dar vadinama Budapešto konvencija, yra teisiškai įpareigojanti tarptautinė sutartis, kurioje numatyta veiksminga sistema, taikytina priimant nacionalinius teisės aktus.

ES jau yra priėmusi teisės aktus dėl elektroninių nusikaltimų, įskaitant direktyvą dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija[22]. Be to, ES beveik baigė susitarti dėl Direktyvos dėl išpuolių prieš informacines sistemas, ypač naudojant kenksmingu programiniu kodu apkrėstų kompiuterių tinklus.

Komisija:

- užtikrins spartų direktyvų dėl elektroninių nusikaltimų perkėlimą ir įgyvendinimą;
- paragins valstybes nares, kurios dar neratifikavo **Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų**, kuo greičiau ratifikuoti ir įgyvendinti jos nuostatas.

Veiklos pajėgumų kovai su elektroniniais nusikaltimais didinimas

Elektroninių nusikaltimų technologijos sparčiai tobulėjo ir teisėsaugos institucijos negali kovoti su elektroniniais nusikaltimais pasenusiomis veiklos priemonėmis. Šiuo metu ne visos ES valstybės narės turi veiklos pajėgumų, kurių reikia norint veiksmingai reaguoti į elektroninius nusikaltimus. Visoms valstybėms narėms reikalingi veiksmingi nacionaliniai elektroninių nusikaltimų padaliniai.

Komisija:

- finansavimo programomis[23] padės valstybėms narėms **nustatyti spragas ir sustiprinti** elektroninių nusikaltimų tyrimo ir kovos su jais **pajėgumus**. Komisija toliau rems subjektus, kurie suveda mokslo ir akademinės visuomenės atstovus, teisėsaugos vykdytojus ir privatųjį sektorių ir kurių darbas panašus į Komisijos finansuojamų elektroninių nusikaltimų kompetencijos centrų, kuriuos jau įsteigė

[22] Direktyva 2011/93/ES, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR.

[23] 2013 m. – pagal Nusikalstamumo prevencijos ir kovos su nusikalstamumu programą (ISEC). Po 2013 m. – naudojant Vidaus saugumo fondą (naują daugiametės finansinės programos priemonę).

kai kurios valstybės narės;

- kartu su valstybėmis narėmis koordinuos pastangas nustatyti kovos su elektroniniais nusikaltimais geriausią praktiką ir geriausias turimas technologijas (panaudojant ir Jungtinio tyrimų centro paramą, pavyzdžiui, dėl teisminių techninių priemonių plėtros ir naudojimo arba dėl grėsmių analizės);

- glaudžiai bendradarbiaus su neseniai **Europolo struktūroje sukurtu Europos kovos su elektroniniu nusikalstamumu centru (EC3)** ir su Eurojustu siekiant tokius politikos modelius suderinti su geriausia operatyvine patirtimi.

ES lygmens koordinavimo gerinimas

ES gali papildyti valstybių narių darbą sudarydama geresnes sąlygas koordinuojamajam ir bendradarbiaujamajam modeliui, pagal kurį kartu dalyvauja teisėsaugos ir teismų institucijos, viešojo ir privačiojo sektorių suinteresuotosios šalys iš ES ir kitur.

Komisija:

- rems neseniai įsteigtą **Europos kovos su elektroniniu nusikalstamumu centrą** (EC3) kaip Europos kovos su elektroniniais nusikaltimais ryšių centrą. EC3 teiks analitinę ir žvalgybinę informaciją, rems tyrimus, suteiks aukšto lygio teisminės ekspertizės paslaugas, gerins bendradarbiavimo sąlygas, sukurs forumus valstybių narių kompetentingų institucijų, privačiojo sektoriaus ir kitų suinteresuotųjų šalių informacijos mainams ir palaipsniui taps teisėsaugos institucijų bendrijos balsu[24];

- rems pastangas padidinti domenų vardų registratorių atskaitomybę ir užtikrinti informacijos apie svetainės savininką tikslumą ir tuo tikslu remsis teisėsaugos rekomendacijomis Interneto vardų ir numerių paskyrimo korporacijai (ICANN) laikydamasi Sąjungos teisės aktų, įskaitant duomenų apsaugos taisykles;

- remsis pastarojo meto teisės aktais, kad būtų stiprinamos ES pastangos kovoti su seksualine prievarta prieš vaikus internete. Komisija priėmė Europos strategiją dėl vaikams geresnio interneto[25] ir kartu su ES ir kitomis valstybėmis sukūrė **pasaulinę kovos su seksualine prievarta prieš vaikus internete sąjungą**[26]. Ta sąjunga yra atrama tolesniems valstybių narių veiksmams, kuriuos remia Komisija ir EC3.

Komisija prašo Europolo (EC3):

[24] 2012 m. kovo 28 d. Europos Komisija priėmė komunikatą „Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su elektroniniu nusikalstamumu centro kūrimas“.

[25] COM(2012) 196 galutinis.

[26] 2012 m. birželio 7–8 d. Tarybos išvados dėl pasaulinės kovos su seksualine prievarta prieš vaikus internete sąjungos (ES ir JAV jungtinis pareiškimas) ir Deklaracija dėl pasaulinės kovos su seksualine prievarta prieš vaikus internete sąjungos sukūrimo (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

- iš pradžių skirti analitinę ir veiklos paramą valstybių narių elektroninių nusikaltimų tyrimams siekiant išardyti ir sustabdyti elektroninių nusikaltimų tinklus, pirmiausia tuos, kurie veikia seksualinės prievartos prieš vaikus, sukčiavimo atliekant mokėjimą, kenksmingu programiniu kodu apkrėstų kompiuterių tinklų ir įsilaužimo srityse;

- reguliariai rengti strategines ir veiklos ataskaitas dėl tendencijų ir kylančių naujų grėsmių, kad kovos su elektroniniais nusikaltimais grupės valstybėse narėse nusistatytų prioritetus ir tiriamosios veiklos kryptis.

Komisija prašo Europos policijos koledžo (CEPOL) bendradarbiaujant su Europolu:

- koordinuoti mokymo kursų parengimą ir planavimą, kad teisėsaugos darbuotojai įgytų informacijos ir techninių žinių veiksmingai kovai su elektroniniais nusikaltimais.

Komisija prašo Eurojusto:

- nustatyti pagrindines teisminio bendradarbiavimo kliūtis vykdant elektroninių nusikaltimų tyrimus ir valstybėms narėms koordinuojant veiksmus su trečiosiomis šalimis; remti elektroninių nusikaltimų tyrimą ir persekiojimą veiklos ir strateginiais lygmenimis, taip pat tos srities mokymo veiklą.

Komisija prašo Eurojusto ir Europolo (EC3):

- glaudžiai bendradarbiauti, *inter alia*, keičiantis informacija, kad jie pagal savo įgaliojimus ir kompetenciją veiksmingiau kovotų su elektroniniais nusikaltimais.

2.3. Kibernetinės gynybos politikos ir pajėgumų, susijusių su bendra saugumo ir gynybos politikos sistema, plėtojimas

Kibernetinio saugumo pastangos Europos Sąjungoje turi būti dedamos ir kibernetinės gynybos srityje. Siekiant sustiprinti valstybių narių gynybos ir nacionalinio saugumo interesams naudojamas ryšių ir informacinės sistemas, kibernetinės gynybos pajėgumai turėtų būti plėtojami aptikimo, reagavimo ir atkūrimo po sudėtingų kibernetinių grėsmių segmentuose.

Kadangi grėsmės yra įvairialypės, reikėtų stiprinti modelių, kuriuos taiko civiliai ir kariškiai saugodami itin svarbius kibernetinius išteklius sinergiją. Tos pastangos turėtų būti palaikomos moksliniais tyrimais ir technologine plėtra, vykdoma glaudžiai bendradarbiaujant vyriausybėms, privačiajam sektoriui ir akademiniams sluoksniams Europos Sąjungoje. Siekiant išvengti kartojimosi, ES turėtų ištirti galimybes, kaip ES ir NATO galėtų papildyti viena kitos pastangas didinti itin svarbių vyriausybės, gynybos ir kitų informacinių infrastruktūrų, nuo kurių priklauso abiejų organizacijų narės, atsparumą.

Vyriausiasis įgaliotinis sutelks dėmesį į toliau nurodomus pagrindinius veiksmus ir paragins valstybes nares ir Europos gynybos agentūrą bendradarbiauti:

- įvertinti operatyvinius ES kibernetinės gynybos reikalavimus ir skatinti ES kibernetinės gynybos pajėgumų ir technologinę plėtrą atsižvelgiant į visus pajėgumų plėtros aspektus, įskaitant doktriną, vadovavimą, organizavimą, personalą, mokymą, technologiją, infrastruktūrą, logistiką ir sąveikumą;

- plėtoti ES kibernetinės gynybos politikos sistemą (įskaitant dinaminį rizikos valdymą, patobulintą grėsmių analizę ir dalijimąsi informacija), kad būtų apsaugomi bendros saugumo ir gynybos politikos misijų ir operacijų tinklai. Pagerinti kibernetinės gynybos mokymo ir pratybų galimybes kariškiams europiniu ir tarptautiniu mastu, įskaitant kibernetinės gynybos elementų integravimą į esamus pratybų katalogus;

- skatinti dialogą ir koordinavimą tarp civilinių ir karinių subjektų Europos Sąjungoje ypač akcentuojant keitimąsi geriausia patirtimi ir informacija, išankstinį perspėjimą, reagavimą į incidentus, rizikos vertinimą, informuotumo didinimą ir kibernetinio saugumo iškėlimą į prioritetus;

- užtikrinti dialogą su tarptautiniais partneriais, įskaitant NATO, kitas tarptautines organizacijas ir daugiašalius kompetencijos centrus, kad būtų užtikrinti veiksmingi gynybos pajėgumai; nustatyti bendradarbiavimo sritis ir išvengti pastangų dubliavimo.

2.4. Pramonės ir technologinių išteklių plėtra siekiant kibernetinio saugumo

Europa turi puikių MTTP pajėgumų, tačiau daugelis novatoriškas IRT prekes ir paslaugas teikiančių pasaulinių lyderių įsisteigę ne Europos Sąjungoje. Kyla grėsmė, kad Europa taps pernelyg priklausoma ne tik nuo kitur pagamintų IRT, bet ir nuo anapus jos sienų sukurtų saugumo sprendimų. Būtina užtikrinti, kad ES ir trečiosiose šalyse pagaminta techninė ir programinė įranga, kuri naudojama ypatingos svarbos paslaugoms ir infrastruktūrai, ir vis labiau – nešiojamiesiems įtaisams, būtų patikima, saugi ir užtikrintų asmens duomenų apsaugą.

Kibernetinio saugumo prekių bendrosios rinkos skatinimas

Aukštas saugumo lygis gali būti užtikrintas tik tada, kai visi vertės grandinės dalyviai, kaip antai įrangos gamintojai, programinės įrangos kūrėjai, informacinės visuomenės paslaugų teikėjai, saugumui teiktų pirmenybę. Tačiau panašu[27], kad daugelis dalyvių saugumą vertina vos ne kaip papildomą naštą, ir saugumo sprendimų paklausa yra menka. Reikia, kad visoje Europoje naudojamų IRT produktų vertės grandinėje būtų įgyvendinti atitinkami kibernetinio saugumo užtikrinimo reikalavimai. Privatųjį sektorių reikia skatinti užtikrinti aukštą kibernetinio saugumo lygį, pavyzdžiui, bendrovių, kurios nuolat užtikrina gerą kibernetinį saugumą, prekės galėtų išsiskirti ženklinimu, kuriuo nurodomas tinkamas kibernetinio saugumo užtikrinimo lygis, ir taip įgyti konkurencinį pranašumą. Be to, siūlomoje tinklų ir informacijos saugumo direktyvoje numatytos prievolės galėtų labai padėti didinti bendrovių konkurencingumą aptariamuose sektoriuose.

[27] Žr. kartu su Komisijos pasiūlymu dėl direktyvos dėl tinklų ir informacijos saugumo pateikiamo Komisijos tarnybų darbinio dokumento (poveikio vertinimo) 4.1.5.2 skirsnį.

Taip pat visoje Europoje turėtų būti stimuliuojama rinkos paklausa itin saugioms prekėms. Pirma, šia strategija siekiama padidinti bendradarbiavimą ir skaidrumą IRT prekių saugumo klausimais. Joje raginama sukurti platformą, kurioje atitinkamos Europos viešosios ir privačiosios suinteresuotosios šalys bendradarbiautų: nustatytų geriausią kibernetinio saugumo patirtį visoje vertės grandinėje ir sukurtų palankias rinkos sąlygas saugiems IRT sprendimams plėtoti ir diegti. Pirmiausia reikia stengtis sukurti paskatas tinkamai valdyti riziką ir priimti saugos standartus bei sprendimus, taip pat galbūt sukurti visoje ES veikiančias savanoriškas sertifikavimo schemas, kurios būtų pagrįstos ES ir tarptautiniu mastu taikomomis schemomis. Komisija skatins valstybes nares priimti tarpusavyje derančius modelius, kad būtų išvengta nevienodų sąlygų, kai tam tikrose šalyse veikiančios įmonės atsiduria nepalankioje padėtyje.

Antra, Komisija rems saugumo standartų plėtrą ir padės plėtoti ES masto savanoriškas sertifikavimo schemas nuotolinės kompiuterijos srityje, tinkamai atsižvelgdama į poreikį užtikrinti duomenų apsaugą. Darbas turėtų būti orientuotas į tiekimo grandinės patikimumą, pirmiausia ypatingos svarbos ekonominiuose sektoriuose (pramoninės kontrolės sistemų, energetikos ir transporto infrastruktūrų sektoriuose). Toks darbas turėtų būti paremtas darbu, kurį nuolat vykdo Europos standartizavimo organizacijos (CEN, CENELEC ir ETSI)[28], Kibernetinio saugumo koordinavimo grupė (angl. CSCG), taip pat ENISA, Komisijos ir kitų su tuo susijusių subjektų techninėmis žiniomis.

Komisija:

- 2013 m. sukurs viešąjį ir privatųjį sektorius jungiančią **tinklų ir informacijos saugumo sprendimų platformą**, kuri plėtotų paskatas diegti saugius IRT sprendimus ir įtvirtinti Europoje naudojamų IRT prekių ženklinimą pagal kibernetinio saugumo užtikrinimo lygį;

- 2014 m. remdamasi platformos darbo rezultatais pasiūlys rekomendacijas, pagal kurias kibernetinis saugumas būtų užtikrintas visoje IRT vertės grandinėje;

- išnagrinės, kaip didžiausi IRT techninės ir programinės įrangos tiekėjai galėtų informuoti nacionalines kompetentingas institucijas apie nustatytą pažeidžiamumą, kuris galėtų padaryti didelį su saugumu susijusį poveikį.

Komisija prašo ENISA:

- bendradarbiaujant su atitinkamomis nacionalinėmis kompetentingomis institucijomis, atitinkamomis suinteresuotosiomis šalimis, tarptautinėmis ir Europos standartizacijos organizacijomis ir Europos Komisijos jungtiniu tyrimo centru parengti **tinklų ir informacijos saugumo standartų ir geriausios patirties diegimo** viešajame ir privačiajame sektoriuose **technines gaires ir rekomendacijas**.

Komisija kviečia viešojo ir privačiojo sektorių suinteresuotąsias šalis:

- duoti akstiną IRT prekių gamintojams ir paslaugų tiekėjams, įskaitant nuotolinės

[28] Ypač rengiant Modernių energetikos tinklų standartą M/490, numatytą pirmam modernaus energetikos tinklo ir pavyzdinės architektūros standartų rinkiniui.

kompiuterijos paslaugų tiekėjus, kad jie plėtotų ir diegtų atsižvelgiant į pramonę pasirinktus **saugumo standartus** bei technines normas ir taikytų principus, pagal kuriuos nuo pat pradžių atsižvelgiama į saugumą ir privatumą; naujos kartos programinę ir techninę įrangą gaminti su **stipresnėmis, įterptomis ir naudotojui patogiomis saugumo** priemonėmis;

- rengti atsižvelgiant į pramonę nustatomus bendrovių kibernetinio saugumo užtikrinimo standartus ir geriau informuoti visuomenę plėtojant **saugumo ženklinimą** arba *Kitemark* tipo ženklus, kurie vartotojui padėtų susiorientuoti rinkoje.

Mokslinių tyrimų ir technologijų plėtros (MTTP) investicijų ir inovacijų palaikymas

MTTP gali užtikrinti tvirtą pramonės politiką, palaikyti patikimą europinę IRT pramonę, išjudinti vidaus rinką ir sumažinti Europos priklausomybę nuo užsienio technologijų. MTTP turėtų užpildyti technologines spragas IRT saugumo srityje, padėti pasirengti naujai saugumo uždavinių kartai, padėti atsižvelgti į nuolatinę naudotojų poreikių raidą ir pasinaudoti dvejopo naudojimo technologijų teikiamomis galimybėmis. MTTP taip pat turėtų būti toliau naudojama kriptografijos plėtrai paremti. Be to, reikia pastangų, kad suteikiant reikiamas paskatas ir sudarant tinkamas politikos sąlygas MTTP rezultatai būtų panaudojami diegiant komercinius sprendimus.

ES turėtų maksimaliai išnaudoti „Horizonto 2020“[29] mokslinių tyrimų ir inovacijų bendrąją programą, kuri turi būti pradėta įgyvendinti 2014 m. Komisijos pasiūlyme įrašyti konkretūs su strategija derantys tikslai, skirti patikimoms IRT ir kovai su elektroniniais nusikaltimais. Pagal „Horizontą 2020“ bus remiami su kuriamomis IRT susiję saugumo moksliniai tyrimai; pateikiami sprendimai saugioms viso proceso metu veikiančioms IRT sistemoms, paslaugoms ir prietaikoms; suteikiamos paskatos įgyvendinti ir įdiegti esamus sprendimus; sprendžiamos tinklų ir informacijos sistemų sąveikos problemos. Ypač bus stengiamasi ES lygmeniu tobulinti ir geriau koordinuoti skirtingas finansavimo programas („Horizontą 2020“, Vidaus saugumo fondą, Europos gynybos agentūros mokslinius tyrimus, įskaitant Europos bendradarbiavimo sistemą (angl. *European Framework Cooperation*)).

Komisija:

- naudos „Horizontą 2020“ siekdama spręsti įvairius IRT privatumo ir saugumo klausimus visuose etapuose nuo MTTP iki inovacijų ir diegimo. Pagal „Horizontą 2020“ bus plėtojamos priemonės ir įrankiai kovai su nusikalstama ir teroristine veikla, kuri nukreipta į kibernetinę aplinką;

- sukurs geresnius ES institucijų ir valstybių narių mokslinių tyrimų darbotvarkių koordinavimo mechanizmus ir suteiks paskatų valstybėms narėms daugiau

[29] „Horizontas 2020“ yra finansinė priemonė, kuria įgyvendinima Inovacijų sąjunga, „Europos 2020“ pavyzdinė iniciatyva, kuria siekiama užtikrinti Europos konkurencingumą pasaulyje. Nauja ES mokslinių tyrimų ir inovacijų bendroji programa, kuri bus vykdoma nuo 2014–2020 m., yra viena pastangų skatinti naują augimą ir darbo vietų kūrimą Europoje.

investuoti į MTTP.

Komisija kviečia valstybes nares:

- iki 2013 m. pabaigos sukaupti geriausią patirtį, kaip panaudoti **viešojo administravimo įstaigų perkamąją galią** (pavyzdžiui, vykdant viešuosius pirkimus) skatinant saugumo funkcijų plėtrą ir diegimą IRT prekėse ir paslaugose;

- skatinti ankstyvą pramonės ir akademinių sluoksnių įsitraukimą plėtojant ir koordinuojant sprendimus. Tai turėtų būti daroma visapusiškai panaudojant Europos pramoninę bazę bei tos srities MTTP technologines inovacijas ir koordinuojant civilinių ir karinių organizacijų mokslinių tyrimų darbotvarkes.

Komisija prašo Europolo ir ENISA:

- nustatyti ryškėjančias tendencijas ir poreikius atsižvelgiant į elektroninių nusikaltimų raidą ir kibernetinio saugumo modelius, kad būtų sukurtos tinkamos teisminės skaitmeninės priemonės ir technologijos;

Komisija kviečia viešąsias ir privačiąsias suinteresuotąsias šalis :

- bendradarbiaujant su draudimo sektoriumi sukurti **suderintus rizikos priedų apskaičiavimo parametrus**, kurie sudarytų sąlygas į saugumą investavusioms bendrovėms mokėti mažesnius rizikos priedus.

2.5. Nuoseklios ES tarptautinės kibernetinės politikos sukūrimas ir ES pagrindinių vertybių rėmimas

Išsaugoti atvirą, laisvą ir saugią kibernetinę erdvę yra pasaulinio masto uždavinys, kurį ES turėtų spręsti kartu su atitinkamais tarptautiniais partneriais ir organizacijomis, privačiuoju sektoriumi ir pilietine visuomene.

Tarptautine kibernetinės erdvės politika ES sieks skatinti interneto atvirumą ir laisvę, palaikys pastangas formuoti elgesio normas ir taikyti kibernetinėje erdvėje galiojančius tarptautinius teisės aktus. ES taip pat sieks mažinti skaitmeninę atskirtį ir aktyviai prisidės prie tarptautinių pastangų sukurti kibernetinio saugumo pajėgumus. ES tarptautinis įsipareigojimas kibernetiniais klausimais bus grindžiamas ES pagrindinėmis vertybėmis – žmogaus orumu, laisve, demokratija, lygybe, teisinės valstybės principais ir pagarba pagrindinėms teisėms.

Kibernetinės erdvės klausimų susiejimas su ES išorės santykiais ir bendra išorės ir saugumo politika

Komisija, Vyriausiasis įgaliotinis ir valstybės narės turėtų suformuluoti nuoseklią ES tarptautinę kibernetinės erdvės politiką, kurios tikslas – sustiprinti įsipareigojimų sąsajas ir ryšius su pagrindiniais tarptautiniais partneriais ir organizacijomis, taip pat su pilietine visuomene ir privačiuoju sektoriumi. ES konsultacijos kibernetinės erdvės klausimais su tarptautiniais partneriais turėtų būti parengiamos, koordinuojamos ir įgyvendinamos taip, kad šiuo metu vykstantys dvišaliai ES valstybių narių ir trečiųjų šalių dialogai taptų naudingesni. ES iš naujo akcentuos dialogą su trečiosiomis šalimis ir bus ypač dėmesinga panašaus

požiūrio besilaikantiems partneriams, kurių vertybės tokios pačios kaip ir Europos Sąjungos. Ji skatins siekti aukšto duomenų apsaugos lygio, įskaitant perduodant duomenis trečiajai šaliai. Spręsdama kibernetinės erdvės pasaulinius uždavinius ES sieks glaudžiau bendradarbiauti su toje srityje veikiančiomis organizacijomis, pavyzdžiui, Europos Taryba, EBPO, JT, ESBO, NATO, AS, ASEAN ir Amerikos valstybių organizacija. Dvišaliu lygmeniu ypač svarbus bendradarbiavimas su Jungtinėmis Valstijomis ir jis bus plėtojamas toliau, konkrečiai – ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupėje.

Vienas iš pagrindinių ES tarptautinės kibernetinės erdvės politikos elementų bus siekti, kad kibernetinė erdvė būtų laisvės ir pagrindinių teisių erdve. Prieigos prie interneto didinimas turėtų skatinti demokratines reformas ir jų palaikymą visame pasaulyje. Pasaulyje gausėjant ryšių, neturėtų daugėti cenzūros ar masinio stebėjimo. ES turėtų remti bendrovių socialinę atsakomybę[30] ir imtis tarptautinių iniciatyvų pasauliniam koordinavimui toje srityje gerinti.

Atsakomybė už saugesnę kibernetinę erdvę tenka visiems pasaulinės informacinės visuomenės dalyviams – nuo piliečių iki vyriausybių. ES turėtų remti pastangas apibrėžti elgesio kibernetinėje erdvėje normas, kurių turėtų laikytis visos suinteresuotosios šalys. Kaip ES tikisi, kad internete piliečiai laikysis pilietinių pareigų, socialinės atsakomybės ir įstatymų, taip ir valstybės turėtų laikytis normų ir galiojančių teisės aktų. Tarptautinio saugumo klausimais ES skatina plėtoti pasitikėjimo stiprinimo priemones kibernetinio saugumo srityje, o valstybes ragina veikti skaidriau ir mažinti klaidingo suvokimo riziką.

ES neragina kurti naujų tarptautinių teisinių dokumentų kibernetinės erdvės klausimais.

Teisinių įsipareigojimų, kurie įtvirtinti Tarptautiniame pilietinių ir politinių teisių pakte, Europos žmogaus teisių konvencijoje ir ES pagrindinių teisių chartijoje, turėtų būti laikomasi ir internete. ES pirmiausia ieškos būdų, kaip užtikrinti tų priemonių vykdymą ir kibernetinėje erdvėje.

Kovoje su elektroniniais nusikaltimais Budapešto konvencija yra dokumentas, kurį gali priimti ir trečiosios šalys. Ji yra pavyzdys rengiant nacionalinius kovos su elektroniniais nusikaltimais teisės aktus ir tarptautinio bendradarbiavimo šioje srityje pagrindas.

Jei į kibernetinę erdvę persikelia ginkluoti konfliktai, tada bus taikoma tarptautinė humanitarinė teisė ir, kai tinka, žmogaus teisių nuostatos. **Pajėgumų didinimas kibernetinio saugumo klausimais ir atsparių informacinių infrastruktūrų trečiosiose šalyse plėtojimas**

Sustiprinus tarptautinį bendradarbiavimą sklandžiau ims veikti bazinės infrastruktūros, kurias naudojant teikiamos ir palengvinamos ryšių paslaugos. Tai vyktų keičiantis geriausia patirtimi, dalijantis informacija, iš anksto perspėjant, vykdant jungtines ankstyvojo incidentų valdymo pratybas ir pan. ES padės siekti šio tikslo stengdamasi, kad būtų intensyviau dedamos tarptautinės pastangos sustiprinti ypatingos svarbos informacinės infrastruktūros apsaugos bendradarbiavimo tinklus, kuriuose dalyvauja vyriausybės ir privatusis sektorius.

[30] „Atnaujinta 2011–2014 m. ES įmonių socialinės atsakomybės strategija“; COM(2011) 681 galutinis

Dėl atviros, saugios, sąveikios ir patikimos prieigos stygiaus teigiamas interneto poveikis pasiekia ne visas pasaulio dalis. Todėl Europos Sąjunga toliau palaikys valstybių pastangas ieškoti būdų savo gyventojams užtikrinti didesnę interneto prieigą ir naudojimą, užtikrinti jo vientisumą ir saugumą, veiksmingai kovoti su elektroniniais nusikaltimais.

Bendradarbiaudami su valstybėmis narėmis Komisija ir Vyriausiasis įgaliotinis:

- dirbs, kad būtų suformuota nuosekli ES tarptautinė kibernetinės erdvės politika, kurios tikslas – stiprinti sąsajas su pagrindiniais tarptautiniais partneriais ir organizacijomis, susieti kibernetinės erdvės klausimus su bendra užsienio ir saugumo politika, gerinti koordinavimą pasauliniais kibernetinės erdvės klausimais;

- rems elgesio normų formavimą ir pasitikėjimo stiprinimo priemones kibernetinio saugumo klausimais. Sudarys geresnes sąlygas dialogams dėl būdų, kaip taikyti tarptautinę teisę kibernetinėje erdvėje ir remti Budapešto konvencijos taikymą kovoje su elektroniniais nusikaltimais;

- rems pagrindinių teisių, įskaitant prieigos prie informacijos ir žodžio laisvės, palaikymą ir apsaugą tokiais būdais: a) plėtos naujas viešas gaires dėl žodžio laisvės internete ir realioje erdvėje; b) stebės prekių ir paslaugų, kurios galėtų būti panaudotos cenzūrai ir masiniam stebėjimui internete, eksportą; c) plėtos priemones ir įrankius, kuriais būtų plečiama prieiga prie interneto, jo atvirumas ir atsparumas cenzūrai bei masiniam stebėjimui ryšių technologijomis; d) suteiks suinteresuotosioms šalims galių naudoti ryšių technologijas pagrindinėms teisėms įtvirtinti;

- kartu su tarptautiniais partneriais ir organizacijomis, privačiuoju sektoriumi ir pilietine visuomene įsipareigos remti bendrą pajėgumų stiprinimą trečiosiose šalyse, kad pagerėtų prieiga prie informacijos ir prie atviro interneto; taip pat kad būtų išvengta kibernetinių grėsmių ir kad jos, įskaitant atsitiktinius įvykius, elektroninius nusikaltimus ir kibernetinį terorizmą, būtų įveiktos; ir kad būtų plėtojamas donorų tarpusavio koordinavimas stebint pajėgumų stiprinimo pastangas;

- naudos skirtingas ES pagalbos priemones kibernetinio saugumo pajėgumams stiprinti, įskaitant teisėsaugos, teismų ir techninių darbuotojų apmokymą kovai su kibernetinėmis grėsmėmis; taip pat remti atitinkamų nacionalinių politikos krypčių, strategijų ar institucijų kūrimą trečiosiose šalyse;

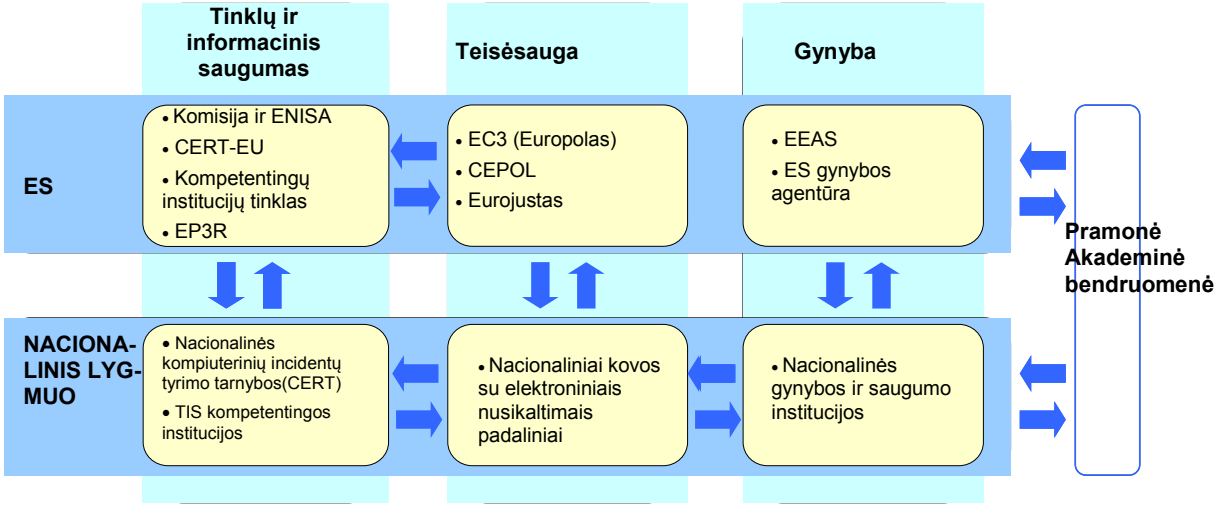
- stiprins politikos koordinavimą ir keitimąsi informacija per ypatingos svarbos informacinės infrastruktūros apsaugos bendradarbiavimo tinklus, kaip antai Meridiano tinklą, bendradarbiaujant tinklų ir informacijos saugumo srityje kompetentingoms institucijoms ir kitoms institucijoms.

3. UŽDUOTYS IR KOMPETENCIJA

Skaitmeninėje ekonomikoje ir visuomenėje, kur visa tarpusavyje susiję, sienos kibernetinių incidentų nesulaiko. Visi subjektai (nuo tinklų ir informacijos saugumo srityje kompetentingų institucijų, kompiuterinių incidentų tyrimo tarnybų ir teisėsaugos institucijų iki pramonės) turi

imtis atsakomybės tiek nacionaliniu, tiek ES lygmeniu ir dirbti drauge siekdami stiprinti kibernetinį saugumą. Kadangi teisinės bazės ir jurisdikcijos gali nesutapti, pagrindinis Europos Sąjungos uždavinys – paaiškinti suinteresuotųjų subjektų, kurių yra daug, užduotis ir kompetenciją.

Dėl objekto kompleksiškumo ir didžiulės suinteresuotųjų subjektų įvairovės, centralizuotą europinę priežiūrą pasiūlyti nėra tikslinga. Nacionalinės vyriausybės yra labiausiai pajėgios organizuoti kibernetinių incidentų ir išpuolių prevenciją ir atsaką į juos, užmegzti ryšius ir sukurti tinklus su privačiuoju sektoriumi ir plačiąja visuomene aprėpdamos visas savo politikos kryptis ir teisines bazes. Tačiau norint, kad reakcija nacionaliniu lygmeniu būtų veiksminga, dažnai reikėtų ES lygmens įsikišimo, nes grėsmės dėl savo pobūdžio gali būti arba yra tokios, kad sienos jų nesulaiko. Kibernetinis saugumas gali būti visapusiškai užtikrintas tik remiantis trimis pagrindiniais elementais – tinklų ir informacijos saugumo, teisėsaugos ir gynybos – kurių kiekvienam galioja skirtingos teisinės bazės:



3.1. Tinklų ir informacijos saugumo srityje kompetentingų institucijų arba kompiuterinių incidentų tyrimo tarnybų, teisėsaugos ir gynybos institucijų tarpusavio koordinavimas

Nacionaliniu lygmeniu

Valstybės narės turėtų jau šiandien (arba įgyvendinusios strategiją) turėti struktūras, kurioms būtų pavesti kibernetinio atsparumo, elektroninių nusikaltimų ir gynybos klausimai; tos struktūros turėtų pasiekti reikalaujamą pajėgumo įveikti kibernetinius incidentus lygį. Tačiau kadangi kai kurie subjektai gali būti įpareigoti veikti skirtingais kibernetinio saugumo lygmenimis ir kadangi labai svarbu įtraukti privatųjį sektorių, reikėtų pagerinti skirtingų ministerijų koordinavimą nacionaliniu lygmeniu. Valstybės narės turėtų kibernetinio saugumo strategijose nustatyti skirtingų nacionalinių subjektų užduotis ir kompetenciją.

Kad valstybės narės ir privatusis sektorius nuolat matytų skirtingų grėsmių panoramą ir geriau suvoktų naujas tendencijas bei technologijas, kurios naudojamos kibernetiniams išpuoliams vykdyti ir sparčiau į juos reaguoti, reikėtų skatinti nacionalinių subjektų keitimąsi informacija tarpusavyje ir su privačiuoju sektoriumi. Sukurdamos nacionalinius tinklų ir informacijos saugumo bendradarbiavimo planus, kuriuos būtų galima panaudoti kibernetinių išpuolių

atveju, valstybės narės turėtų galėti aiškiai paskirstyti užduotis bei kompetencijas ir pagerinti atsakomuosius veiksmus.

ES lygmeniu

Kaip ir nacionaliniu, taip ir ES lygmeniu kibernetiniu saugumu rūpinasi nemažai subjektų. ENISA, Europolo EC3 ir Europos gynybos agentūra yra trys agentūros, kurios veikia atitinkamai tinklų ir informacijos saugumo, teisėsaugos ir gynybos srityse. Tos agentūros turi valdančiąsias tarybas, kuriose atstovaujamos valstybės narės, ir jos sudaro sąlygas koordinuoti veiksmus ES lygmeniu.

Bus skatinamas ENISA, Europolo EC3 ir Europos gynybos agentūros koordinavimas ir bendradarbiavimas daugelyje sričių, kuriose veikia jos visos: analizuojant tendencijas, vertinant riziką, vykdant mokymą ir dalijantis geriausia patirtimi. Jos turėtų bendradarbiauti ir sykiu išsaugoti savo ypatumus. Tos agentūros kartu su CERT-EU, Komisija ir valstybėmis narėmis turėtų palaikyti patikimos techninių ir politikos ekspertų bendruomenės formavimąsi šioje srityje.

Neformalūs koordinavimo ir bendradarbiavimo būdai bus papildyti oficialesniais ryšiais. ES ginkluotųjų pajėgų atstovai ir Europos gynybos agentūros kibernetinės apsaugos projekto komanda turėtų padėti vykdyti koordinavimą gynybos srityje. Europolo EC3 programos valdyboje tarp kitų subjektų dalyvaus Eurojustas, Europos policijos koledžas (CEPOL), valstybės narės[31], ENISA ir Komisija, ir joje bus sudarytos sąlygos kiekvienai institucijai pasidalyti skirtingomis praktinėmis žiniomis ir užtikrinti, kad EC3 veikla būtų vykdoma laikantis partnerystės principų, pripažįstant papildomą visų suinteresuotųjų subjektų praktinių žinių naudą ir atsižvelgiant į jų įgaliojimus. Nauji įgaliojimai turėtų sudaryti sąlygas agentūrai ENISA užmegzti daugiau ryšių su Europolu ir sustiprinti ryšius su pramonės suinteresuotosiomis šalimis. Svarbiausia tai, kad Komisijos teisės akto dėl tinklų ir informacijos saugumo pasiūlymu būtų sukurta bendradarbiavimo per nacionalines institucijas, kompetentingas tinklų ir informacijos saugumo srityje, sistema ir sudarytos sąlygos tinklų ir informacijos saugumo institucijoms keistis informacija su teisėsaugos institucijomis.

Tarptautiniu lygmeniu

Komisija ir Vyriausiasis įgaliotinis kartu su valstybėmis narėmis užtikrina koordinuotą tarptautinę veiklą kibernetinio saugumo srityje. Tokiu būdu Komisija ir Vyriausiasis įgaliotinis puoselės ES pagrindines vertybes ir skatins taikų, atvirą ir skaidrų interneto technologijų naudojimą. Komisija, Vyriausiasis įgaliotinis ir valstybės narės įsitrauks į politikos dialogą su tarptautiniais partneriais ir tokiomis tarptautinėmis organizacijomis, kaip Europos Taryba, EBPO, ESBO, NATO ir JT.

3.2. ES parama didelio kibernetinio incidento ar išpuolio atveju

Dideli kibernetiniai incidentai ar išpuoliai gali paveikti ES vyriausybes, bendroves ir individus. Įgyvendinus šią strategiją ir ypač pasiūlytąją direktyvą dėl tinklų ir informacijos saugumo, turėtų pagerėti kibernetinių incidentų prevencija, aptikimas ir reagavimas į juos, o

[31] Per atstovus ES kovos su elektroniniais nusikaltimais darbo grupėje, kuri sudaryta iš valstybių narių ES kovos su elektroniniais nusikaltimais skyrių vadovų.

valstybės narės ir Komisija turėtų vienos kitas išsamiau informuoti apie didžiausius kibernetinius incidentus ar išpuolius. Tačiau reagavimo mechanizmai skirsis pagal incidento pobūdį, mastą ir tarpvalstybinį poveikį.

Tinklų ir informacijos saugumo direktyvoje siūloma atsižvelgiant į tarpvalstybinį incidento pobūdį pradėti vykdyti nacionalinius arba Sąjungos tinklų ir informacijos saugumo planus, jei incidentas daro didelį poveikį tolesniam funkcijų vykdymui. Tokiomis aplinkybėmis keičiantis informacija būtų pasinaudota institucijų, kompetentingų tinklų ir informacijos saugumo srityje, tinklu. Tai padėtų išsaugoti paveiktų tinklų ir paslaugų veikimą arba juos atnaujinti.

Jei atrodo, kad incidentas atrodo susijęs su nusikaltimu, turėtų būti informuotas Europolo EC3, kad kartu su paveiktų valstybių teisėsaugos institucijomis galėtų pradėti tyrimą, išsaugoti įrodymus, nustatyti vykdytojus ir galiausiai užtikrinti, kad pastarieji būtų patraukti baudžiamojon atsakomybėn.

Jei atrodo, kad incidentas atrodo susijęs su kibernetiniu šnipinėjimu ar valstybės remiamu išpuoliu arba daro poveikį nacionaliniam saugumui, nacionalinio saugumo ir gynybos institucijos gali informuoti kolegas kitose valstybėse, kad ir jie žinotų galį tapti išpuolio taikiniu ir galėtų apsiginti. Tada būtų pritaikyti išankstinio perspėjimo mechanizmai, o prireikus – krizės valdymo ar kitos procedūros. Ypač grėsmingi kibernetiniai incidentai ar išpuoliai valstybei narei galėtų būti pakankamu pagrindu pasinaudoti ES solidarumo sąlyga (Sutarties dėl Europos Sąjungos veikimo 222 straipsnis).

Jei atrodo, kad incidento metu atskleisti asmens duomenys, turi įsitraukti nacionalinės duomenų apsaugos institucijos arba nacionalinė reguliavimo institucija pagal Direktyvą 2002/58/EB.

Be to, reaguojant į kibernetinius incidentus ir išpuolius, bus naudingi asmenų ryšiams tinklai ir tarptautinių partnerių parama. Tai galėtų būti ir techninės poveikio mažinimo priemonės, baudžiamasis tyrimas arba atsakomieji krizės valdymo mechanizmai.

4. IŠVADA IR TOLESNI VEIKSMAI

Šioje Komisijos ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai siūlomoje Europos Sąjungos kibernetinio saugumo strategijoje išdėstoma ES vizija ir būtini veiksmai orientuojantis į tvirtą apsaugą ir paramą piliečių teisėms, kad ES internetinė aplinka taptų saugiausia pasaulyje.[32]

[32] Strategija bus finansuojama ne didesnėmis lėšomis, nei numatyta kiekvienai iš atitinkamų politikos krypčių (Europos infrastruktūros tinklų priemonė, „Horizontas 2020“, Vidaus saugumo fondas, bendra užsienio ir saugumo politika bei išorinis bendradarbiavimas, konkrečiai stabilumo priemonė) Komisijos pasiūlyme dėl 2014–2020 m. daugiametės finansinės programos (jeigu ją patvirtins biudžeto valdymo institucija ir jei tai atitiks patvirtintos 2014–2020 m. daugiametės finansinės programos galutines sumas). Atsižvelgiant į poreikį užtikrinti bendrą derėjimą su decentralizuotoms agentūroms leidžiamu etatų skaičiumi ir decentralizuotoms agentūroms skirta tarpine viršutine riba kiekvienoje būsimos daugiametės finansinės programos išlaidų kategorijoje, agentūros, kurių Komisija prašo prisiimti naujas užduotis (CEPOL, Europos gynybos agentūra, ENISA, Eurojustas ir Europolo EC3), bus raginamos tai

Ši vizija gali būti įgyvendinta tik daugeliui subjektų laikantis tikros partnerystės principų, prisiimant atsakomybę ir pasitinkant laukiančius iššūkius.

Todėl Komisija ir Vyriausiasis įgaliotinis kviečia Tarybą ir Europos Parlamentą pritarti strategijai ir padėti įgyvendinti išvardytuosius veiksmus. Tvirtos paramos ir įsipareigojimo reikia ir iš privačiojo sektoriaus bei pilietinės visuomenės, kurie yra labai svarbūs norint padidinti saugumo lygį ir užtikrinti piliečių teises.

Veikti reikia dabar. Komisija ir Vyriausiasis įgaliotinis yra pasiryžę dirbti drauge su visais proceso dalyviais, kad būtų pasiektas Europai reikalingas saugumas. Siekdami užtikrinti spartų strategijos įgyvendinimą ir įvertinimą pagal galimus pokyčius, jie po 12 mėnesių sukvies visas suinteresuotąsias šalis į aukšto lygio konferenciją ir įvertins pažangą.

daryti tiek, kiek agentūra turi faktinių pajėgumų priimti augančius išteklius ir kiek iš viso nustatyta galimybių perskirstyti užduotis.