EUROPOS
KOMISIJA

SĄJUNGOS VYRIAUSIASIS
ĮGALIOTINIS UŽSIENIO
REIKALAMS IR
SAUGUMO POLITIKAI

Briuselis, 2017 09 13
JOIN(2017) 450 final

BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI

Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas

1. ĮVADAS

Kibernetinis saugumas labai svarbus tiek mūsų gerovei, tiek saugumui. Kasdienis mūsų gyvenimas ir ekonomika vis labiau priklauso nuo skaitmeninių technologijų, todėl mums kyla vis daugiau pavojų. Kibernetinio saugumo incidentų iniciatoriai ir jų tikslai įvairėja. Piktavališka kibernetinė veikla kelia grėsmę ne tik mūsų šalių ekonomikai ir bendrosios skaitmeninės rinkos kūrimui, bet ir pačiam mūsų demokratijos, laisvių ir vertybių sistemų veikimui. Kad ateityje būtume saugūs, turime iš esmės pakeisti savo gebėjimą saugoti ES nuo kibernetinių grėsmių – tiek civilinė infrastruktūra, tiek karinis pajėgumas priklauso nuo saugių skaitmeninių sistemų. Tai pripažinta ir 2017 m. birželio mėn. Europos Vadovų Tarybos susitikime[1], ir Visuotinėje Europos Sąjungos užsienio ir saugumo politikos strategijoje[2].

Rizika sparčiai didėja. Tyrimai rodo, kad ekonominis kibernetinių nusikaltimų poveikis nuo 2013 m. iki 2017 m. išaugo penkis kartus, o iki 2019 m. gali padidėti dar keturgubai[3]. Ypač padaugėjo išpuolių naudojant išpirkos reikalaujančią programinę įrangą[4] – naujausi jų[5] rodo didžiulį kibernetinės nusikalstamos veiklos suaktyvėjimą. Tačiau išpirkos reikalaujanti programinė įranga – toli gražu ne vienintelė grėsmė.

Kibernetines grėsmes sukelia ir nevalstybiniai, ir valstybiniai subjektai. Dažnai tai daroma nusikalstamais tikslais (norint pasipelnyti), tačiau motyvai gali būti ir politiniai bei strateginiai. Nusikalstamumo grėsmę didina tai, kad nyksta kibernetinius ir tradicinius nusikaltimus skirianti riba, nes nusikaltėliai naudojasi internetu ir kaip priemone savo veiklai plėsti, ir kaip informacijos apie naujus nusikaltimo metodus ir priemones šaltiniu[6]. Tačiau didžiąja dauguma atvejų galimybė susekti nusikaltėlį yra labai nedidelė, o patraukti jį baudžiamojon atsakomybėn – dar mažesnė.

Tuo pat metu valstybiniai subjektai savo geopolitiniams tikslams įgyvendinti vis dažniau naudoja ne tik tradicines priemones, kaip antai, karinę jėgą, bet ir diskretiškesnes kibernetines priemones, kuriomis, pavyzdžiui, kišamasi į vidaus demokratinius procesus. Šiuo metu plačiai pripažįstama, kad kibernetinė erdvė naudojama kaip atskira arba kaip viena iš kelių karo priemonių. Dezinformacijos kampanijos, melagingos žinios ir į ypatingos svarbos infrastruktūros objektus nukreiptos kibernetinės operacijos tampa vis dažnesnės ir į jas būtina reaguoti. Dėl šios priežasties Komisija savo parengtame diskusijoms skirtame dokumente dėl Europos gynybos ateities[7] pabrėžė, kad svarbu bendradarbiauti kibernetinės gynybos srityje.

Jei gerokai nepadidinsime savo kibernetinio saugumo, rizika, vykstant skaitmeninei pertvarkai, didės. Numatoma, kad 2020 m. prie interneto bus prijungta dešimtys milijardų daiktų interneto įrenginių, tačiau juos projektuojant kibernetiniam saugumui vis dar nėra teikiama pirmenybė[8]. Jei nebus užtikrinta įrenginių, kurie valdys mūsų elektros tinklus,

---

1 http://www.consilium.europa.eu/lt/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Žr., pavyzdžiui, „McAfee“ ir Strateginių ir tarptautinių tyrimų centro ataskaitą „Net losses: Estimating the Global Cost of Cybercrime“, 2014.

4 Išpirkos reikalaujanti programinė įranga – kenkimo programinė įranga, dėl kurios naudotojai visiškai arba iš dalies nebegali naudotis savo sistema, nes jos ekranas arba naudotojų rinkmenos užrakinami iki tol, kol bus sumokėta išpirka.

5 Nuo 2017 m. gegužės mėn. išpuolio „WannaCry“, įvykdyto naudojant išpirkos reikalaujančią programinę įrangą, nukentėjo per 400 000 kompiuterių daugiau kaip 150-yje šalių. Po mėnesio tokio paties pobūdžio išpuolį „Petya“ patyrė Ukraina ir kelios bendrovės visame pasaulyje.

6 Europolo atliktas sunkių formų ir organizuoto nusikalstamumo grėsmių vertinimas (2017).

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_lt.pdf.

8 Komisijos užsakymu bendrovių IDC ir „TXT Solutions“ atliktas tyrimas SMART 2013/0037 „Cloud and IoT combination“ (2014).

automobilius ir transporto tinklus, gamyklas, finansus, ligonines ir namus, apsauga, tai gali turėti pražūtingų padarinių ir smarkiai smogti vartotojų pasitikėjimui besiformuojančiomis technologijomis. Šią riziką dar didina politinių išpuolių prieš civilinius taikinius pavojus ir tai, kad karinė kibernetinė gynyba gali turėti trūkumų.

Šiame bendrame komunikate išdėstytas metodas pagerins ES galimybes kovoti su šiomis grėsmėmis. Šis metodas padėtų stiprinti atsparumą ir strateginę autonomiją, didinti technologinį pajėgumą, gerinti gebėjimus ir kurti stiprią bendrąją rinką. Tam reikalingos tinkamos struktūros, kurios padėtų užtikrinti didelį kibernetinį saugumą ir prireikus reaguoti, ir visapusiškas visų pagrindinių subjektų dalyvavimas. Šis metodas taip pat padėtų labiau atgrasyti nuo kibernetinių išpuolių, nes pagal jį būtų dedama daugiau pastangų nustatyti, susekti ir patraukti atsakomybėn jų vykdytojus. Juo būtų atsižvelgta ir į pasaulinį aspektą – siekiant padėti pagrindą ES pirmavimui kibernetinio saugumo srityje būtų plėtojamas tarptautinis bendradarbiavimas. Šie veiksmai nustatyti remiantis principais, išdėstytais bendrosios skaitmeninės rinkos strategijoje, Visuotinėje ES strategijoje, Europos saugumo darbotvarkėje[9], Bendroje kovos su hibridinėmis grėsmėmis sistemoje[10] ir komunikate „Pradeda veikti Europos gynybos fondas“[11, 12].

ES jau sprendžia daugelį šių klausimų – dabar metas sujungti įvairius darbo barus. 2013 m. ES parengė kibernetinio saugumo strategiją, pagal kurią imtasi veiksmų keliose pagrindinėse srityse, siekiant sustiprinti kibernetinį atsparumą[13]. Pagrindiniai šios strategijos tikslai ir principai – skatinti kurti patikimą, saugią ir atvirą kibernetinę ekosistemą – tebegalioja. Tačiau grėsmėms nuolat kintant ir didėjant būtina imtis daugiau veiksmų, kad būtų galima atremti būsimus išpuolius ir nuo jų atgrasyti[14].

ES, atsižvelgiant į jos įvairių sričių politikos aprėptį ir turimas priemones, struktūras ir pajėgumus, yra pajėgi spręsti kibernetinio saugumo klausimus. Valstybės narės ir toliau atsako už nacionalinį saugumą, tačiau šios grėsmės mastas ir tarpvalstybinis pobūdis yra svarus argumentas imtis ES lygmens veiksmų, kuriais valstybėms narėms būtų teikiamos paskatos ir parama, kad jos didintų, gerintų ir išlaikytų savo pajėgumą užtikrinti nacionalinį kibernetinį saugumą, kartu stiprindamos ES lygmens pajėgumą. Siūlomu metodu siekiama paskatinti visus subjektus – ES, valstybes nares, pramonės atstovus ir privačius asmenis – teikti kibernetiniam saugumui pirmenybę, būtiną siekiant stiprinti atsparumą kibernetiniams išpuoliams ir užtikrinti geresnį ES reagavimą. Juo nustatomi konkretūs veiksmai, kurie padės nustatyti ir tirti bet kokio pobūdžio kibernetinius išpuolius prieš ES ir jos valstybes nares ir tinkamai į juos reaguoti, be kita ko, patraukti nusikaltėlius baudžiamojon atsakomybėn. Šis metodas suteiks galimybę ES išorės veiksmų vykdytojams veiksmingai propaguoti kibernetinį saugumą pasaulinėje arenoje. Taip, užuot vien reagavusi į susidariusias aplinkybes, ES taps iniciatyvia Europos gerovės, visuomenės, vertybių, pagrindinių teisių ir laisvių saugotoja, nes bus pasirengusi reaguoti tiek į esamas, tiek į būsimas grėsmes.

---

[9] COM(2015) 185 *final*.

[10] JOINT(2016) 18 *final*.

[11] COM(2017) 295.

[12] Šis metodas taip pat pagrįstas nepriklausomomis mokslinėmis konsultacijomis, kurias suteikė Europos Komisijos mokslinių konsultacijų mechanizmo mokslinių konsultantų aukšto lygio darbo grupė (žr. tolesnes nuorodas).

[13] JOINT(2013) 1 *final*. Šios strategijos vertinimas pateikiamas dokumente SWD (2017) 295.

[14] Jei nenurodyta kitaip, šiame komunikate pateikiami pasiūlymai nedaro poveikio biudžetui. Poveikį biudžetui darančios iniciatyvos bus teikiamos deramai laikantis metinio biudžeto procedūrų ir negalės daryti įtakos sprendimams dėl būsimos daugiametės finansinės programos po 2020 m.

2. ES ATSPARUMO KIBERNETINIAMS IŠPUOLIAMS STIPRINIMAS

Siekiant sustiprinti kibernetinį atsparumą būtina laikytis bendro ir plataus požiūrio. Todėl reikia sukurti tvirtesnes ir veiksmingesnes struktūras, kurių paskirtis – propaguoti kibernetinį saugumą ir reaguoti į kibernetinius išpuolius ne tik valstybėse narėse, bet ir pačios ES institucijose, agentūrose ir įstaigose. Be to, būtina taikyti įvairiapusiškesnį kelias politikos sritis apimantį kibernetinio atsparumo ir strateginės autonomijos stiprinimo metodą, be kita ko, kurti stiprią bendrąją rinką, daryti svarbius žingsnius į priekį ES technologinio pajėgumo srityje ir gerokai padidinti kvalifikuotų specialistų skaičių. Svarbiausia – plačiau pripažinti, kad kibernetinis saugumas yra bendras visuomenės uždavinys, kurį turėtų spręsti įvairių lygmenų valdžios, ekonomikos ir visuomenės atstovai.

2.1. Europos Sąjungos tinklų ir informacijos apsaugos agentūros stiprinimas

Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA) turi atlikti labai svarbų vaidmenį stiprinant ES kibernetinį atsparumą ir gerinant reagavimą, tačiau ją varžo dabartiniai įgaliojimai. Todėl Komisija siūlo atlikti plataus užmojo pertvarką, be kita ko, **suteikti šiai agentūrai nuolatinį įgaliojimą**[15]. Taip bus užtikrinta, kad ENISA galėtų teikti valstybėms narėms, ES institucijoms ir įmonėms paramą pagrindinėse srityse, įskaitant Tinklų ir informacinių sistemų saugumo direktyvos[16] (toliau – TIS direktyva) ir siūlomos kibernetinio saugumo sertifikavimo sistemos įgyvendinimą.

Pertvarkyta ENISA bus svarbi patarėja politikos formavimo ir įgyvendinimo klausimais, be kita ko, skatins sektorių iniciatyvų ir TIS direktyvos suderinamumą ir padės kurti keitimosi informacija ir jos analizės centrus ypatingos svarbos sektoriuose. ENISA pakels kartelę ir stiprins Europos pasirengimą rengdama kasmetines visos Europos kibernetinio saugumo srities pratybas, per kurias bus skirtingais lygmenimis reaguojama į situaciją. Ji taip pat padės formuoti informacinių ir ryšių technologijų (IRT) kibernetinio saugumo sertifikavimo politiką ir atliks svarbų vaidmenį stiprinant tiek operatyvinį bendradarbiavimą, tiek krizių valdymą visoje ES. Agentūra taip pat atliks ryšių centro, kuriame kaupiama kibernetinio saugumo bendruomenei aktuali informacija ir žinios, funkcijas.

Kad būtų galima nuspręsti, ar reikia imtis ES remiamų jungtinių poveikio mažinimo ar reagavimo veiksmų, būtina greitai ir vienodai suprasti kylančias grėsmes ir vykstančius incidentus. Siekiant užtikrinti tokį keitimąsi informacija, būtinas visų atitinkamų subjektų – ES įstaigų bei agentūrų ir valstybių narių – dalyvavimas techniniu, operatyviniu ir strateginiu lygmenimis. Bendradarbiaudama su atitinkamomis valstybių narių ir ES įstaigomis, visų pirma reagavimo į kompiuterių saugumo incidentus tarnybų tinklu[17], CERT-EU, Europolu ir ES žvalgybos analizės centru (INTCEN), ES lygmens informuotumą apie padėtį padės užtikrinti ir ENISA. Šia informacija galės būti remiamasi žvalgybinių duomenų apie grėsmes rinkimo ir politikos formavimo veikloje, kuria siekiama nuolat stebėti grėsmes ir užtikrinti veiksmingą operatyvinį bendradarbiavimą, taip pat reaguojant į didelio masto tarpvalstybinius incidentus.

---

[15] COM(2017) 477.

[16] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

[17] Kaip numatyta TIS direktyvos 9 straipsnyje.

2.2. Bendrosios kibernetinio saugumo rinkos kūrimas

Kibernetinio saugumo produktų, paslaugų ir procesų rinkos augimą ES stabdo keletas veiksnių. Vienas pagrindinių trukdžių – tai, kad nėra visoje ES pripažįstamų kibernetinio saugumo sertifikavimo schemų, būtinų, kad kuriant produktus būtų laikomasi aukštesnių atsparumo standartų ir kad visoje ES sustiprėtų pasitikėjimas šia rinka. Todėl Komisija siūlo nustatyti **ES kibernetinio saugumo sertifikavimo sistemą**[18]. Šioje sistemoje būtų nustatyta tvarka, kurios reikėtų laikytis kuriant visoje ES taikomas kibernetinio saugumo produktų, paslaugų ir (arba) sistemų sertifikavimo schemas, pagal kurias patikinimo dėl sertifikuojamų objektų saugumo lygis priklausytų nuo jų paskirties (pavyzdžiui, atsižvelgiant į tai, ar tai ypatingos svarbos infrastruktūros objektai, ar vartotojų prietaisai)[19]. Tai duotų akivaizdžios naudos tarpvalstybinę prekybą vykdančioms įmonėms, nes joms nebereikėtų to paties produkto sertifikuoti kelis kartus ir dėl to sumažėtų jų administracinės ir finansinės išlaidos. Pagal šią sistemą sukurtų schemų taikymas taip pat padėtų stiprinti vartotojų pasitikėjimą, nes atitikties sertifikatu pirkėjai ir naudotojai būtų informuojami ir patikinami, kad jų perkami ir naudojami produktai ir paslaugos pasižymi konkrečiomis saugumo savybėmis. Taip atitiktis aukštiems kibernetinio saugumo standartams taptų konkurenciniu pranašumu. Dėl to sustiprėtų kibernetinis atsparumas, nes IRT produktai ir paslaugos būtų oficialiai vertinami pagal nustatytus kibernetinio saugumo standartus, kurie galėtų būti parengti atidžiai sekant IRT standartų srityje vykdomą bendresnio pobūdžio veiklą[20].

Sertifikavimas pagal tokias schemas būtų savanoriškas, ir jomis pardavėjams ar paslaugų teikėjams nebūtų nustatyti jokie iš karto vykdytini reglamentavimo įpareigojimai. Schemos neprieštarautų jokiems taikomiems teisiniams reikalavimams, pavyzdžiui, ES teisės aktams dėl duomenų apsaugos.

Kai sistema bus nustatyta, Komisija paragins atitinkamus suinteresuotuosius subjektus sutelkti dėmesį į tris prioritetines sritis:

- saugumą ypatingos svarbos ar didelės rizikos srityse[21]. Sistemos, nuo kurių esame priklausomi savo kasdienėje veikloje, pradedant automobiliais ir baigiant gamyklų mašinomis, pradedant didžiausiomis sistemomis, tokiomis kaip lėktuvai ar elektrinės, ir baigiant mažiausiomis sistemomis, tokiomis kaip medicinos prietaisai, vis labiau skaitmenėja ir yra vis labiau vienos su kitomis susiejamos. Todėl pagrindinių tokius produktus ir sistemas sudarančių IRT komponentų saugumą reikėtų vertinti nuodugniai;
- skaitmeninių produktų, tinklų, sistemų ir paslaugų (pavyzdžiui, e. laiškų šifravimo, užkardų (ugniasienių) ir virtualiųjų privačiųjų tinklų), ir privačiajame, ir viešajame sektoriuose plačiai naudojamų siekiant gintis nuo išpuolių ir vykdyti reglamentavimo įpareigojimus[22], kibernetinį saugumą. Labai svarbu, kad dėl vis platesnio tokių priemonių naudojimo nekiltų naujų pavojų ar naujų pažeidžiamumo problemų;

---

[18] COM(2017) 477.

[19] Patikinimo lygis rodo saugumo vertinimo nuodugnumo laipsnį ir paprastai atitinka su objektų taikymo sritimis ar funkcijomis susijusį rizikos lygį (t. y. vertinant IRT produktus ar paslaugas, su kurių taikymo sritimis ar funkcijomis susijusi rizika yra didelė, būtinas aukštesnio lygio patikinimas).

[20] COM(2016) 176.

[21] Išimtis būtų atvejai, kuriais privalomasis ar savanoriškas sertifikavimas reglamentuojamas kitais Sąjungos aktais.

[22] Pavyzdžiui, Direktyvoje (ES) 2016/1148, Reglamente (ES) 2016/679, Direktyvoje (ES) 2015/2366 ir kituose siūlomuose teisės aktuose, kaip antai Europos elektroninių ryšių kodekse, reikalaujama, kad organizacijos taikytų tinkamas saugumo priemones, kuriomis būtų valdomi atitinkami kibernetiniam saugumui kylantys pavojai.

- metodų, kuriais nebrangių skaitmeninių masinio vartojimo įrenginių, susietų tarpusavyje ir sudarančių daiktų internetą, saugumas užtikrinamas juos projektuojant, taikymą. Pagal sistemą sukurtomis schemomis galėtų būti naudojamasi siekiant parodyti, kad atitinkami produktai yra suprojektuoti taikant naujausius saugaus kūrimo metodus, kad jų saugumas tinkamai išbandytas ir kad jų pardavėjai yra įsipareigoję atnaujinti savo programinę įrangą, jei būtų nustatyta naujų pažeidžiamumo problemų ar grėsmių.

Nustatant šiuos prioritetus visų pirma reikėtų atsižvelgti į grėsmių kibernetiniam saugumui kitimą ir į esminių paslaugų, pavyzdžiui, transporto, energetikos, sveikatos priežiūros, bankininkystės, finansų rinkos infrastruktūros, geriamojo vandens ar skaitmeninės infrastruktūros[23], svarbą.

Nors jokie IRT produktai, sistemos ar paslaugos negali būti visiškai saugūs, yra keletas gerai žinomų ir išsamiai aprašytų IRT produktų projektavimo trūkumų, kuriais gali būti pasinaudojama per išpuolius. Jei susietųjų įrenginių ir IT programinės bei aparatinės įrangos gamintojai imtų taikyti saugumo užtikrinimo projektuojant principą, kibernetinio saugumo klausimas būtų sprendžiamas prieš pateikiant naujus produktus rinkai. Tai galėtų sudaryti dalį rūpestingumo pareigos principo, kurį reikėtų išplėtoti kartu su pramonės atstovais ir kurio laikantis produktų ir (arba) programinės įrangos pažeidžiamumas galėtų būti mažinamas taikant įvairius metodus, pradedant saugiu projektavimu ir baigiant bandymais bei tikrinimu, įskaitant, jei taikytina, oficialų tikrinimą, ilgalaike technine priežiūra, saugių kūrimo ciklo procesų taikymu ir naujinių bei pataisų kūrimu siekiant spręsti anksčiau nenustatytas pažeidžiamumo problemas ir greitai atnaujinti ir pataisyti produktą[24]. Tai taip pat padidintų vartotojų pasitikėjimą skaitmeniniais produktais.

Be to, reikia pripažinti, kad svarbus vaidmuo nustatant esamų produktų ir paslaugų pažeidžiamumo problemas tenka saugumo tyrimus atliekančioms trečiosioms šalims, todėl visose valstybėse narėse turėtų būti sudarytos sąlygos koordinuotam pažeidžiamumo problemų atskleidimui[25] remiantis geriausia praktika[26] ir atitinkamais standartais[27].

Kartu **konkrečiuose sektoriuose** susiduriama su savitomis problemomis, todėl jų atstovai turėtų būti skatinami kurti savo metodus. Taip bendrosios kibernetinio saugumo strategijos būtų papildomos konkrečių sektorių, pavyzdžiui, finansinių paslaugų[28], energetikos, transporto ir sveikatos priežiūros[29], kibernetinio saugumo strategijomis.

---

[23] Sektoriai, kuriems taikoma 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

[24] Mokslinių konsultantų aukšto lygio darbo grupė. „Cybersecurity in the European Digital Single Market“, 2017 m. kovo mėn.

[25] Koordinuotas pažeidžiamumo problemų atskleidimas – tam tikro pobūdžio bendradarbiavimas, kuriuo saugumo tyrimus atliekantiems asmenims sudaromos palankesnės sąlygos ir suteikiama galimybė pranešti apie pažeidžiamumo problemas informacinės sistemos savininkui arba pardavėjui, kad šis galėtų tinkamai ir laiku nustatyti bei išspręsti pažeidžiamumo problemą, kol išsami informacija apie tai nepasiekė trečiųjų šalių ar visuomenės.

[26] Pavyzdžiui, agentūros ENISA parengtu pažeidžiamumo problemų atskleidimo gerosios praktikos vadovu „From challenges to recommendations“ (2016).

[27] ISO/IEC 29147:2014 „Informacinės technologijos. Saugumo metodai. Pažeidžiamumo problemų atskleidimas“.

[28] Būsimas su finansinėmis technologijomis susijęs Komisijos darbas apims ir finansų sektoriaus kibernetinio saugumo klausimą.

[29] Energetikos sektoriuje, pavyzdžiui, svarbus klausimas, kaip suderinti labai senas ir pačias naujausias informacines technologijas, visų pirma atsižvelgiant į tikralaikius elektros tinklo reikalavimus.

Komisija jau atkreipė dėmesį į konkrečius naujų skaitmeninių technologijų keliamus klausimus dėl **atsakomybės**[30]. Šiuo metu atliekama poveikio analizė, o kiti veiksmai bus užbaigti iki 2018 m. birželio mėn. Kibernetinio saugumo srityje kyla klausimų, susijusių su įmonių ir tiekimo grandinių atsakomybės už žalą nustatymu. Neišspręsti šie klausimai trukdys kurti stiprią bendrąją kibernetinio saugumo produktų ir paslaugų rinką.

Galiausiai ES bendrosios rinkos plėtra priklauso ir nuo to, ar kibernetinio saugumo aspektas bus įtrauktas į prekybos ir investicijų politiką. Užsienio investuotojų vykdomų įsigijimų poveikis ypatingos svarbos technologijoms, kurių svarbus pavyzdys yra kibernetinio saugumo technologijos, yra vienas iš aspektų, kuriems skiriama daugiausia dėmesio **tiesioginių užsienio investicijų Europos Sąjungoje atrankos sistemoje**[31], kuria siekiama sudaryti sąlygas atlikti trečiųjų šalių investicijų atranką saugumo ir viešosios tvarkos atžvilgiais. Be to, keliose trečiosiose valstybėse dėl kibernetinio saugumo reikalavimų jau yra kilę kliūčių prekybai ES prekėmis ir paslaugomis svarbiuose sektoriuose. ES kibernetinio saugumo sertifikavimo sistema padės toliau stiprinti Europos poziciją tarptautinėje arenoje. Kartu turėtų būti toliau dedamos pastangos nustatyti aukštus pasaulinius saugumo standartus ir sudaryti tarpusavio pripažinimo susitarimus.

2.3. Visapusiškas Tinklų ir informacinių sistemų saugumo direktyvos įgyvendinimas

Atsižvelgdama į tai, kad kibernetinis saugumas šiuo metu iš esmės yra valstybių narių rankose, ES pripažįsta, kad būtina nustatyti aukštesnius standartus. Pagrindiniai sektoriai, pavyzdžiui, bankininkystės, energetikos arba transporto, darosi vis globalesni, labiau priklausomi nuo skaitmeninių technologijų ir susieti, todėl didelio masto kibernetinio saugumo incidentai retai paveikia tik vieną valstybę narę.

Tinklų ir informacinių sistemų saugumo direktyva (toliau – TIS direktyva) – pirmasis ES masto teisės aktas dėl kibernetinio saugumo[32]. Ja siekiama stiprinti atsparumą didinant valstybių narių pajėgumą užtikrinti kibernetinį saugumą, skatinant geresnį valstybių narių bendradarbiavimą ir nustatant svarbių ekonomikos sektorių įmonėms reikalavimą taikyti veiksmingus rizikos valdymo metodus ir pranešti apie pavojingus incidentus nacionalinėms valdžios institucijoms. Šie įpareigojimai taikomi ir trijų rūšių pagrindinių interneto paslaugų – debesijos kompiuterijos, paieškos sistemų ir elektroninių prekyviečių – teikėjams. Direktyva siekiama užtikrinti, kad būtų laikomasi tvirtesnio ir sistemingesnio požiūrio ir kad būtų geriau keičiamasi informacija.

ES kibernetiniam atsparumui labai svarbu, kad visos valstybės narės visapusiškai įgyvendintų šią direktyvą iki 2018 m. gegužės mėn. Valstybės narės deda bendras pastangas paremti šį procesą – iki 2017 m. rudens pabaigos jos parengs gaires, padėsiančias įgyvendinti direktyvą laikantis suderintų principų, visų pirma susijusių su esminių paslaugų operatoriais. Komisija šiame kibernetinio saugumo dokumentų rinkinyje taip pat pateikia komunikatą[33], kuriuo siekiama paremti jų pastangas pristatant geriausią su direktyvos įgyvendinimu susijusią valstybių narių patirtį ir pateikiant rekomendacijų dėl praktinio direktyvos taikymo.

Direktyva turės būti papildyta keitimosi informacija nuostatomis. Pavyzdžiui, ši direktyva taikoma tik pagrindiniams strateginiams sektoriams, tačiau panašų metodą logiškai turės taikyti visi kibernetinių išpuolių patiriantys suinteresuotieji subjektai, kad būtų galima

[30] COM(2017) 228.
[31] COM(2017) 478.
[32] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.
[33] COM(2017) 476.

sistemingai nustatyti pažeidžiamumo problemas ir galimas kibernetinių užpuolikų įsilaužimo vietas. Be to, esama tam tikrų kliūčių viešajam ir privačiajam sektoriams bendradarbiauti ir keistis informacija. Valdžios ir viešosios institucijos nenoriai keičiasi su kibernetiniu saugumu susijusia informacija, nes bijo statyti į pavojų nacionalinį saugumą ar konkurencingumą. Privačiosios įmonės nenori keistis informacija apie savo kibernetinio saugumo problemas ir susijusius nuostolius, nes bijo atskleisti neskelbtiną verslo informaciją, rizikuoti savo reputacija ar pažeisti duomenų apsaugos taisykles[34]. Kad viešojo ir privačiojo sektorių partnerystės organizacijos prisidėtų prie platesnio bendradarbiavimo ir keitimosi informacija įvairesniuose sektoriuose, būtinas didesnis pasitikėjimas. Užtikrinant pasitikėjimą, būtiną, kad privatusis ir viešasis sektoriai keistųsi informacija, itin svarbus keitimosi informacija ir jos analizės centrų vaidmuo. Tam tikruose ypatingos svarbos sektoriuose jau žengti pirmieji žingsniai – aviacijos sektoriuje sukurtas Europos aviacijos kibernetinio saugumo centras[35], o energetikos sektoriuje – keitimosi informacija ir jos analizės centrai[36]. Padedama agentūros ENISA, Komisija visapusiškai prisidės prie šio metodo įgyvendinimo, kiek būtina, spartindama šį procesą – ypač TIS direktyvoje nustatytų esminių paslaugų sektoriuose.

2.4. Atsparumas užtikrinant greitą reagavimą į krizes

Vykstančio kibernetinio išpuolio poveikį galima sumažinti greitai ir veiksmingai reaguojant. Toks reagavimas parodytų ir tai, kad viešosios institucijos nėra bejėgės ir gali atremti kibernetinius išpuolius, ir padėtų didinti pasitikėjimą. Dėl pačių ES institucijų reagavimo pasakytina, kad pirmiausia reikėtų įtraukti kibernetinio saugumo aspektus į esamus ES krizių valdymo mechanizmus – Tarybai pirmininkaujančios valstybės narės koordinuojamą ES integruoto politinio atsako į krizes mechanizmą[37] ir ES bendrąsias ankstyvojo perspėjimo sistemas[38]. Būtinybė reaguoti į ypač pavojingą kibernetinį incidentą ar išpuolį galėtų būti pakankamas pagrindas valstybei narei pasinaudoti ES solidarumo sąlyga[39].

Kad būtų galima greitai ir veiksmingai reaguoti, taip pat būtinas mechanizmas, suteikiantis galimybę visiems pagrindiniams nacionalinio ir ES lygmenų subjektams greitai keistis informacija, o tam savo ruožtu būtina, kad šie subjektai aiškiai žinotų savo funkcijas ir pareigas. Komisija pasikonsultavo su institucijomis ir valstybėmis narėmis dėl veiksmingos operatyvinio reagavimo Sąjungos ir valstybių narių lygmenimis į didelio masto kibernetinį incidentą procedūros projekto. Į šį dokumentų rinkinį įeinančioje rekomendacijoje[40] pateiktame **projekte** aiškinama, kaip įtraukti kibernetinio saugumo aspektą į esamus ES lygmens krizių valdymo mechanizmus, ir nustatomi valstybių narių tarpusavio bendradarbiavimo ir jų bendradarbiavimo su atitinkamomis ES institucijomis, tarnybomis,

---

[34] Mokslinių konsultantų aukšto lygio darbo grupė. „Cybersecurity in the European Digital Single Market“, 2017 m. kovo mėn**.** Viena konkreti problema yra susijusi su prekybos paslaptimis. 2016 m. liepos mėn. komunikate „Europos kibernetinio atsparumo sistemos stiprinimas“ atkreiptas dėmesys į polinkį nutylėti kibernetines prekybos paslapčių vagystes ir į tai, kad svarbu sukurti patikimus pranešimo kanalus, kuriais būtų užtikrintas konfidencialumas.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Šie centrai – naryste grindžiamos ne pelno organizacijos, į kurias buriasi privatieji ir viešieji subjektai siekdami keistis informacija apie kibernetines grėsmes, riziką, prevenciją, poveikio mažinimą ir reagavimą. Žr., pavyzdžiui, informaciją apie Europos energetikos keitimosi informacija ir jos analizės centrus (http://www.ee-isac.eu).

[37] Tai suteikia galimybę aukščiausiu politiniu lygmeniu koordinuoti reagavimą į dideles tarpsektorines krizes.

[38] Šios sistemos sudaro sąlygas viduje keistis informacija apie bręstančias daug sektorių paveiksiančias krizes arba numatomas ar neišvengiamas grėsmes, dėl kurių reikia imtis ES lygmens veiksmų, ir suteikia galimybę koordinuoti susijusius veiksmus.

[39] Pagal Sutarties dėl Europos Sąjungos veikimo 222 straipsnį.

[40] C(2017) 6100.

agentūromis ir įstaigomis[41] reaguojant į didelio masto kibernetinio saugumo incidentus tikslai ir būdai. Kad projekte numatytą procedūrą būtų galima taikyti, rekomendacijoje taip pat reikalaujama, kad valstybės narės ir ES institucijos sukurtų ES reagavimo į kibernetinio saugumo krizes sistemą. Projekto koncepcija bus reguliariai išbandoma kibernetinių ir kitokių krizių valdymo pratybose[42] ir prireikus atnaujinama.

Atsižvelgiant į tai, kad kibernetinio saugumo incidentai gali suduoti didelį smūgį ekonomikos veikimui ir kasdieniam žmonių gyvenimui, būtų galima išnagrinėti galimybę, sekant kitose ES politikos srityse taikomų krizių valdymo mechanizmų pavyzdžiu, įsteigti **Reagavimo į kibernetinio saugumo krizes fondą**. Tai suteiktų valstybėms narėms galimybę vykstant ar jau įvykus dideliam incidentui prašyti ES lygmens pagalbos su sąlyga, kad prieš incidentą ta valstybė narė taikė gerai apgalvotą kibernetinio saugumo sistemą, be kita ko, buvo visapusiškai įgyvendinusi TIS direktyvą ir taikė brandžias nacionalinio lygmens rizikos valdymo ir priežiūros sistemas. Tokiame fonde, kuriuo būtų papildomi esami ES lygmens krizių valdymo mechanizmai, būtų galima solidarumo labui sutelkti greitojo reagavimo pajėgumus ir iš jo finansuoti konkrečius reagavimo į krizes veiksmus, pavyzdžiui, užvaldytos įrangos keitimą nauja įranga arba poveikio mažinimo ar reagavimo priemonių diegimą, vykdomus remiantis nacionalinių ekspertų žiniomis, kaip kad daroma taikant ES civilinės saugos mechanizmą.

2.5. Kibernetinio saugumo kompetencijos tinklas ir Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centras

Technologinės kibernetinio saugumo priemonės yra ir strateginis turtas, ir pagrindinės ateities augimo technologijos. ES yra strategiškai svarbu išlaikyti ir plėtoti pajėgumus, būtinus siekiant užtikrinti savo skaitmeninės ekonomikos, visuomenės ir demokratijos saugumą, apsaugoti ypatingos svarbos aparatinę ir programinę įrangą ir teikti pagrindines kibernetinio saugumo paslaugas.

2016 m. pradėta viešojo ir privačiojo sektorių partnerystė kibernetinio saugumo srityje[43] buvo svarbus pirmasis žingsnis, kuriuo iki 2020 m. bus pritraukta iki 1,8 mlrd. EUR investicijų. Tačiau kitose pasaulio dalyse[44] daromų investicijų mastas rodo, kad ES turi daugiau nuveikti investicijų srityje ir išspręsti pajėgumų išsibarstymo po visas valstybes nares problemą.

Atsižvelgiant į tai, kad kibernetinio saugumo technologijos sudėtingos, kad reikia didelių investicijų ir kad būtini sprendimai, kurie veiktų visoje Europos Sąjungoje, ES lygmens veiksmais būtų sukurta pridėtinė vertė. Remiantis valstybių narių ir viešojo bei privačiojo sektorių partnerystės įdirbiu, kitas žingsnis būtų stiprinti ES pajėgumą užtikrinti kibernetinį saugumą sukuriant **kibernetinio saugumo kompetencijos centrų tinklą**[45], kurio branduolys būtų **Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centras**. Šis tinklas ir Centras skatintų kurti ir diegti kibernetinio saugumo technologijas ir prisidėtų prie pastangų stiprinti šios srities pajėgumus ES ir nacionaliniu lygmenimis. Siekdama sukurti šią

---

[41] Įskaitant Europolą, ENISA, ES institucijų, įstaigų ir agentūrų Kompiuterinių incidentų tyrimo tarnybą (CERT-EU) ir ES žvalgybos analizės centrą (INTCEN).

[42] Pavyzdžiui, ENISA vykdomose pratybose – https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

[43] COM(2016) 4400 *final*.

[44] Vien 2017 m. JAV į kibernetinį saugumą investuos 19 mlrd. dolerių, t. y. 35 proc. daugiau nei 2016 m. Baltųjų rūmų atstovo spaudai biuro parengta informacijos suvestinė „Fact Sheet: Cybersecurity National Action Plan“, 2016 m. vasario 9 d.

[45] Tinklą sudarytų esami ir būsimi valstybėse narėse įsteigti kibernetinio saugumo centrai, kurių nariai paprastai būtų viešosios mokslinių tyrimų organizacijos ir laboratorijos.

struktūrą 2018 m., Komisija atliks poveikio vertinimą, kad išnagrinėtų įmanomas galimybes, be kita ko, galimybę įsteigti bendrąją įmonę.

Siekdama žengti pirmąjį žingsnį ir surinkti informacijos, kuria būtų galima remtis ateityje, Komisija pasiūlys pagal programą „Horizontas 2020“ pradėti bandomąjį etapą, kuris padėtų sujungti nacionalinius centrus į tinklą siekiant suteikti naują postūmį kibernetinio saugumo kompetencijos ugdymui ir kibernetinio saugumo technologijų plėtrai. Šiuo tikslu ji planuoja pasiūlyti trumpalaikį 50 mln. EUR finansavimą. Šia veikla bus papildytas tebevykstantis viešojo ir privačiojo sektorių partnerystės kibernetinio saugumo srityje įgyvendinimas.

Iš pradžių tinklas ir Centras daugiausia dėmesio skirtų mokslinių tyrimų išteklių telkimui ir formavimui. Kad būtų remiamas pramonės pajėgumų didinimas, Centras galėtų veikti kaip pajėgumų projektų valdytojas, gebantis administruoti daugiašalius projektus. Tai taip pat suteiktų papildomą postūmį inovacijoms ir paskatintų ES pramonės konkurencingumą pasaulyje tokiose srityse kaip naujos kartos skaitmeninių technologijų, įskaitant dirbtinį intelektą, kūrimas, kvantinė kompiuterija, blokų grandinės ir saugi skaitmeninė tapatybė, taip pat padėtų geriau užtikrinti ES įsikūrusių įmonių prieigą prie masinių duomenų, o visa tai labai svarbu kibernetiniam saugumui ateityje. Centras taip pat naudotųsi ES pastangų išplėsti itin našaus skaičiavimo infrastruktūrą rezultatais. Išplėsti šią infrastruktūrą labai svarbu siekiant analizuoti didelius duomenų kiekius, greitai šifruoti ir iššifruoti duomenis, tikrinti tapatybę, modeliuoti kibernetinius išpuolius ir analizuoti vaizdo medžiagą[46].

Kompetencijos centrų tinklas taip pat galėtų turėti pajėgumų teikti pramonės atstovams paramą atliekant bandymus ir modeliavimą, kurie padėtų atitikti 2.2 skirsnyje aprašyto kibernetinio saugumo sertifikavimo reikalavimus. Dalyvaudamas įvairioje ES kibernetinio saugumo veikloje, Centras galėtų nuolat atnaujinti savo veiklos kryptį atsižvelgdamas į poreikius. Centras siektų užtikrinti, kad aukšti kibernetinio saugumo standartai būtų taikomi ne tik technologijoms ir kibernetinio saugumo sistemoms, bet ir aukščiausios klasės profesinių gebėjimų ugdymui – tuo tikslu Centras siūlytų valstybėms narėms sprendimus ir modelius, aktualius stengiantis išplėtoti skaitmeninius gebėjimus. Šiuo atžvilgiu jis taip pat didintų ES lygmens kibernetinio saugumo pajėgumus ir remtųsi sąveika su, visų pirma, ENISA, CERT-EU, Europolu, galimu būsimu Reagavimo į kibernetinio saugumo krizes fondu ir nacionalinėmis CSIRT.

Ypatingas dėmesys kompetencijos tinklo veikloje turėtų būti skiriamas nepakankamam Europos pajėgumui vertinti produktų ir paslaugų, kuriais bendrojoje skaitmeninėje rinkoje naudojasi piliečiai, įmonės ir valdžios sektorius, **šifravimo** patikimumą. Patikimas šifravimas – saugių skaitmeninio tapatybės nustatymo sistemų, kurios atlieka labai svarbų vaidmenį veiksmingai užtikrinant kibernetinį saugumą[47], pagrindas; Jis taip pat padeda užtikrinti asmenų intelektinės nuosavybės saugumą, suteikia galimybę saugoti pagrindines teises, pavyzdžiui, užtikrinti žodžio laisvę ir asmens duomenų apsaugą, ir vykdyti saugią elektroninę prekybą[48].

ES civilinio ir gynybinio kibernetinio saugumo rinkas sieja bendri uždaviniai[49] ir dvejopos paskirties technologijos – tai skatina glaudžiai bendradarbiauti ypatingos svarbos srityse.

---

[46] COM(2012) 45 *final* ir COM(2016) 178 *final*.

[47] Komisija jau yra suplanavusi pagal programą „Horizontas 2020“ pakviesti kurti novatoriškus elektroninio tapatumo nustatymo metodus – už geriausią šio uždavinio sprendimą bus skirta 4 mln. EUR „Horizonto“ premija.

[48] Mokslinių konsultantų aukšto lygio darbo grupė. „Cybersecurity in the European Digital Single Market“, 2017 m. kovo mėn.

[49] Tyrimas „Synergies between the civilian and the defence cybersecurity markets“ („Optimity“, SMART 2014-0059).

Todėl antruoju etapu į tinklo ir Centro veiklą, visapusiškai laikantis Sutarties nuostatų dėl bendros saugumo ir gynybos politikos, galėtų būti įtrauktas ir kibernetinės gynybos aspektas. Gynybos srityje daugiausia dėmesio būtų skiriama technologijoms, tačiau taip pat būtų galima prisidėti prie valstybių narių bendradarbiavimo kibernetinės gynybos srityje, be kita ko, padėti joms keistis informacija, užtikrinti informuotumą apie padėtį, kaupti ekspertines žinias, koordinuoti reagavimo veiksmus ir plėtoti bendrus pajėgumus. Šioje srityje, Centrui atliekant pagalbinį ir patariamąjį vaidmenį, taip pat galėtų būti sudaromos sąlygos valstybėms narėms nustatyti ES kibernetinės gynybos prioritetus, nagrinėjamos galimybės taikyti bendrus sprendimus, padedama rengti bendras strategijas, sudaromos palankesnės sąlygos rengti ES lygmens jungtinius kibernetinės gynybos mokymus, pratybas ir bandymus, taip pat padedama rengti kibernetinės gynybos standartus ir taksonomijos sistemas. Kad galėtų vykdyti nurodytą veiklą, kibernetinės gynybos srityje Centras turėtų glaudžiai bendradarbiauti su Europos gynybos agentūra, o kibernetinio atsparumo srityje – su ENISA, ir jo veikla turėtų visapusiškai papildyti šių agentūrų veiklą. Ši gynybos srities veikla būtų vykdoma atsižvelgiant į diskusijoms skirtu dokumentu dėl Europos gynybos ateities pradėtą procesą.

Siekiant užtikrinti kibernetinei gynybai reikalingą aukšto lygio atsparumą, būtini tikslingi moksliniai tyrimai ir technologijų plėtra. Vykdydamos kibernetinės gynybos projektus ar kurdamos šios srities technologijas, įmonės galėtų naudotis Europos gynybos fondo finansavimu ir mokslinių tyrimų, ir plėtros etapais[50]. Šiame kontekste ypač svarbios galėtų būti tokios sritys kaip kvantinėmis technologijomis pagrįstos šifravimo sistemos, informuotumas apie kibernetinę padėtį, biometrinės prieigos kontrolės sistemos, aukšto lygmens ilgalaikių grėsmių nustatymas arba duomenų gavyba. Sąjungos vyriausioji įgaliotinė, Europos gynybos agentūra ir Komisija padės valstybėms narėms nustatyti sritis, kurių bendri kibernetinio saugumo projektai galėtų būti svarstomi kaip galimi finansuoti Europos gynybos fondo lėšomis.

2.6. Stiprios ES kibernetinių gebėjimų bazės kūrimas

Kibernetiniam saugumui labai svarbus švietimo aspektas. Veiksmingas kibernetinio saugumo užtikrinimas labai priklauso nuo atitinkamų asmenų gebėjimų. Tačiau prognozuojama, kad iki 2022 m. kvalifikuotų kibernetinio saugumo srities darbuotojų trūkumas Europos privačiajame sektoriuje pasieks 350 000[51]. Su kibernetiniu saugumu susijęs švietimas turėtų būti vykdomas visais lygmenimis, pradedant įprastu informatikos srities darbuotojų rengimu ir baigiant papildomu visiems IRT specialistams skirtu kibernetinio saugumo mokymu bei nauja specialia kibernetinio saugumo mokymo programa. Siekiant patenkinti spartesnio švietimo ir mokymo poreikius, turėtų būti įsteigti stiprūs akademiniai kompetencijos centrai, kurie galėtų vadovautis Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centro ir ENISA rekomendacijomis. Tikslas turėtų būti užtikrinti, kad taptų įprasta projektuojant IRT produktus ir sistemas nuo pat pradžių atsižvelgti į saugumo principus. Su kibernetiniu saugumu susijęs švietimas turėtų būti skirtas ne tik IT specialistams – jis turėtų būti integruotas ir į kitų sričių, pavyzdžiui, inžinerijos, verslo vadybos arba teisės, mokymo programas ir į konkrečių sektorių švietimo krypčių programas. Galiausiai per skaitmeninių įgūdžių lavinimo pamokas pradinio ir vidurinio mokymo įstaigose turėtų būti ugdomas mokytojų ir moksleivių dėmesingumas kibernetinių nusikaltimų ir kibernetinio saugumo klausimams.

[50] Kibernetinės gynybos projektams jau dabar bus suteikta pirmenybė Europos gynybos pramonės plėtros programoje. Kibernetinė gynyba bus ir viena iš 2018 m. paskelbsimų kvietimų teikti pasiūlymus temų.

[51] Tyrimas „Global Information Security Workforce Study 2017“. Visame pasaulyje trūksta 1,8 mln. kvalifikuotų darbuotojų.

ES kartu su valstybėmis narėmis turėtų prisidėti prie šio darbo naudodamosi Skaitmeninių įgūdžių ir užimtumo koalicijos[52] įdirbiu ir parengdamos, pavyzdžiui, MVĮ skirtas kibernetinio saugumo srities pameistrystės programas.

2.7. Kibernetinės higienos ugdymas ir informuotumo didinimas

Nurodoma, kad sąlygas 95 proc. incidentų įvykti sudaro kokia nors tyčinė arba netyčinė žmogaus klaida[53], taigi žmogaus veiksnys atlieka svarbų vaidmenį. Todėl kibernetinis saugumas yra mūsų visų atsakomybė. Tai reiškia, kad asmenų, įmonių ir viešojo administravimo institucijų elgsena turi pasikeisti taip, kad būtų užtikrinta, jog visi suprastų grėsmę ir turėtų priemonių bei įgūdžių, būtinų siekiant greitai nustatyti išpuolius ir aktyviai nuo jų saugotis. Žmonės turi išsiugdyti kibernetinės higienos įpročius, o įmonės ir organizacijos turi patvirtinti tinkamas rizikos vertinimu pagrįstas kibernetinio saugumo programas ir jas reguliariai atnaujinti, atsižvelgdamos į grėsmių pokyčius.

TIS direktyvoje valstybės narės įpareigojamos ne tik ES lygmeniu keistis informacija apie kibernetinius išpuolius, bet ir parengti brandžias nacionalines kibernetinio saugumo strategijas ir tinklų bei informacinių sistemų saugumo sistemas. Įgyvendinant šiuos veiksmus pagrindinį vaidmenį toliau turėtų atlikti ES ir nacionalinės viešojo administravimo institucijos.

Pirma, valstybės narės turi užtikrinti kuo geresnes įmonių ir privačių asmenų naudojimosi kibernetinio saugumo priemonėmis galimybes. Visų pirma reikėtų daugiau nuveikti kibernetinių nusikaltimų poveikio galutiniams vartotojams prevencijos ir mažinimo srityje. Jau dabar yra pavyzdys – Europolo vykdoma kampanija „NoMoreRansom“[54], parengta glaudžiai bendradarbiaujant teisėsaugos institucijoms ir kibernetinio saugumo bendrovėms, siekiant padėti naudotojams užkirsti kelią užkrėtimui išpirkos reikalaujančia programine įranga ir iššifruoti duomenis tais atvejais, kai jie tampa išpuolio aukomis. Turėtų būti parengtos ir kitose srityse taikytinos kovai su kitų rūšių kenkimo programine įranga skirtos programos, o ES turėtų sukurti **vieną bendrą portalą, kuriame pagal vieno langelio principą būtų sutelktos visos tokios priemonės** ir kuriame naudotojams būtų teikiami patarimai dėl užkrėtimo kenkimo programine įranga prevencijos bei nustatymo ir pateikiamos nuorodos į pranešimų teikimo mechanizmus.

Antra, valstybės narės turėtų užtikrinti, kad **plėtojant e. valdžią būtų** greičiau **pradėtos naudoti kibernetiniu požiūriu saugesnės priemonės**, ir visapusiškai pasinaudoti kompetencijos tinklo teikiamais pranašumais. Remiantis ES elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje sistema, kuri galioja nuo 2016 m. ir kuria užtikrinama nuspėjama reglamentavimo aplinka, kad elektroninis įmonių, piliečių ir viešųjų institucijų bendravimas vyktų saugiai ir sklandžiai[55], turėtų būti skatinama pradėti taikyti saugias tapatybės nustatymo priemones. Be to, viešosios institucijos, ypač tos, kurios teikia esmines paslaugas, turėtų užtikrinti savo darbuotojų parengimą su kibernetiniu saugumu susijusiose srityse.

Trečia, valstybės narės turėtų teikti pirmenybę informuotumui apie kibernetinį saugumą vykdydamos **informavimo kampanijas**, be kita ko, kampanijas, skirtas mokykloms,

---

52 https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

53 IBM ataskaita „The Cybersecurity Intelligence Index 2014“, nurodoma Securitymagazine.com, 2014 m. birželio 19 d.

54 https://www.nomoreransom.org/.

55 2014 m. liepos 23 d. priimtas Reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje (eIDAS reglamentas). Be to, Europos Komisija pagal Europos infrastruktūros tinklų priemonės programą teikia elektroninės atpažinties ir e. parašo sistemų sąveikumui užtikrinti būtinas pagrindines sudedamąsias dalis ir priemones.

universitetams, verslo bendruomenei ir mokslinių tyrimų įstaigoms. ENISA koordinuojama kasmet spalio mėn. vykdoma kibernetinio saugumo mėnesio iniciatyva bus pradėta taikyti plačiau kaip bendra ES ir nacionalinio lygmenų informavimo priemonė. Lygiai taip pat svarbu didinti informuotumą apie internetu socialiniuose tinkluose **vykdomas dezinformacijos kampanijas ir skelbiamas melagingas žinias**, kuriomis taikomasi sugriauti demokratinių procesų ir Europos vertybių pamatus. Nors pagrindinė atsakomybė, įskaitant atsakomybę už Europos Parlamento rinkimus, ir toliau tenka valstybėms narėms, patirtis rodo, kad keitimasis patirtimi ir ekspertinių žinių telkimas Europos lygmeniu padeda nukreipti veiksmus tinkama kryptimi[56].

Svarbus vaidmuo tenka ir visos **pramonės atstovams**, ypač – skaitmeninių paslaugų teikėjams ir gamintojams. Jie turi teikti naudotojams (privatiems asmenims, įmonėms ir viešojo administravimo institucijoms) priemones, leidžiančias jiems prisiimti atsakomybę už savo veiksmus internete, ir aiškiai nurodyti, kad kibernetinė higiena yra neatskiriama pasiūlymo vartotojams dalis[57]. Kad galėtų nustatyti ir spręsti pažeidžiamumo problemas, pramonės atstovai turėtų stengtis nustatyti vidaus tvarką, pagal kurią jos būtų tiriamos, rūšiuojamos ir sprendžiamos, nepriklausomai nuo to, ar potenciali pažeidžiama vieta atsirado dėl išorės ar dėl atitinkamos bendrovės vidaus veiksnių.

Pagrindiniai veiksmai:

- visapusiškai įgyvendinti Tinklų ir informacinių sistemų saugumo direktyvą;
- Europos Parlamentui ir Tarybai greitai priimti reglamentą, kuriuo nustatomi nauji agentūros ENISA įgaliojimai ir Europos sertifikavimo sistema[58];
- Komisijai ir pramonės atstovams imtis jungtinės iniciatyvos apibrėžti rūpestingumo pareigos principą, kuriuo būtų mažinamas produktų ir programinės įrangos pažeidžiamumas ir skatinamas saugumo užtikrinimas projektuojant;
- greitai įgyvendinti atsako į didelius tarpvalstybinius incidentus projektą;
- atlikti poveikio vertinimą, kurio tikslas – išnagrinėti galimybę 2018 m. pateikti Komisijos pasiūlymą sukurti kibernetinio saugumo kompetencijos centrų tinklą ir įsteigti Europos kibernetinio saugumo mokslinių tyrimų ir kompetencijos centrą remiantis iš karto pradėsimo bandomojo etapo rezultatais;
- padėti valstybėms narėms nustatyti sritis, kurių bendri kibernetinio saugumo projektai galėtų būti svarstomi kaip galimi remti Europos gynybos fondo lėšomis;
- siekiant padėti kibernetinių išpuolių aukoms, sukurti ES masto vieno langelio sistemą, kurioje būtų teikiama informacija apie naujausias grėsmes ir kaupiami praktiniai patarimai bei kibernetinio saugumo priemonės;
- valstybėms narėms imtis veiksmų siekiant įtraukti kibernetinio saugumo aspektą į gebėjimų ugdymo programas, e. valdžios sritį ir informavimo kampanijas;
- pramonės atstovams imtis veiksmų siekiant sustiprinti su kibernetiniu saugumu susijusį savo darbuotojų parengimą ir taikyti saugumo užtikrinimo projektuojant principą savo produktams, paslaugoms ir procesams.

[56] Pavyzdys – valstybių narių ir Sąjungos vyriausiosios įgaliotinės 2015 m. sukurta Strateginės komunikacijos Rytų kaimynystės šalyse darbo grupė, kurios tikslas – kovoti su Rusijos vykdomomis dezinformacijos kampanijomis. Ši darbo grupė kuria informavimo produktus ir kampanijas, kuriais siekiama aiškinti ES politiką Rytų partnerystės regione.

[57] Kai kuriems gamintojams ši koncepcija jau gerai žinoma, nes kai kuriuose gaminius reglamentuojančiuose ES teisės aktuose (pavyzdžiui, Mašinų direktyvoje 2006/42/EB) nurodoma taikyti saugumo užtikrinimo projektuojant principus.

[58] COM(2017) 477.

3. VEIKSMINGŲ ES KIBERNETINIŲ ATGRASYMO PRIEMONIŲ SUKŪRIMAS

Potencialūs kibernetiniai nusikaltėliai ir užpuolikai veiksmingai atgrasomi tada, kai įdiegiama patikimų atgrasomųjų priemonių sistema. Jei kibernetinių išpuolių vykdytojai (jie gali būti nevalstybiniai arba valstybiniai subjektai) nerizikuoja niekuo, išskyrus nesėkmę, jie turi mažai paskatų liautis bandyti. Siekiant veiksmingo atgrasomojo poveikio būtinas veiksmingesnis teisėsaugos atsakas, daugiausia dėmesio skiriant kibernetinių nusikaltėlių išaiškinimui, atsekamumui ir patraukimui baudžiamojon atsakomybėn. Be to, ES turi padėti valstybėms narėms kurti dvejopos paskirties kibernetinio saugumo priemones ir technologijas. Kibernetinių išpuolių antplūdį sustabdysime tik užtikrinę, kad galimybė sugauti ir nubausti juos surengusius asmenis būtų didesnė. Kibernetiniai išpuoliai turėtų būti greitai ištirti, o juos padarę asmenys patraukti atsakomybėn arba imtasi veiksmų, kuriais sudaromos sąlygos tinkamam politiniam ar diplomatiniam atsakui. Įvykus su svarbiais tarptautiniais ar gynybos klausimais susijusiai didelei krizei, vyriausiasis įgaliotinis galėtų pasiūlyti Tarybai imtis atitinkamų atsakomųjų priemonių.

Vienas toks žingsnis gerinant baudžiamosios teisės atsaką į kibernetinius išpuolius jau buvo Direktyvos dėl atakų prieš informacines sistemas[59] priėmimas 2013 m. Šia direktyva nustatytos būtiniausios taisyklės, susijusios su nusikalstamų veikų apibrėžtimi, ir sankcijos už išpuolius prieš informacines sistemas, taip pat numatytos operatyvinės priemonės institucijų bendradarbiavimui gerinti. Priėmus direktyvą, didelė pažanga padaryta visose valstybėse narėse panašiu mastu kriminalizuojant kibernetinius išpuolius – tai sudaro palankesnes sąlygas šios rūšies nusikaltimus tiriančių teisėsaugos institucijų tarptautiniam bendradarbiavimui. Vis dėlto tam, kad būtų išnaudotas visas direktyvos potencialas, valstybės narės turi visapusiškai įgyvendinti visas jos nuostatas[60]. Komisija ir toliau teiks paramą valstybėms narėms, šioms įgyvendinant direktyvą, ir, jos nuomone, šiuo metu nėra reikalo siūlyti direktyvos pakeitimų.

3.1. Piktavališkų subjektų nustatymas

Kad galimybė pažeidėjus patraukti atsakomybėn būtų didesnė, reikia skubiai stiprinti gebėjimą nustatyti už kibernetinius išpuolius atsakingus subjektus. Viena didžiausių problemų, su kuriomis susiduria teisėsaugos institucijos, – galimybė rasti kibernetiniams nusikaltimams tirti naudingos informacijos, visų pirma skaitmeninių pėdsakų. Todėl reikia stiprinti technologinį pajėgumą veiksmingai atlikti tyrimą, be kita ko, Europolo kovos su kibernetiniais nusikaltimais skyriuje didinant kibernetikos ekspertų skaičių. Europolas yra tapęs vienu pagrindinių subjektų, padedančių valstybėms narėms vykdyti tarpvalstybinius tyrimus. Jis turėtų tapti valstybių narių teisėsaugos institucijų tyrimų internete ir kibernetinės kriminalistikos kompetencijos centru.

Dėl paplitusios praktikos vieną IP adresą priskirti keletui – o kartais net tūkstančiams – vartotojų yra techniškai sudėtinga tirti piktavališką veiklą internete. Be to, siekiant nustatyti vieną piktavališką vartotoją, pavyzdžiui, tokių sunkių nusikaltimų, kaip seksualinė prievarta prieš vaikus, atvejais, kartais būtina tirti didelį vartotojų skaičių. Todėl ES skatins pereiti prie naujojo protokolo (IPv6), nes jis sudaro sąlygas kiekvienam vartotojui priskirti atskirą IP adresą – tai neabejotinai naudinga teisėsaugos institucijų darbui ir kibernetinio saugumo tyrimams. Kad paskatintų pereiti prie naujojo protokolo, Komisija pirmiausia reikalavimą pereiti prie IPv6 įtrauks į savo politiką, įskaitant viešųjų pirkimų, projektų ir mokslinių tyrimų

[59] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas.

[60] COM(2017) 474.

finansavimo reikalavimus, ir teiks paramą reikalingai mokymo medžiagai rengti. Be to, siekdamos skatinti interneto paslaugų teikėjus pereiti prie IPv6, valstybės narės turėtų apsvarstyti galimybę su jais sudaryti savanoriškus susitarimus.

Pasaulyje pagal IPv6 naudojimo mastą pirmauja Belgija[61] *– prie to taip pat prisidėjo viešojo ir privačiojo sektorių bendradarbiavimas: atitinkami suinteresuotieji subjektai nustatė, kad vienu IP adresu gali naudotis ne daugiau kaip 16 naudotojų, – tai savanoriška savireguliacijos priemonė, kuria skatinama pereiti prie IPv6*[62].

Apskritai, atskaitomybė internete turėtų būti skatinama dar labiau. Tai reiškia, kad reikia skatintis imtis priemonių, kuriomis užkertamas kelias piktnaudžiauti domenų vardais, siekiant siuntinėti nepageidaujamus pranešimus arba vogti duomenis. Šiuo tikslu Komisija imsis veiksmų, kuriais, prisidedant prie Interneto vardų ir numerių paskyrimo korporacijos[63] pastangų, gerinamas sistemose *Domain Name* ir IP WHOIS[64] esančios informacijos veikimas ir didinamas jos prieinamumas bei tikslumas.

3.2. Teisėsaugos atsako stiprinimas

Norint atgrasyti nuo kibernetinių išpuolių reikia veiksmingai **ištirti** nusikaltimus, padarytus pasinaudojant kibernetine erdve, ir **patraukti už juos baudžiamojon atsakomybėn**. Tačiau dabartinė procedūrinė sistema turi būti geriau pritaikyta prie esamų interneto amžiaus aplinkybių[65]. Taikant galiojančias procedūras gali būti sudėtinga greitai reaguoti į kibernetinių išpuoliuos, nes jie įvykdomi žaibiškai, be to, ypač reikalingas spartus tarpvalstybinis bendradarbiavimas. Kaip nurodyta Europos saugumo darbotvarkėje, šiuo tikslu Komisija 2018 m. pradžioje pateiks pasiūlymų, kaip **palengvinti tarpvalstybinę prieigą prie elektroninių įrodymų**. Kartu Komisija įgyvendina praktines priemones, palengvinsiančias tarpvalstybinę prieigą prie elektroninių įrodymų tiriant kriminalinius nusikaltimus; tarp jų – tarpvalstybinio bendradarbiavimo mokymų finansavimas, ES elektroninės informacijos mainų platformos kūrimas ir valstybių narių naudojamų teisminio bendradarbiavimo formų standartizavimas.

Kita veiksmingo patraukimo baudžiamojon atsakomybėn kliūtis – nevienodi e. įrodymų rinkimo kriminalistikos metodai, taikomi skirtingose valstybėse narėse tiriant kibernetinius nusikaltimus. Padėtis pagerėtų, jei būtų imtasi veiksmų bendriems kriminalistikos standartams nustatyti. Be to, siekiant geriau atsekti nusikaltimus ir priskirti juos padariusiems subjektams, reikia didinti kriminalistikos pajėgumus. Vienas iš būdų – toliau plėtoti Europolo kriminalistikos pajėgumus, geriau panaudojant esamus Europolo Europos kovos su elektroniniu nusikalstamumu centro finansinius ir žmogiškuosius išteklius, kad būtų galima patenkinti augantį operatyvinės pagalbos poreikį tiriant tarpvalstybinius kibernetinius nusikaltimus. Kitas būdas – pirmiau apibūdintą orientavimosi į technologijas principą taikyti

[61] https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

[62] http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

[63] Interneto vardų ir numerių paskyrimo korporacija (ICANN) yra ne pelno organizacija, atsakinga už kelių duomenų bazių, susijusių su interneto vardų sritimis, tvarkymo ir procedūrų koordinavimą.

[64] Užklausos ir atsakymo protokolas, plačiai naudojamas užklausoms duomenų bazėse, kuriose saugomi registruotų vartotojų ar interneto išteklių perėmėjų duomenys.

[65] Vienas pavyzdys: grupuotės *Avalanche* botneto (virtualus) centrinis valdymo ir kontrolės serveris iš vieno fizinio serverio ir domeno į kitą kėlėsi kas penkias minutes.

ir šifravimui, ištiriant, kokių didelių problemų kovojant su sunkiais nusikaltimais, įskaitant terorizmą ir kibernetinius nusikaltimus, kelia nusikaltėlių piktnaudžiavimo šifravimo spragomis atvejai. Šių svarstymų dėl **šifravimo vaidmens nusikalstamų veikų tyrimuose**[66] rezultatus Komisija pateiks iki 2017 m. spalio mėn.[67]

Kadangi internetas neturi sienų, Europos Tarybos **Budapešto konvencijoje dėl elektroninių nusikaltimų**[68] nustatyta tarptautinio bendradarbiavimo sistema yra optimalus teisinis standartas, kurį gali taikyti skirtingos šalys, atsižvelgdamos į tai, kad kiekvienos iš jų kovos su kibernetiniais nusikaltimais srities nacionaliniai teisės aktai yra skirtingi. Šiuo metu svarstoma galimybė papildyti Konvencijos protokolą[69], be to, tai galėtų būtų naudinga proga tarptautiniu lygiu išspręsti tarpvalstybinės prieigos prie elektroninių įrodymų problemą. Užuot priimant naujų kovos su kibernetiniais nusikaltimais srities tarptautinės teisės aktų, ES ragina visas šalis parengti tinkamus nacionalinės teisės aktus ir plėtoti bendradarbiavimą, kuris grindžiamas šia galiojančia tarptautine sistema.

Plintant anoniminimo priemonėms, nusikaltėliams tampa lengviau pasislėpti. Naujų būdų nusikaltėliams gauti prieigą prie seksualinės prievartos prieš vaikus medžiagos, narkotikų ar šaunamųjų ginklų atsirado kartu su **tamsiuoju internetu**[70], kuriame tikimybė būti pagautam dažnai yra nedidelė[71]. Dabar jis yra ir vienas iš pagrindinių kibernetiniams nusikaltimams naudojamų priemonių, kaip antai kenkimo programinės įrangos ir įsilaužimo priemonių, šaltinų. Siekdama rasti naujų sprendimų, Komisija kartu su atitinkamais suinteresuotaisiais subjektais išanalizuos nacionalines priemones. Europolas turėtų sudaryti palankesnes sąlygas atlikti tyrimus tamsiajame internete ir juos remti, vertinti grėsmes, padėti nustatyti jurisdikciją ir teikti prioritetą didelės rizikos atvejams, o ES galėtų būti vienas iš pagrindinių subjektų, koordinuojančių tarptautinius veiksmus[72].

Viena iš augančių kibernetinių nusikaltimų sričių – sukčiavimas naudojant kredito kortelių duomenis ar kitas elektronines mokėjimo priemones. Per kibernetinį išpuolį prieš interneto prekybininkus ar kitas teisėtai veikiančias įmones gauti mokėjimo priemonių duomenys vėliau parduodami internete, o nusikaltėliai gali juos panaudoti sukčiavimo tikslams[73]. Komisija siūlo atgrasomąjį poveikį sustiprinti priimant **Direktyvą dėl kovos su sukčiavimu**

---

66 Tarybai pirmininkaujančios valstybės narės pranešimas spaudai „2016 m. gruodžio 8 ir 9 d. vykusio Teisingumo ir vidaus reikalų tarybos posėdžio rezultatai“, dok. 15391/16.

67 2017 m. birželio 29 d. Aštuntoji pažangos, padarytos kuriant tikrą veiksmingą saugumo sąjungą, ataskaita (COM(2017) 354 *final*).

68 Konvencija yra pirmoji tarptautinė sutartis dėl nusikaltimų, įvykdytų internetu bei kituose kompiuterių tinkluose, visų pirma susijusi su autorių teisių pažeidimais, kompiuteriniu sukčiavimu, vaikų pornografija ir tinklo saugumo pažeidimais. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. 2017 m. ratifikavusios Europos Tarybos konvenciją dėl elektroninių nusikaltimų ar prie jos prisijungusios buvo 55 valstybės.

69 Įgaliojimai parengti Budapešto konvencijos dėl elektroninių nusikaltimų 2-ojo papildomo protokolo projektą, T-CY (2017)3.

70 Tamsųjį internetą sudaro tapačiųjų tinklų turinys; šiems tinklams naudojamas internetas, bet prie jų prisijungti reikalinga speciali programinė įranga, konfigūracija ar prieigos teisė. Tamsusis internetas sudaro nedidelę dalį giliojo saityno – paieškos sistemų neindeksuotos saityno dalies.

71 Žymesnė išimtis yra neseniai suardytos dvi iš didžiausių kriminalinių tamsiojo interneto rinkų – *AlphaBay* ir *Hansa*: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 Šioje srityje Europolui jau tenka svarbus vaidmuo. Naujausias pavyzdys: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

73 Iš sukčiavimo gaunamos pajamos sudaro didelę dalį organizuoto nusikalstamo pasaulio pajamų, taigi jos gali būti panaudotos kitiems nusikaltimams daryti, pavyzdžiui, užsiimti terorizmu, prekiauti narkotikais ar žmonėmis.

negrynosiomis mokėjimo priemonėmis ir jų klastojimu[74]. Taip siekiama atnaujinti šioje srityje galiojančias taisykles ir sustiprinti teisėsaugos institucijų gebėjimą kovoti su šių rūšių nusikaltimais.

Be to, turi būti stiprinami valstybių narių teisėsaugos institucijų pajėgumai ištirti kibernetinius nusikaltimus ir gilinamos prokurorų bei teisėjų žinios apie kibernetinėje erdvėje daromus nusikaltimus ir galimus jų tyrimo metodus. Prie šio tikslo bei tvirtesnio bendradarbiavimo prisideda Eurojustas ir Europolas, kurie glaudžiai bendradarbiauja su Europolo kovos su elektroniniu nusikalstamumu centro specializuotomis patariamosiomis grupėmis ir kovos su kibernetiniais nusikaltimais skyrių vadovų bei šioje srityje besispecializuojančių prokurorų tinklais. Kovai su kibernetiniais nusikaltimais Komisija skirs 10,5 mln. EUR, visų pirma pagal **policijos bendradarbiavimo, nusikalstamumo prevencijos, kovos su juo ir krizių valdymo finansinės paramos priemonę**. Suprasdama, kad mokymas yra svarbus elementas, Europos mokymo ir švietimo elektroninių nusikaltimų srityje grupė yra parengusi naudingos medžiagos. Europos Sąjungos teisėsaugos mokymo agentūrai teikiant paramą, dabar ši medžiaga turėtų būti pradėta platinti teisėsaugos pareigūnams.

3.3. Viešojo ir privačiojo sektorių bendradarbiavimas kovojant su kibernetiniais nusikaltimais

Įprasti teisėsaugos mechanizmai yra mažiau veiksmingi dėl skaitmeninio pasaulio specifikos: jį sudaro daugiausia privati infrastruktūra ir daugybė skirtingų subjektų įvairiose valstybėse. Todėl tam, kad būtų galima veiksmingai kovoti su nusikalstamumu, valdžios institucijoms yra ypač svarbu bendradarbiauti su privačiuoju sektoriumi, įskaitant ekonominio sektoriaus atstovus ir pilietinę visuomenę. Šiomis aplinkybėmis svarbus yra ir finansinis sektorius, todėl bendradarbiavimas su juo turėtų būti sustiprintas. Pavyzdžiui, finansinės žvalgybos padalinių[75] vaidmuo kovojant su kibernetiniais nusikaltimais turėtų būti didesnis.

Kai kurios valstybės narės jau ėmėsi svarbių veiksmų. Nyderlanduose finansų įstaigos ir teisėsaugos institucijos, siekdamos kovoti su sukčiavimu internete ir kibernetiniais nusikaltimais, kartu dalyvauja Elektroninių nusikaltimų darbo grupės veikloje. Vokietijos kovos su kibernetiniais nusikaltimais kompetencijos centras yra operatyvinis centras, kuris sudaro sąlygas savo nariams keistis informacija glaudžiai bendradarbiaujant su Vokietijos federaline policija ir rengti priemones, kuriomis siekiama užtikrinti apsaugą nuo kibernetinių nusikaltimų. Siekdamos sudaryti palankesnes sąlygas teisėsaugos institucijoms, akademinei bendruomenei ir privatiesiems partneriams bendradarbiauti geriausios praktikos plėtros ir keitimosi ja, mokymo ir pajėgumų stiprinimo srityse, 16 valstybių narių[76] yra įsteigusios kovos su kibernetiniais nusikaltimais kompetencijos centrus.
Komisija remia viešojo ir privačiojo sektorių partnerystę ir bendradarbiavimo mechanizmus vykdant tikslinius projektus, kaip antai plėtojant Kovos su sukčiavimu internete kibernetinio centro ir ekspertų tinklo[77] veiklą, ir užtikrina keitimosi informacija modelio ir standarto

[74] COM(2017) 489.

[75] Finansinės žvalgybos padaliniai yra nacionaliniai centrai, kuriems teikiami pranešimai apie įtartinus sandorius bei kita su pinigų plovimu, susijusiais pirminiais nusikaltimais ir terorizmo finansavimu susijusi informacija, ir kurie analizuoja tuos pranešimus bei informaciją ir skelbia tos analizės rezultatus.

[76] Belgija, Bulgarija, Čekija, Vokietija, Estija, Airija, Graikija, Ispanija, Prancūzija, Kipras, Lietuva, Austrija, Lenkija, Rumunija, Slovėnija ir Jungtinė Karalystė.

[77] Iniciatyva *EU-OF2CEN* siekiama suteikti galimybę bankams ir teisėsaugos institucijoms keistis su sukčiavimu internete susijusia informacija, kad būtų užkirstas kelias atlikti mokėjimus sukčių bei vadinamųjų pinigų mulų naudai ir būtų galima atlikti tyrimą, o nusikaltėlius patraukti baudžiamojon atsakomybėn. Šią iniciatyvą finansuoja ir ES (pagal policijos bendradarbiavimo, nusikalstamumo prevencijos, kovos su juo ir krizių valdymo finansinės paramos priemonę).

įgyvendinimą, kad būtų galima analizuoti ir sumažinti elektroninių nusikaltimų bei sukčiavimo internete riziką.

Plintant kibernetiniams nusikaltimams, privačiosioms įmonėms turi būti suteikta galimybė su teisėsaugos institucijomis keistis informacija apie konkrečius incidentus, įskaitant asmens duomenis, visapusiškai laikantis duomenų apsaugos taisyklių. 2018 m. gegužės mėn. pradėsiant vykdyti ES duomenų apsaugos reformą bus taikomos bendros taisyklės, kuriose nustatytos teisėsaugos institucijų ir privačiųjų subjektų bendradarbiavimo sąlygos. Europos Komisija dirbs kartu su Europos duomenų apsaugos valdyba ir atitinkamais suinteresuotaisiais subjektais, siekdama nustatyti šios srities geriausios praktikos pavyzdžių, ir atitinkamais atvejais teiks rekomendacijų.

3.4. Politinio atsako stiprinimas

Neseniai priimtoje **bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemoje**[78] (Kibernetinio saugumo diplomatijos priemonių rinkinyje) išdėstyta, kokių bendros užsienio ir saugumo politikos priemonių, įskaitant atsakomąsias priemones, galima imtis siekiant sustiprinti ES atsaką į veiklą, kuria kenkiama jos politiniams, saugumo ir ekonominiams interesams. Ši sistema yra svarbus žingsnis plėtojant ES ir valstybių narių lygmens gebėjimus atkreipti dėmesį į susidariusią padėtį ir į ją reaguoti. Ji padės padidinti gebėjimą kibernetinę kenkimo veiklą priskirti atitinkamiems subjektams, siekiant daryti įtaką potencialių agresorių elgesiui ir kartu atsižvelgti į poreikį užtikrinti proporcingą atsaką. Veikos priskyrimas valstybiniam ar nevalstybiniam subjektui išlieka suverenus politinis sprendimas, priimamas remiantis iš visų šaltinių surinktais žvalgybos duomenimis. Šiuo metu su valstybėmis narėmis pradėta įgyvendinti sistemą, tačiau siekiant reaguoti į didelio masto kibernetinius incidentus reikėtų daryti pažangą ir bendro projekto įgyvendinimo srityje[79]. INTCEN[80], glaudžiai bendradarbiaudamas su valstybėmis narėmis ir ES institucijomis, turėtų bendrinti ir analizuoti informaciją apie padėtį, reikalingą sistemos teikiamoms priemonėms panaudoti, ir ta informacija dalytis.

3.5. Atgrasomųjų kibernetinio saugumo priemonių stiprinimas pasitelkiant valstybių narių gynybos pajėgumus

Valstybės narės jau didina kibernetinės gynybos pajėgumus. Be to, atsižvelgiant į tai, kad nyksta skirtumas tarp kibernetinės gynybos ir kibernetinio saugumo ir dvejopos paskirties kibernetinių priemonių ir technologijų, o valstybių narių taikomi metodai labai skiriasi, tinkamai padėti skatinti karinių ir civilinių pastangų sinergiją gali ES.[81]

Valstybės narės, kurių kibernetinio saugumo pajėgumai yra didesni ir kurios pageidauja juos bendrai sutelkti, galėtų apsvarstyti galimybę, padedant Sąjungos vyriausiajam įgaliotiniui, Komisijai ir Europos gynybos agentūrai, kibernetinio saugumo klausimą įtraukti į nuolatinio struktūrizuoto bendradarbiavimo programą. Taip galėtų būtų remiama pirmiau nurodyta veikla, kuria siekiama didinti ES pramonės pajėgumus ir strateginę autonomiją. ES taip pat gali skatinti sąveiką, be kita ko, sudarydama palankesnes sąlygas plėtoti pajėgumus ir koordinuoti mokymą, švietimą ir pastangas standartizuoti dvejopos paskirties priemones ir technologijas.

---

[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

[79] C(2017) 6100.

[80] JOIN(2016) 18 *final*.

[81] ES suvokia, kad kibernetinė erdvė yra tokia pati veiklos sritis, kaip ir sausuma, oro erdvė ar jūra. Kibernetinės gynybos pastangos taip pat apima kosmoso infrastruktūros ir susijusios antžeminės infrastruktūros apsaugą bei atsparumo užtikrinimą.

Be to, reikėtų visapusiškai išnaudoti bendros sistemos teikiamas galimybes reaguoti į hibridines grėsmes, kurios dažnai pasireiškia kibernetiniais išpuoliais, visų pirma pasitelkiant ES hibridinių grėsmių analizės ir informavimo centrą ir neseniai Helsinkyje įsteigtą Europos kovos su hibridinėmis grėsmėmis kompetencijos centrą, kuriam pavesta skatinti strateginį dialogą ir atlikti mokslinius tyrimus bei analizę.

ES vėl skirs dėmesį 2014 m. ES kibernetinės gynybos politikos sistemai[82], kuri yra priemonė kibernetiniam saugumui ir gynybai labiau integruoti į bendrą saugumo ir gynybos politiką (BSGP). Ypač svarbus pačių BSGP misijų ir operacijų kibernetinis atsparumas: bus parengtos standartinės procedūros ir sustiprinti techniniai pajėgumai, kurie galėtų būti naudingi tiek dislokuotoms civilinėms ir karinėms misijoms ir operacijoms, tiek atitinkamoms jų planavimo ir vykdymo pajėgumų struktūroms ir Europos išorės veiksmų tarnybos (EIVT) informacinių technologijų paslaugų teikėjams. Siekdamos gerinti valstybių narių bendradarbiavimą ir tinkamiau reguliuoti ES pastangas šioje srityje, Europos gynybos agentūra ir EIVT, bendradarbiaudamos su Komisijos tarnybomis, sudarys palankesnes sąlygas valstybių narių kibernetinės gynybos politikos formuotojams palaikyti ryšį strateginiu lygiu. ES taip pat rems Europos kibernetinio saugumo sprendimų paieškas – taip, be kita ko, remiama Europos gynybos pramoninė ir technologinė bazė. Šie veiksmai apima ir paramą regioninėms kibernetinio saugumo ir gynybos srities kompetencijos grupėms.

Komisijos tarnybos, glaudžiai bendradarbiaudamos su EIVT, valstybėmis narėmis ir kitomis atitinkamomis ES įstaigomis, iki 2018 m. sukurs **kibernetinės gynybos mokymų ir švietimo platformą**, skirtą esamoms kibernetinės gynybos įgūdžių spragoms užpildyti. Ši platforma papildys Europos gynybos agentūros darbą šioje srityje ir padės stiprinti kibernetinio saugumo ir kibernetinės gynybos įgūdžius, kurie šiuo metu yra nepakankami.

Pagrindiniai veiksmai:

- pateikti Komisijos iniciatyvą dėl tarpvalstybinės prieigos prie elektroninių įrodymų (2018 m. pradžioje);
- Europos Parlamente ir Taryboje greitai priimti siūlomą Direktyvą dėl kovos su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu;
- ES viešųjų pirkimų, mokslinių tyrimų ir projektų finansavimo srityje nustatyti su IPv6 susijusius reikalavimus; numatyti galimybę sudaryti savanoriškus valstybių narių ir interneto paslaugų teikėjų susitarimus, siekiant juos paskatinti pereiti prie IPv6;
- atnaujinti ir išplėsti Europolo įgaliojimus kibernetinės kriminalistikos ir tamsiojo interneto stebėjimo srityse;
- įgyvendinti bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą priemonių sistemą;
- teikti didesnę finansinę paramą nacionaliniams ir tarpvalstybiniams projektams, kuriais siekiama gerinti padėtį su kibernetine erdve susijusios baudžiamosios teisenos srityje;
- 2018 m. sukurti su kibernetiniu saugumu susijusio mokymo platformą, skirtą nepakankamiems kibernetinio saugumo ir kibernetinės gynybos įgūdžiams stiprinti.

4. TARPTAUTINIO BENDRADARBIAVIMO KIBERNETINIO SAUGUMO SRITYJE STIPRINIMAS

Nuolat besikeičiantys ES tarptautinės kibernetinio saugumo politikos, kurioje vadovaujamasi tokiomis pagrindinėmis teisėmis, kaip saviraiškos laisvė ir teisė į privatų gyvenimą ir asmens duomenų apsaugą, ir kuria siekiama atviros, laisvos ir saugios kibernetinės erdvės, uždaviniai

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

– propaguoti kibernetinį stabilumą visame pasaulyje ir prisidėti prie Europos strateginės autonomijos ir saugumo kibernetinėje erdvėje.

4.1. Kibernetinis saugumas išorės santykiuose

Iš turimų duomenų matyti, kad iš kitų šalių vykdomi kibernetiniai išpuoliai visame pasaulyje laikomi viena didžiausių grėsmių nacionaliniam saugumui[83]. Kadangi ši grėsmė yra visuotinė, labai svarbi kibernetinių išpuolių, kurie vis stipriau veikia tarptautinį stabilumą ir saugumą, prevencijos ir atgrasymo nuo jų dalis – kurti ir palaikyti tvirtas sąjungas ir partnerystės ryšius su trečiosiomis šalimis. Palaikydama dvišalius, regioninio lygmens ir daugiašalius bei daugelį subjektų apimančius santykius ES teiks pirmenybę strateginei konfliktų prevencijos ir saugumo kibernetinėje erdvėje užtikrinimo programai.

ES ryžtingai pasisako už tai, kad kibernetinėje erdvėje būtų taikoma tarptautinė teisė, visų pirma Jungtinių Tautų Chartija. ES pritaria, kad, be teisiškai privalomų tarptautinės teisės normų, būtų taikomos ir savanoriškos privalomos teisinės galios neturinčios normos, taisyklės ir Jungtinių Tautų vyriausybių ekspertų grupės suformuluoti atsakingo valstybių elgesio principai[84]; ji taip pat skatina kurti ir įgyvendinti regionines tiek Europos saugumo ir bendradarbiavimo organizacijos (ESBO), tiek kitų regionų pasitikėjimo stiprinimo priemones.

Dvišaliuose santykiuose bus toliau plėtojami dialogai kibernetinio saugumo klausimais[85] ir juos papildys pastangos sudaryti palankesnes sąlygas bendradarbiauti su trečiosiomis šalimis siekiant užtikrinti, kad kibernetinėje erdvėje būtų griežčiau vadovaujamasi deramo rūpestingumo ir valstybės atsakomybės principais. Tarptautinėje arenoje ES teiks pirmenybę tarptautinio saugumo kibernetinėje erdvėje klausimams, kartu užtikrindama, kad kibernetinis saugumas netaptų pretekstu taikyti rinkos protekcionizmo priemones ir riboti pagrindines teises ir laisves, be kita ko, saviraiškos laisvę ir teisę gauti informaciją. Kad kibernetinio saugumo samprata būtų plati, ji turi apimti pagarbą žmogaus teisėms, todėl ES ir toliau visame pasaulyje puoselės pagrindines Sąjungos vertybes, remdamasi ES žmogaus teisių gairėmis dėl saviraiškos laisvės internete.[86] Šiuo atžvilgiu ES pabrėžia, jog svarbu, kad reguliuojant internetą dalyvautų visi suinteresuotieji subjektai.

Komisija taip pat pasiūlė[87] modernizuoti ES eksporto kontrolę, be kita ko, nustatant ypatingos svarbos kibernetinio stebėjimo technologijų, kuriomis galėtų būti pažeistos žmogaus teisės arba kurias neteisėtai naudojant galėtų kilti grėsmė pačios ES saugumui, eksporto kontrolę, ir, siekdama visame pasaulyje skatinti konvergenciją ir atsakingą elgesį šioje srityje, stiprins dialogą su trečiosiomis šalimis.

4.2. Kibernetinio saugumo pajėgumų stiprinimas

Pasaulinis kibernetinis stabilumas priklauso nuo to, kaip visoms šalims vietos ir nacionaliniu lygmenimis pavyks užkirsti kelią kibernetiniams incidentams ir į juos reaguoti, ištirti kibernetinius nusikaltimus ir už juos patraukti baudžiamojon atsakomybėn. Padedant trečiosioms šalims tapti atsparesnėms, pakils visuotinis kibernetinio saugumo lygis, o tai turės teigiamą poveikį ES. Norint kovoti su greitai besivystančiomis kibernetinėmis grėsmėmis reikėtų dėti mokymo, politikos ir teisėkūros pastangas, be to, kiekvienoje pasaulio šalyje

---

83 Pew mokslinių tyrimų centro tyrimas *Global Attitudes Survey*, 2017 m. pavasaris.
84 Dok. A/68/98 ir A/70/174.
85 2017 m. rugsėjo mėn. dialogą kibernetinio saugumo klausimais ES palaikė su JAV, Kinija, Japonija, Korėjos Respublika ir Indija.
86 ES žmogaus teisių gairės dėl saviraiškos laisvės internete ir realiame gyvenime.
87 COM(2016) 616.

reikėtų įsteigti veiksmingas kompiuterinių incidentų tyrimo tarnybas ir kovos su kibernetiniais nusikaltimais skyrius.

Nuo 2013 m. ES pirmauja tarptautinio kibernetinio saugumo gebėjimų stiprinimo srityje ir šias pastangas sistemingai susieja su vystomojo bendradarbiavimo veikla. ES toliau skatins taikyti pagarba žmogaus teisėms grindžiamą pajėgumų stiprinimo modelį, kuris atitinka *Digital4Development* modelį[88]. Pajėgumų stiprinimo srityje prioritetas bus teikiamas ES kaimynystės politikos šalims ir besivystančioms šalims, kuriose dėl greitai plintančio interneto ryšio sparčiai daugėja grėsmių. ES pastangos papildys jos vystymosi veiksmus pagal Darnaus vystymosi darbotvarkę iki 2030 m. ir bendras pastangas stiprinti institucinius pajėgumus.

Kad ES galėtų geriau sutelkti savo kolektyvines ekspertų žinias ir taip sustiprinti savo pajėgumus, reikėtų įsteigti specialų ES kibernetinių pajėgumų stiprinimo tinklą, kurį sudarytų EIVT, valstybių narių kibernetinio saugumo institucijų, ES agentūrų, Komisijos tarnybų, akademinės bendruomenės ir pilietinės visuomenės atstovai. Bus parengtos ES kibernetinių pajėgumų stiprinimo gairės, kuriose bus išdėstytos ES pagalbos trečiosioms šalims politinės gairės ir prioritetai.

Šioje srityje ES bendradarbiaus ir su kitais rėmėjais, kad būtų išvengta pastangų dubliavimo ir kad skirtinguose regionuose pajėgumai būtų stiprinami kryptingiau.

4.3. ES ir NATO bendradarbiavimas

Didindama jau padarytą pažangą, ES imsis tvirtesnio bendradarbiavimo su NATO kibernetinio saugumo, hibridinių grėsmių ir gynybos srityje, kaip numatyta 2016 m. liepos 8 d. bendrame pareiškime[89]. Prioritetas teikiamas sąveikos skatinimui užtikrinant kibernetinės gynybos reikalavimų ir standartų nuoseklumą, su mokymu ir pratybomis susijusio bendradarbiavimo stiprinimui ir mokymui keliamų reikalavimų suderinimui.

ES ir NATO taip pat skatins bendradarbiauti kibernetinės gynybos mokslinių tyrimų ir inovacijų srityje ir plėtoti turimus techninius susitarimus dėl atitinkamų jų kibernetinio saugumo įstaigų[90] keitimosi kibernetinio saugumo informacija. Siekiant stiprinti atsparumą ir atsaką į kibernetines krizes, turėtų būti geriau išnaudojamos naujausios bendros kovos su hibridinėmis grėsmėmis pastangos, visų pirma ES hibridinių grėsmių analizės ir informavimo centro ir NATO hibridinių grėsmių analizės skyriaus bendradarbiavimo teikiama nauda. Tolesnis ES ir NATO bendradarbiavimas bus remiamas rengiant kibernetinės gynybos pratybas, į jas įtraukiant EIVT bei kitus ES subjektus ir atitinkamas NATO įstaigas, įskaitant NATO bendros kibernetinės gynybos kompetencijos centrą Taline. NATO ir ES surengs pirmąsias lygiagrečiąsias koordinuojamas reagavimo į hibridinį scenarijų pratybas: 2017 metais joms vadovaus NATO, o 2018 metais panašias pratybas surengs ES. 2017 m. gruodžio mėn. kiekvienos iš šių asociacijų tarybai bus pateikta ES ir NATO santykių ataskaita; tai bus proga apsvarstyti galimybę dar labiau plėtoti bendradarbiavimą, visų pirma užtikrinant, kad visų atitinkamų institucijų ir įstaigų, įskaitant ENISA, tarpusavio ryšio priemonės būtų bendrai prieinamos, saugios ir atsparios.

Pagrindiniai veiksmai:

- remti strateginę konfliktų prevencijos ir saugumo kibernetinėje erdvėje užtikrinimo programą;

[88] SWD(2017) 157.
[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] CERT-EU ir NATO reagavimo į kompiuterinius incidentus tarnyba (NCIRC).

- įsteigti naują kibernetinių pajėgumų stiprinimo tinklą, kuris teiktų paramą trečiosioms šalims, kad jos galėtų šalinti kibernetines grėsmes, ir parengti ES kibernetinio saugumo gebėjimų stiprinimo gaires, kad būtų tinkamiau nustatomi ES pastangų prioritetai;
- toliau plėtoti ES ir NATO bendradarbiavimą – dalyvauti lygiagrečiose ir koordinuojamose pratybose ir užtikrinti didesnį kibernetinio saugumo standartų sąveikumą.

5. IŠVADA

ES kibernetinė parengtis yra ypač svarbi tiek bendrajai skaitmeninei rinkai, tiek saugumo ir gynybos sąjungai. Privalu stiprinti Europos kibernetinį saugumą ir šalinti tiek civiliniams, tiek kariniams objektams kylančias grėsmes.

2017 m. rugsėjo 29 d. Tarybai pirmininkaujančios Estijos surengsimas aukščiausiojo lygio susitikimas skaitmeniniais klausimais bus proga parodyti, jog visi esame pasiryžę imtis priemonių, kad ES, kaip skaitmeninei visuomenei, kibernetinis saugumas taptų vienu pagrindinių klausimų. Siekdama įgyvendinti šį bendrą įsipareigojimą, Komisija ragina valstybes nares pateikti įsipareigojimų dėl to, kokių veiksmų jos ketina imtis tose srityse, kuriose pagrindinė atsakomybė tenka joms. Be kita ko, kibernetinis saugumas turėtų būti stiprinamas:

- užtikrinant, kad iki 2018 m. gegužės 9 d. būtų visapusiškai ir veiksmingai įgyvendinta TIS direktyva ir už kibernetinį saugumą atsakingoms valdžios institucijoms būtų skirta pakankamai išteklių funkcijoms veiksmingai vykdyti;
- tas pačias taisykles taikant viešojo administravimo institucijoms, priklausomai nuo jų vaidmens visuomenėje ir ekonomikoje apskritai;
- viešojo administravimo institucijose rengiant su kibernetiniu saugumu susijusius mokymus;
- informavimo kampanijose teikiant prioritetą informuotumui apie kibernetinius nusikaltimus ir kibernetinį saugumą įtraukiant į akademines ir profesinio mokymo programas;
- pasinaudojant nuolatinio struktūrizuoto bendradarbiavimo iniciatyvų ir Europos gynybos fondo teikiamomis galimybėmis remti kibernetinės gynybos projektų rengimą.

Šiame bendrame komunikate aprašytas problemos mastas ir nurodyta, kokių priemonių ES gali imtis. Mums reikia atsparios Europos, kuri galėtų veiksmingai apsaugoti savo piliečius numatydama galimus kibernetinius incidentus, savo struktūromis ir elgesiu užtikrindama veiksmingą apsaugą, gebėdama greitai atsigauti nuo kibernetinių išpuolių ir atgrasydama už juos atsakingus subjektus. Šiame komunikate siūloma imtis tikslinių priemonių, kuriomis, visapusiškai dalyvaujant valstybėms narėms ir įvairioms atitinkamoms ES struktūroms ir atsižvelgiant į jų kompetenciją bei atsakomybės sritis, bus toliau koordinuotai stiprinamos ES kibernetinio saugumo struktūros ir pajėgumai. Įgyvendinę šį komunikatą aiškiai parodysime, kad ES ir valstybės narės veiks kartu, kad nustatytų kibernetinio saugumo standartą, kuris nenusileistų vis augančioms grėsmėms, su kuriomis šiandien susiduria Europa.