EIROPAS
KOMISIJA

SAVIENĪBAS AUGSTĀ
PĀRSTĀVE ĀRLIETĀS UN
DROŠĪBAS POLITIKAS
JAUTĀJUMOS

Briselē, 13.9.2017.
JOIN(2017) 450 final

KOPĪGS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību

1. IEVADS

Kiberdrošība ir ļoti svarīga gan mūsu labklājībai, gan drošībai. Tā kā mūsu ikdiena un ekonomika aizvien vairāk kļūst atkarīga no digitālajām tehnoloģijām, mēs tiekam pakļauti arvien lielākam riskam. Kiberincidenti variē gan atkarībā no tā, kurš par tiem ir atbildīgs, gan kāds ir to nolūks. Ļaunprātīgas kiberdarbības apdraud ne tikai ekonomiku un virzību uz digitālo vienoto tirgu, bet arī demokrātijas pamatfunkcijas, brīvību un mūsu vērtības. Turpmāk mūsu drošība būs atkarīga no spējas pārveidoties, lai aizsargātu ES pret kiberdraudiem: gan civilās infrastruktūras, gan militāro spēju pamatā ir drošas digitālās sistēmas. To 2017. gada jūnijā atzina Eiropadomē[1], kā arī Eiropas Savienības globālajā ārpolitikas un drošības politikas stratēģijā (*EUGS*)[2].

Riski pieaug eksponenciāli. Pētījumos ir konstatēts, ka kibernoziegumu ietekme uz ekonomiku no 2013. gada līdz 2017. gadam ir palielinājusies pieckārt, un tā var kļūt četrreiz lielāka laikā līdz 2019. gadam[3]. Izspiedējvīruss[4] tiek izmantots aizvien biežāk, un ar tā palīdzību veiktie uzbrukumi pēdējā laikā[5] atspoguļo straujo kibernoziedzības pastiprināšanos. Tomēr izspiedējvīruss nepavisam nav vienīgais apdraudējums.

Kiberdraudus rada gan nevalstiskie, gan valsts izpildītāji. Visbiežāk tas ir krimināla rakstura apdraudējums peļņas gūšanas nolūkā, tomēr tas var būt arī politiski un stratēģiski motivēts. Kriminālos draudus pastiprina robežu saplūšana starp kibernoziedzību un "tradicionālo" noziedzību, jo noziedznieki izmanto internetu gan savas darbības paplašināšanai, gan kā izziņas avotu jaunām noziegumu pastrādāšanas metodēm un līdzekļiem[6]. Tomēr lielākajā daļā gadījumu noziedznieka izsekošanas iespējas ir niecīgas, un izredzes veikt krimināltvajāšanu — vēl mazākas.

Tajā pašā laikā valsts izpildītāji aizvien biežāk īsteno savus ģeopolitiskos mērķus ne tikai ar tradicionālu līdzekļu, piemēram, militāro spēku palīdzību, bet arī ar diskrētākiem kiberrīkiem, tostarp iejaucoties iekšējos demokrātiskajos procesos. Tagad ir plaši atzīts, ka kibertelpa (vai nu atsevišķi, vai kā daļa no hibrīdpieejas) tiek izmantota kā karadarbības domēns. Dezinformācijas kampaņas, nepatiesas ziņas un kiberoperācijas, kuru mērķis ir kritiskā infrastruktūra, kļūst aizvien vairāk izplatītas, un uz tām ir jāreaģē. Šajā nolūkā savā pārdomu dokumentā par Eiropas aizsardzības nākotni[7] Eiropas Komisija uzsver to, cik svarīga ir sadarbība kiberaizsardzības jomā.

Ja mēs būtiski neuzlabosim savu kiberdrošību, līdz ar digitālajām pārmaiņām risks pieaugs. Ir sagaidāms, ka līdz 2020. gadam desmitiem miljardu "lietu interneta" ierīču tiks pieslēgtas internetam, bet kiberdrošība vēl joprojām nav prioritāra to izstrādē[8]. Nespējai aizsargāt ierīces, kuras kontrolēs mūsu elektrotīklus, auto un transporta tīklus, rūpnīcas, finanšu līdzekļus, slimnīcas un mājas, var būt postošas sekas, un tā var graut patērētāju uzticību

---

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

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

3 Skatīt, piemēram, *McAfee* un Stratēģisko un starptautisko pētījumu centra (*Center for Strategic and International Studies (CSIS)*) 2014. gadā veikto pētījumu "*Net losses: Estimating the Global Cost of Cybercrime*".

4 Izspiedējvīruss ir ļaunprogrammatūras veids, kas neļauj vai ierobežo lietotāju piekļuvi savai sistēmai, vai nu nobloķējot sistēmas ekrānu vai lietotāju failus, kamēr nav samaksāta izpirkuma maksa.

5 2017. gada maijā izspiedējvīrusa *WannaCry* uzbrukums skāra vairāk nekā 400 000 datoru vairāk nekā 150 valstīs. Pēc mēneša no izspiedējvīrusa *Petya* uzbrukuma cieta Ukraina un vairāki uzņēmumi visā pasaulē.

6 Eiropols, Smagu un organizēto noziegumu draudu novērtējums 2017. gadā.

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

8 *IDC and TXT Solutions* (2014), *SMART 2013/0037,* Mākoņa un lietu interneta apvienojums, pētījums Komisijai (*Cloud and IoT combination, study for the Commission*).

jaunajām tehnoloģijām. Risku jo vairāk pastiprina politiski motivētu uzbrukumu civiliem mērķiem iespējamība un nepilnības militārajā kiberaizsardzībā.

Šajā kopīgajā paziņojumā izklāstītā pieeja ļaus ES labāk reaģēt uz minētajiem draudiem. Tas nodrošinās noturību un stratēģisko autonomiju, palielinot ar tehnoloģiju un prasmēm saistītās iespējas, kā arī palīdzēs veidot spēcīgu vienoto tirgu. Lai nostiprinātu kiberdrošību un reaģētu attiecīgā gadījumā, ir nepieciešams izveidot pareizās struktūras, pilnībā iesaistot visus galvenos dalībniekus. Šī pieeja arī labāk novērstu kiberuzbrukumus, paātrinot to atklāšanu, izsekošanu un personu saukšanu pie atbildības. Tā arī ietvertu globālo dimensiju, attīstot starptautisko sadarbību kā platformu ES vadošajai lomai kiberdrošības jomā. Šie pasākumi balstās uz pieejām, ko izmanto digitālā vienotā tirgus ietvaros, globālajā stratēģijā, Eiropas Drošības programmā[9], Kopīgajā regulējumā hibrīddraudu apkarošanai[10] un paziņojumā par Eiropas Aizsardzības fonda izveidi[11][12].

ES jau strādā pie daudziem no šiem jautājumiem, un ir laiks apkopot visus darba virzienus vienuviet. 2013. gadā ES laida klajā kiberdrošības stratēģiju, aptverot galvenos darba virzienus, lai uzlabotu kibernoturību[13]. Tās galvenie mērķi un principi, kas veicina uzticamu, drošu un atvērtu kiberekosistēmu, paliek spēkā. Bet pastāvīgā attīstībā esošā situācija ar pastiprinātu apdraudējumu pieprasa papildu darbības, kas ļautu izturēt uzbrukumus nākotnē un novērst tos[14].

ES ir pietiekami nodrošināta, lai reaģētu uz kiberdrošības izaicinājumiem, ņemot vērā tās politikas tvērumu un tās rīcībā esošos rīkus, struktūras un iespējas. Dalībvalstis joprojām ir atbildīgas par valsts drošību, taču apdraudējuma tvērums un pārrobežu raksturs nepārprotami liecina par nepieciešamību rīkoties ES līmenī, sniedzot dalībvalstīm stimulus un atbalstu valsts kiberdrošības spēju attīstībai un uzlabošanai, tajā pašā laikā stiprinot ES līmeņa spējas. Šī pieeja ir izstrādāta, lai pamudinātu visus dalībniekus — ES, dalībvalstis, nozari un personas — noteikt kiberdrošībai tādu prioritāti, kas ir nepieciešama noturības veidošanai un labākai ES reaģēšanas spējai pret kiberuzbrukumiem. Tajā ir noteikti konkrēti pasākumi, lai palīdzētu atklāt un izmeklēt jebkura veida kiberincidentus pret ES un tās dalībvalstīm un atbilstoši uz tiem reaģētu, tostarp izvirzītu apsūdzību noziedzniekiem. Tas sekmēs ES ārējo darbību, lai efektīvi nodrošinātu kiberdrošību globālā mērogā. Rezultātā ES sagaidāma pāreja no reaģējošas pieejas uz proaktīvu, lai aizsargātu Eiropas labklājību, sabiedrību un vērtības, kā arī pamatvērtības un pamatbrīvības, reaģējot uz pastāvošajiem un iespējamiem draudiem.

2. ES NOTURĪBAS PRET KIBERUZBRUKUMIEM VEIDOŠANA

Spēcīgai kibernoturībai nepieciešama kopēja un plaša tvēruma pieeja. Tai ir nepieciešamas stabilākas un efektīvākas struktūras, lai stiprinātu kiberdrošību un reaģētu uz kiberuzbrukumiem ne tikai dalībvalstīs, bet arī ES iestādēs, aģentūrās un struktūrās. Kibernoturības un stratēģiskās autonomijas veidošanai ir nepieciešama visaptverošāka daudznozaru politiskā pieeja ar spēcīgu vienoto tirgu, nozīmīgu ES tehnoloģisko spēju progresu un daudz lielāku skaitu kvalificētu ekspertu. Tā visa pamatā ir nepieciešama

[9] COM(2015) 185 *final*.
[10] JOIN(2016) 18 *final*.
[11] COM(2017) 295.
[12] Pieeju arī pamato neatkarīgas zinātniskas konsultācijas, ko sniedz Eiropas Komisijas Zinātnisko konsultāciju mehānisma augsta līmeņa zinātnisko padomdevēju grupa (skatīt atsauces turpmāk).
[13] JOIN(2013) 1 *final*. Šīs stratēģijas novērtējums ir pieejams SWD (2017) 295.
[14] Ja nav noteikts citādi, šajā paziņojumā izklāstītie priekšlikumi neietekmē budžetu. Jebkura iniciatīva, kura ietekmē budžetu, tiek pienācīgi izskatīta ikgadējā budžeta procedūru ietvaros, un tā neietekmē nākamo daudzgadu finanšu shēmu pēc 2020. gada.

vispārēja atziņa, ka kiberdrošība ir kopīgs izaicinājums sabiedrībai, lai tajā iesaistītos daudzējādie valdības, ekonomikas un sabiedrības slāņi.

2.1. Eiropas Savienības Tīklu un informācijas drošības aģentūras stiprināšana

Eiropas Savienības Tīklu un informācijas drošības aģentūrai (*ENISA*) ir viena no galvenajām lomām ES kibernoturības un reaģēšanas spēju stiprināšanā, bet to ierobežo aģentūras pašreizējās pilnvaras. Tādēļ Komisija nāk klajā ar vērienīgas reformas priekšlikumu, kas ietver arī **pastāvīgu aģentūras pilnvaru nodrošināšanu**[15]. Tas nodrošinātu, ka *ENISA* varētu sniegt atbalstu dalībvalstīm, ES iestādēm un uzņēmumiem galvenajās jomās, tostarp direktīvas par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā[16] ("kiberdrošības direktīvas") un ierosinātā kiberdrošības sertifikācijas satvara īstenošanā.

Pēc reformu veikšanas *ENISA* būs ietekmīgs konsultants politikas izstrādē un īstenošanā, tostarp veicinot saskaņotību starp nozaru iniciatīvām un kiberdrošības direktīvu un palīdzot izveidot informācijas apmaiņas un analīzes centrus kritiskajās nozarēs. *ENISA* paaugstinātu prasības un veicinātu Eiropas sagatavotību, organizējot ikgadējās Eiropas mēroga kiberdrošības mācības, kas apvienotu dažādu līmeņu reaģēšanas spējas. Tā arī sniegtu atbalstu ES politikas izstrādē attiecībā uz informācijas un komunikācijas tehnoloģiju (IKT) kiberdrošības sertifikāciju, un tai būtu svarīga loma operatīvās sadarbības un krīzes pārvarēšanas sekmēšanā visā ES. Aģentūra darbotos arī kā informācijas un zināšanu kontaktpunkts kiberdrošības kopienā.

Ātra un kopīgota izpratne attiecībā uz atklātajiem draudiem un incidentiem ir priekšnoteikums lēmuma pieņemšanai par to, vai ir nepieciešama ES atbalstīta kopējas draudu mazināšanas vai reaģēšanas darbība. Šādai informācijas apmaiņai ir nepieciešama visu attiecīgo dalībnieku — ES struktūru un aģentūru, kā arī dalībvalstu — iesaiste tehniskajā, operatīvajā un stratēģiskajā līmenī. *ENISA*, sadarbojoties ar attiecīgajām struktūrām dalībvalstu un ES līmenī, jo īpaši ar datordrošības incidentu reaģēšanas vienību tīklu[17], ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienību (*CERT-EU*), Eiropolu un ES Izlūkdatu analīzes centru (*INTCEN*), dos arī ieguldījumu situāciju apzināšanā ES līmenī. Tas var tikt izmantots izlūkdatos par draudiem un politikas veidošanā regulāras vispārējā apdraudējuma stāvokļa uzraudzības un efektīvas operatīvās sadarbības kontekstā, kā arī reaģēšanā uz plaša mēroga pārrobežu incidentiem.

2.2. Virzība uz vienotu kiberdrošības tirgu

Kiberdrošības tirgus izaugsme ES — produktu, pakalpojumu un procesu ziņā — tiek kavēta vairākos veidos. Galvenais aspekts ir visā ES atzītu kiberdrošības sertifikācijas shēmu trūkums, kas noteiktu augstākus produktu noturības standartus un liktu pamatus ES mēroga tirgus ticamībai. Tādēļ Komisija nāk klajā ar priekšlikumu izveidot **ES kiberdrošības sertifikācijas satvaru**[18]. Satvarā tiktu noteikta procedūra ES mēroga kiberdrošības sertifikācijas shēmu izveidei, kas attiektos uz produktiem, pakalpojumiem un/vai sistēmām un

[15] COM(2017) 477.

[16] Eiropas Parlamenta un Padomes Direktīva 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

[17] Kā noteikts kiberdrošības direktīvas 9. pantā.

[18] COM(2017) 477.

kas ļautu pielāgot ticamības līmeni konkrētajam lietošanas veidam (piemēram, kritiskai infrastruktūrai vai patērētāju ierīcēm)[19]. Tas dotu nepārprotamas priekšrocības uzņēmumiem, izslēdzot nepieciešamību kārtot dažādas sertifikācijas formalitātes pārrobežu tirdzniecībā un samazinot administratīvās un finanšu izmaksas. Saskaņā ar šo satvaru izstrādāto shēmu izmantošana arī palielinātu patērētāju uzticēšanos; ar atbilstības sertifikāta palīdzību pircēji un lietotāji tiktu informēti un pārliecināti par viņu iegādāto un izmantoto produktu un pakalpojumu drošības īpašībām. Kiberdrošības augstie standarti uzlabotu arī konkurētspēju. Tā rezultātā tiktu uzlabota noturība, jo IKT produkti un pakalpojumi tiktu oficiāli novērtēti saskaņā ar noteiktu kiberdrošības standartu kopumu, kuru var izstrādāt ciešā saistībā ar pašlaik notiekošo plašāko darbu pie IKT standartiem[20].

Satvara shēmas būtu brīvprātīgi piemērojamas un neradītu nekādus tūlītējus regulatīvos pienākumus tirgotājiem vai pakalpojumu sniedzējiem. Shēmas nebūtu pretrunā piemērojamām juridiskajām prasībām, piemēram, ES tiesību aktiem par datu aizsardzību.

Tiklīdz satvars būs izstrādāts, Eiropas Komisija uzaicinās attiecīgās ieinteresētās personas pievērst galveno uzmanību trim prioritārajām jomām:

- drošība kritiskās vai augsta riska līmeņa lietotnēs[21]: sistēmas, no kurām ir atkarīga mūsu ikdienas dzīve, no mūsu automobiļiem līdz rūpnīcu iekārtām vai no lielākajām sistēmām, piemēram, lidmašīnām vai spēkstacijām, līdz mazākajām, piemēram, medicīniskajām ierīcēm, kļūst aizvien vairāk digitalizētas un savstarpēji saistītas. Tādēļ IKT pamata sastāvdaļām šādos produktos un sistēmās būtu nepieciešams rūpīgs drošības novērtējums;

- kiberdrošība plaši izmantotos digitālajos produktos, tīklos, sistēmās un pakalpojumos, kurus izmanto gan privātajā, gan valsts sektorā, lai aizsargātos pret uzbrukumiem un izpildītu tiesību aktos noteiktos pienākumus[22], – piemēram, e-pasta šifrēšana, ugunsmūri un virtuālie privātie tīkli; ir ļoti svarīgi, lai šādu rīku arvien plašākā izmantošana neradītu jaunus riska avotus vai ievainojamību;

- integrētās drošības metožu izmantošana zemu izmaksu digitālās, savstarpēji savienotās plaša patēriņa ierīcēs, kas veido lietu internetu: saskaņā ar satvaru shēmas var norādīt uz to, ka produkti ir ražoti, izmantojot drošas jaunākās izstrādes metodes, ka to drošība ir pienācīgi pārbaudīta un ka tirgotāji ir apņēmušies atjaunināt savu programmatūru gadījumā, ja tiek atklāta jauna ievainojamība vai apdraudējums.

Šajās prioritātēs sevišķa uzmanība būtu jāpievērš progresējošai kiberdrošības apdraudējuma situācijai, kā arī pamatpakalpojumu, piemēram, transporta, enerģētikas pakalpojumu, veselības aprūpes, banku pakalpojumu, finanšu tirgu infrastruktūru, dzeramā ūdens vai digitālās infrastruktūras nozīmībai[23].

Lai arī nevienam IKT produktam, sistēmai vai pakalpojumam nevar garantēt "100 %" drošību, ir vairāki labi zināmi un dokumentēti trūkumi IKT produktu izstrādē, kurus var izmantot kā uzbrukumu mērķus. Integrētās drošības pieeja, kuru izmanto savienoto ierīču, IT

---

[19] Ticamības līmenis norāda uz drošības novērtējuma precizitātes pakāpi, un tas parasti ir proporcionāls riska līmenim saistībā ar darbības jomām vai funkcijām (t. i., augstāks ticamības līmenis ir nepieciešams IKT produktiem vai pakalpojumiem, kurus izmanto augsta riska darbības jomās vai funkcijās).

[20] COM(2016) 176.

[21] Izņēmums būtu gadījumi, kad obligāto vai brīvprātīgo sertifikāciju regulē citi Savienības tiesību akti.

[22] Piemēram, Direktīvā (ES) 2016/1148, Regulā (ES) 2016/679, Direktīvā (ES) 2015/2366 un citos ierosinātajos tiesību aktos, piemēram, Eiropas Elektronisko sakaru kodeksā, ir noteiktas prasības organizācijām īstenot piemērotus drošības pasākumus, lai novērstu attiecīgus kiberdrošības riskus.

[23] Nozares Eiropas Parlamenta un Padomes Direktīvas 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā tvērumā.

programmatūras un aprīkojuma ražotāji, nodrošinātu kiberdrošību, vēl pirms jaunie produkti nonāk pārdošanā. Tā var būt daļa no rūpības pienākuma principa. Šī pieeja ir jāturpina attīstīt kopā ar nozari, un tā varētu samazināt produkta/programmatūras ievainojamību, piemērojot dažādas metodes — no projektēšanas līdz testēšanai un pārbaudei, tostarp oficiālu pārbaudi attiecīgā gadījumā, uzturēšanu ilgtermiņā, drošu dzīves cikla attīstības procesu izmantošanu, kā arī jauninājumu un ielāpu izstrādi, lai reaģētu uz iepriekš neatklātu ievainojamību, un ātru atjaunināšanu un labošanu[24]. Tas arī palielinātu patērētāju uzticēšanos digitālajiem produktiem.

Turklāt ir jāapzinās trešo pušu drošības pētnieku svarīgā loma ievainojamības atklāšanā esošajos produktos un pakalpojumos, un dalībvalstīs jārada apstākļi, kas nodrošina koordinētu ievainojamības atklāšanu[25], pamatojoties uz labāko praksi[26] un attiecīgajiem standartiem[27].

Tajā pašā laikā **specifiskām nozarēm** ir jārisina specifiskas problēmas, un vajadzētu tās mudināt izstrādāt savu pieeju. Tādējādi vispārējās kiberdrošības stratēģijas tiktu papildinātas ar specifiskām nozaru kiberdrošības stratēģijām, piemēram, finanšu pakalpojumu[28], enerģētikas, transporta un veselības aprūpes jomās[29].

Komisija jau ir noteikusi specifiskus jautājumus par **atbildību** saistībā ar jaunajām digitālajām tehnoloģijām[30], un notiek darbs pie ietekmes analīzes; nākamie pasākumi ir paredzēti 2018. gada jūnijā. Kiberdrošība raisa jautājumus par uzņēmumiem un piegādes ķēdēm radušos zaudējumu attiecināmību, un šo jautājumu nerisināšana kavēs spēcīga kiberdrošības produktu un pakalpojumu vienotā tirgus attīstību.

Visbeidzot, ES vienotā tirgus attīstība arī ir atkarīga no kiberdrošības iekļaušanas tirdzniecības un investīciju politikā. Ārvalstu veiktās iegādes ietekme uz kritiskajām tehnoloģijām — kuras svarīgs piemērs ir kiberdrošība — ir galvenais aspekts satvarā par **ārvalstu tiešo investīciju Eiropas Savienībā pārbaudi**[31], kura mērķis ir veikt trešo valstu investīciju pārbaudi, pamatojoties uz drošību un sabiedrisko kārtību. Līdzīgā veidā kiberdrošības prasības jau ir radījušas ES preču un pakalpojumu tirdzniecības šķēršļus vairākās svarīgās trešo valstu ekonomikas nozarēs. ES kiberdrošības sertifikācijas satvars turpinās nostiprināt Eiropas pozīciju starptautiski, kuru vajadzētu papildināt ar nepārtrauktiem centieniem augstu globālo drošības standartu izstrādē un savstarpējās atzīšanas līgumu noslēgšanu.

---

[24] Kiberdrošība Eiropas digitālajā vienotajā tirgū, augsta līmeņa zinātnisko padomdevēju grupa, 2017. gada marts.

[25] Koordinēta ievainojamības atklāšana ir sadarbības veids, kas ļauj drošības pētniekiem ziņot par ievainojamību informācijas sistēmas īpašniekam vai tirgotājam, dodot organizācijai iespēju identificēt un pareizi un savlaicīgi novērst ievainojamību, pirms detalizēta informācija par ievainojamību tiek izpausta trešajām pusēm vai sabiedrībai.

[26] Piemēram, Labas prakses rokasgrāmata par ievainojamību atklāšanu. No izaicinājumiem līdz ieteikumiem, *ENISA*, 2016. gads.

[27] ISO/IEC 29147:2014 Informācijas tehnoloģija -- Drošības tehnikas -- Ievainojamības atklāšana.

[28] Komisijas nākamais uzdevums finanšu tehnoloģiju jomā ietvers finanšu nozares kiberdrošību.

[29] Piemēram, enerģētikas nozarē tiek apvienotas ļoti vecas un pašas jaunākās informācijas tehnoloģijas, jo īpaši attiecībā uz reāllaika prasībām elektrotīkliem.

[30] COM(2017) 228.

[31] COM(2017) 478.

2.3. Direktīvas par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā pilnīga īstenošana

Lai gan galvenie rīki cīņā par kiberdrošību šobrīd ir dalībvalstu ziņā, ES atzīst nepieciešamību paaugstināt standartus. Liela mēroga kiberincidenti reti kad ietekmē tikai vienu dalībvalsti, jo tādi galvenie sektori kā banku nozare, enerģētika un transports tiek arvien vairāk globalizēti, kļūst digitāli atkarīgi un savstarpēji savienoti.

Direktīva par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā ("kiberdrošības direktīva") ir pirmais tiesību akts par kiberdrošību, kas aptver visu ES[32]. Tas ir izstrādāts, lai veidotu noturību, uzlabojot valstu kiberdrošības spējas, veicinot labāku sadarbību starp dalībvalstīm, un pieprasot svarīgu ekonomikas nozaru uzņēmumiem ieviest efektīvu riska pārvaldības praksi, kā arī ziņot par nopietniem incidentiem valsts iestādēm. Šie pienākumi attiecas arī uz trīs galveno interneta pakalpojumu veidu sniedzējiem: mākoņdatošanu, meklētājprogrammām un tiešsaistes tirdzniecības vietām. To mērķis ir spēcīgāka un sistemātiskāka pieeja un uzlabota informācijas plūsma.

ES kibernoturības nodrošināšanai ir svarīgi, lai visas dalībvalstis pilnībā īstenotu direktīvu līdz 2018. gada maijam. Šo procesu atbalsta dalībvalstu kolektīvais darbs, kura rezultātā līdz 2017. gada rudenim tiks izdotas pamatnostādnes saskaņotākas īstenošanas veicināšanai, jo īpaši saistībā ar pamatpakalpojumu operatoriem. Komisija kā daļu no šīs kiberdrošības paketes izdod arī paziņojumu[33] , lai atbalstītu dalībvalstu centienus, sniedzot dalībvalstu labākās prakses piemērus saistībā ar direktīvas īstenošanu un ieteikumiem par to, kā direktīvai būtu jādarbojas praksē.

Informācijas plūsma ir joma, kurā direktīvai ir nepieciešami papildinājumi. Piemēram, direktīva aptver tikai galvenos stratēģiskos sektorus, bet būtu loģiski, ja līdzīgu pieeju īstenotu visas ieinteresētās personas, kuras ir cietušas kiberuzbrukumā, lai varētu sistemātiski novērtēt ievainojamību un kibernoziedznieku piekļuves punktus. Turklāt pastāv vairāki šķēršļi sadarbībai un informācijas apmaiņai starp valsts un privāto sektoru. Valdības un valsts sektora iestādes nevēlas apmainīties ar informāciju, kas saistīta ar kiberdrošību, baidoties apdraudēt valsts drošību vai konkurētspēju. Privātie uzņēmumi nevēlas apmainīties ar informāciju par savu kiberievainojamību un no tās izrietošajiem zaudējumiem, baidoties izpaust sensitīvu komerciālo informāciju, riskēt ar savu reputāciju vai datu aizsardzības noteikumu pārkāpšanu[34]. Publiskajā un privātajā partnerībā ir jānostiprina uzticēšanās, lai liktu pamatus plašākai sadarbībai un informācijas apmaiņai starp lielāku skaitu nozaru. Informācijas apmaiņas un analīzes centru loma ir jo īpaši svarīga, lai veidotu nepieciešamo uzticēšanos informācijas apmaiņai starp privāto un publisko sektoru. Ir veikti pirmie pasākumi attiecībā uz specifiskiem kritiskajiem sektoriem, piemēram, aviāciju, izveidojot Eiropas Aviācijas drošības aģentūru[35], un enerģētiku, veidojot informācijas apmaiņas un analīzes centrus[36].

---

[32] Eiropas Parlamenta un Padomes Direktīva 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

[33] COM(2017) 476.

[34] Kiberdrošība Eiropas digitālajā vienotajā tirgū, augsta līmeņa zinātnisko padomdevēju grupa, 2017. gada marts. Komercnoslēpumi ir specifisks jautājums, attiecībā uz kuru 2016. gada jūlija paziņojumā "Kā nostiprināt Eiropas Kiberizturētspējas sistēmu " norādīta nevēlēšanās ziņot par komercnoslēpumu kiberzādzību un nepieciešamība pēc uzticamiem ziņošanas kanāliem, kuri nodrošina konfidencialitāti.

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

[36] Tās ir bezpeļņas, pašiniciatīvas organizācijas, kuras veido privāti un valsts sektora uzņēmumi, lai apmainītos ar informāciju par kiberdraudiem, risku, novēršanu, mazināšanu un reaģēšanu. Skatīt, piemēram, Eiropas Enerģētikas informācijas apmaiņas un analīzes centrus (http://www.ee-isac.eu).

Komisija pilnībā atbalstīs šo pieeju ar *ENISA* palīdzību, lai ātrāk panāktu nepieciešamo progresu nozarēs, kas sniedz pamatpakalpojumus, kā noteikts kiberdrošības direktīvā.

2.4. Noturība, ko nodrošina ātra ārkārtas reaģēšana

Ja notiek kiberuzbrukums, ātra un efektīva reaģēšana var mazināt tā ietekmi. Tā var arī pierādīt, ka valsts sektora iestādes nav bezpalīdzīgas pret kiberuzbrukumiem, un var veicināt uzticēšanos. Attiecībā uz ES iestāžu reaģēšanu vispirms kiberdrošības aspekti būtu jāintegrē esošajos ES krīžu pārvarēšanas mehānismos, proti, integrētajos ES krīzes situāciju politiskās reaģēšanas mehānismos, kurus koordinē Padomes prezidentūra[37], un ES vispārējās agrīnās brīdināšanas sistēmās[38]. Nepieciešamība reaģēt uz īpaši nopietnu kiberincidentu vai uzbrukumu var būt pietiekams pamatojums tam, lai dalībvalsts varētu iedarbināt ES solidaritātes klauzulu[39].

Ātra un efektīva reaģēšana ir atkarīga arī no ātras informācijas apmaiņas mehānisma starp visiem galvenajiem dalībniekiem valstu un ES līmenī, kam savukārt ir nepieciešama skaidrība par dalībnieku lomām un pienākumiem. Komisija ir sniegusi konsultācijas iestādēm un dalībvalstīm par plānu, kas nodrošinātu efektīvu procesu efektīvai reaģēšanai Savienības un dalībvalstu līmenī uz liela mēroga kiberincidentiem. **Plānā**[40], kas kā ieteikums ietverts šajā paketē, ir izskaidrots, kā kiberdrošību integrē esošajos krīzes pārvarēšanas mehānismos ES līmenī, un tajā ir noteikti mērķi un sadarbības veidi starp dalībvalstīm, kā arī starp dalībvalstīm un attiecīgajām ES iestādēm, dienestiem, aģentūrām un struktūrām,[41] ja nākas reaģēt uz liela mēroga kiberincidentiem un krīzēm. Ieteikumā tiek arī izteikta prasība dalībvalstīm un ES iestādēm izstrādāt ES satvaru reaģēšanai kiberdrošības krīzēs, lai praktiski īstenotu plānu. Plāns tiks regulāri testēts kiberdrošības un citu krīžu pārvarēšanas praktiskajās nodarbībās[42] un attiecīgā gadījumā atjaunināts.

Ņemot vērā to, ka kiberincidenti var ievērojami ietekmēt ekonomikas funkcionēšanu un cilvēku ikdienas dzīvi, kā risinājumu var izskatīt iespēju izveidot **Kiberdrošības ātrās reaģēšanas fondu**, sekojot citu šādu krīzes pārvarēšanas mehānismu piemēram citās ES politikas jomās. Tas ļautu dalībvalstīm vērsties pēc palīdzības ES līmenī nopietna incidenta laikā vai pēc tā ar noteikumu, ka dalībvalsts ir ieviesusi pārdomātu kiberdrošības sistēmu pirms incidenta, ietverot pilnīgu kiberdrošības direktīvas īstenošanu un rūpīgi izstrādātus riska pārvaldības un uzraudzības satvarus valsts līmenī. Šāds fonds papildus esošajiem krīzes pārvarēšanas mehānismiem ES līmenī varētu izvērst ātrās reaģēšanas spējas solidaritātes interesēs un finansēt specifiskas ārkārtas reaģēšanas darbības, piemēram, uzbrukuma skartā aprīkojuma nomaiņu vai riska mazināšanas vai reaģēšanas instrumentu izmantošanu, turklāt ar ES civilās aizsardzības mehānisma palīdzību varētu izmantot valstu zinātību.

2.5. Kiberdrošības zināšanu tīkls ar Eiropas kiberdrošības pētniecības un zināšanu centru

Kiberdrošības tehnoloģiskie rīki ir stratēģiskie līdzekļi, kā arī galvenās izaugsmes tehnoloģijas nākotnē. ES stratēģiskajās interesēs ir nodrošināt to, ka ES saglabā un attīsta

---

[37] Tas ļauj augstākajā politiskajā līmenī koordinēt reaģēšanu liela mēroga krīžu gadījumos, kas skar vairākas nozares.

[38] Tas dod iespēju iekšējās informācijas apmaiņai un koordinēšanai attiecībā uz radušos krīzi, kas skar vairākas nozares, vai paredzamu vai nenovēršamu apdraudējumu, kuram nepieciešama rīcība ES līmenī.

[39] Saskaņā ar Līguma par Eiropas Savienības darbību 222. pantu.

[40] C(2017) 6100.

[41] Ietverot Eiropolu, *ENISA*, ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienību (*CERT-EU*) un ES Izlūkdatu analīzes centru (*INTCEN*).

[42] Piemēram, *ENISA* pārziņā: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

nepieciešamās spējas, lai nodrošinātu tās digitālo ekonomiku, sabiedrību un demokrātiju, aizsargātu kritisko aparatūru un programmatūru un sniegtu galvenos kiberdrošības pakalpojumus.

Valsts un privātā sektora partnerība kiberdrošības jautājumos[43], kas tika izveidota 2016. gadā, bija svarīgs pirmais solis, nodrošinot investīcijas līdz EUR 1,8 miljardu apmērā līdz 2020. gadam. Tomēr plānotais investīciju apmērs citās pasaules daļās[44] rosina domāt, ka ES ir jādara vairāk investīciju ziņā un jāpārvar spēju sadrumstalotība visā ES teritorijā.

ES var nodrošināt pievienoto vērtību, ņemot vērā kiberdrošības tehnoloģijas sarežģītību, nepieciešamās lielās investīcijas un nepieciešamību rast risinājumus, kas darbojas visā ES. Turpinot iesākto dalībvalstu un valsts un privātā sektora partnerības darbu, nākamais solis būtu ES kiberdrošības spēju nostiprināšana, izmantojot **kiberdrošības zināšanu centru tīklu**[45]**,** kura pamatā būtu **Eiropas kiberdrošības pētniecības un zināšanu centrs**. Šis tīkls ar tā centru stimulētu kiberdrošības tehnoloģijas attīstību un izvēršanu un papildinātu centienus uzlabot spējas šajā jomā ES un valstu līmenī. Komisija sāks ietekmes novērtējumu, lai izskatītu pieejamās iespējas, tostarp iespēju izveidot kopuzņēmumu, kas būtu jāpaveic 2018. gadā.

Kā pirmo soli un pamatu nākotnes plāniem Komisija ierosinās īstenot izmēģinājuma posmu programmas "Apvārsnis 2020" ietvaros, lai palīdzētu apvienot valstu centrus tīklā, kas radītu jaunu impulsu kiberdrošības zināšanu un tehnoloģijas attīstībai. Šajā nolūkā tā plāno ierosināt īstermiņa finansējuma piešķiršanu EUR 50 miljonu apmērā. Šis solis papildinās pašreiz notiekošo valsts un privātā sektora partnerības kiberdrošības jautājumos īstenošanu.

Pētniecības centienu savstarpēja izmantošana un veidošana būtu tīkla pamatā un centra sākotnēji prioritārā joma. Lai atbalstītu rūpniecisko spēju attīstību, centrs varētu darboties kā spēju projekta vadītājs, kas var strādāt ar daudznacionāliem projektiem. Tas dotu papildu stimulu ES rūpniecības inovācijām un konkurētspējai globālā tvērumā nākamās paaudzes digitālo tehnoloģiju, tostarp mākslīgā intelekta, kvantu skaitļošanas, blokķēžu un drošas digitālās identitātes, izstrādē, kā arī nodrošinātu ES bāzētu uzņēmumu piekļuvi masveida datiem, kas viss kopā ir ļoti svarīgi aspekti kiberdrošībai nākotnē. Tāpat arī centrs balstītos uz ES darbu pie augstas veiktspējas skaitļošanas tehnikas infrastruktūras uzlabošanas: tas ir svarīgi liela datu apjoma analīzei, ātrai datu šifrēšanai un atšifrēšanai, identitātes pārbaudei, kiberuzbrukumu simulācijai un videomateriālu analīzei[46].

Zināšanu centru tīklam varētu būt arī iespējas atbalstīt nozari ar testēšanas un simulācijas palīdzību, kas liktu pamatus 2.2. punktā minētajai kiberdrošības sertifikācijai. Tā pilnīga iesaiste ES kiberdrošības darbībā nodrošinātu nepārtrauktu tā mērķu precizēšanu atbilstoši vajadzībām. Centra mērķis būtu ne tikai augstu kiberdrošības standartu noteikšana tehnoloģijas un kiberdrošības sistēmu jomā, bet arī profesionāļu augstākās klases prasmju attīstībā, nodrošinot risinājumus un paraugus valstu centieniem attīstīt digitālās prasmes. Šādā mērā tas arī nostiprinātu kiberdrošības spējas ES līmenī un izveidotu sinerģiju jo īpaši ar *ENISA*, *CERT-EU*, Eiropolu, potenciālo Kiberdrošības ātrās reaģēšanas fondu un valstu datordrošības incidentu reaģēšanas vienībām (*CSIRT*).

---

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

[44] ASV investēs 19 miljardus dolāru kiberdrošībā tikai 2017. gadā vien, kas ir par 35 % vairāk nekā 2016. gadā. Baltais nams, preses sekretāra birojs: 'Faktu lapa: kiberdrošības valsts rīcības plāns', 2016. gada 9. februāris.

[45] Tīkls ietvers arī dalībvalstīs izveidotos un plānotos kiberdrošības centrus, kuru dalībnieki būs sabiedriskās pētniecības organizācijas un laboratorijas.

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

Zināšanu tīkla darbs jo īpaši jākoncentrē uz to, ka trūkst spēju novērtēt pilsoņu, uzņēmumu un valdību izmantoto produktu un pakalpojumu **šifrēšanu** digitālā vienotā tirgus ietvaros. Spēcīga šifrēšana ir pamats drošām digitālās identifikācijas sistēmām, kurām ir noteicošā loma efektīvā kiberdrošībā[47]; tā garantē arī cilvēku intelektuālā īpašuma drošību un dod iespēju aizstāvēt pamattiesības, piemēram, vārda brīvību un personas datu aizsardzību, un nodrošina drošu komercdarbību tiešsaistē[48].

Tā kā ES civilās un aizsardzības kiberdrošības tirgiem ir kopīgi izaicinājumi[49] un divējāda lietojuma tehnoloģijas, kurām nepieciešama cieša sadarbība kritiskajās jomās, varētu izveidot tīkla un tā centra otro posmu kiberaizsardzības dimensijā, pilnībā ievērojot līguma noteikumus attiecībā uz kopējo drošības un aizsardzības politiku. Tāpat kā darbības koncentrēšana uz tehnoloģijām arī aizsardzības dimensija var dot ieguldījumu dalībvalstu sadarbībā kiberaizsardzības jomā, tostarp saistībā ar informācijas apmaiņu, situācijas apzināšanos, zinātības uzkrāšanu un reakcijas koordinēšanu un dalībvalstu kopējo spēju attīstības atbalstīšanu. Tā var kalpot arī kā platforma, dodot dalībvalstīm iespēju apzināt ES kiberaizsardzības prioritātes, izskatīt kopīgus risinājumus, dodot ieguldījumu kopēju stratēģiju izstrādē, veicinot kopēju apmācību kiberaizsardzībā, mācības un testēšanu Eiropas līmenī un atbalstot darbu pie kiberaizsardzības taksonomijas un standartiem, kurā centram ir atbalstoša un konsultatīva loma. Lai īstenotu iepriekšminētās darbības, centram vajadzētu darboties ciešā sadarbībā un pilnīgā papildināmībā ar Eiropas Aizsardzības aģentūru kiberaizsardzības jomā, kā arī ar *ENISA* — kibernoturības jomā. Aizsardzības dimensijā tiktu ņemts vērā process, kas ir sākts ar pārdomu dokumentu par Eiropas aizsardzības nākotni.

Kiberaizsardzībā nepieciešamais augstais noturības līmenis pieprasa specifisku mērķu izvirzīšanu pētniecības un tehnoloģiskajiem centieniem. Uzņēmumu izstrādātie kiberaizsardzības projekti vai tehnoloģijas var saņemt Eiropas Aizsardzības fonda finansējumu gan pētniecības, gan izstrādes posmam[50]. Šajā kontekstā īpaši svarīgas varētu būt specifiskās jomas, piemēram, uz kvantu tehnoloģijām balstītas šifrēšanas sistēmas, situācijas apzināšanās, biometriskās piekļuves kontroles sistēmas, attīstīta pastāvīga apdraudējuma (*Advanced Persistent Threats*) atklāšana vai datizrace. Augstā pārstāve, Eiropas Aizsardzības aģentūra un Komisija atbalstīs dalībvalstis attiecībā uz to jomu identificēšanu, kurās var apsvērt kopēju kiberdrošības projektu finansēšanu no Eiropas Aizsardzības fonda.

2.6. Spēcīgas ES kiberprasmju bāzes izveide

Kiberdrošībā ir spēcīgs izglītības aspekts. Efektīva kiberdrošība ir ļoti atkarīga no iesaistīto personu prasmēm. Bet tiek prognozēts, ka līdz 2022. gadam privātajā sektorā Eiropā trūks 350 000 profesionāļu ar kiberdrošības prasmēm[51]. Kiberdrošības izglītība būtu jāattīsta visos līmeņos, sākot ar regulāru kiberdrošības personāla apmācību, papildu kiberdrošības apmācību visiem IKT speciālistiem un jaunām, specifiskām kiberdrošības mācību programmām. Lai apmierinātu vajadzības pēc paātrinātas izglītības un apmācības, būtu jāizveido spēcīgi

---

47 Programmas "Apvārsnis 2020" ietvaros Eiropas Komisija noteiks jaunu "*Horizon*" balvas izaicinājumu, kura tvērumā EUR 4 miljoni tiks piešķirti labākajam inovatīvajam risinājumam par vienotām tiešsaistes autentifikācijas metodēm.

48 Kiberdrošība Eiropas digitālajā vienotajā tirgū, augsta līmeņa zinātnisko padomdevēju grupa, 2017. gada marts.

49 "Pētījums par sinerģijām starp civilo un aizsardzības kiberdrošības tirgu" (*Optimity*; *SMART* 2014-0059).

50 Jau tagad Eiropas aizsardzības nozares attīstības programma nosaka prioritāti kiberaizsardzības projektiem, un kiberaizsardzība būs viens no tematiem uzaicinājumam iesniegt priekšlikumus, kas tiks uzsākts 2018. gadā.

51 Pētījums par globālās informācijas drošības personālu, 2017. gads. Pasaules mērogā trūkst 1,8 miljoni profesionāļu.

akadēmisko zināšanu centri, , kas varētu orientēties pēc Eiropas kiberdrošības pētniecības un zināšanu centra un *ENISA*. Būtu jāpanāk, ka ir pašsaprotami IKT produktu un sistēmu izstrādē jau no paša sākuma ievērot drošības principus. Kiberdrošības izglītība būtu jāattiecina ne tikai uz IT profesionāļiem, bet arī jāintegrē citu jomu, piemēram, inženierzinātņu, uzņēmējdarbības vadības un jurisprudences mācību programmās, kā arī specifiskos nozaru izglītības virzienos. Visbeidzot, pamatskolu un vidējās izglītības iestāžu skolotāji un skolēni būtu jāiepazīstina ar kibernoziedzības un kiberdrošības jautājumiem digitālo kompetenču apguves laikā.

ES kopā ar dalībvalstīm arī būtu jādod ieguldījums šajā darbā, balstoties uz Digitālo prasmju un darbvietu koalīcijas darbu[52] un ieviešot, piemēram, māceklības shēmas kiberdrošībā maziem un vidējiem uzņēmumiem.

2.7. Kiberhigiēnas un izpratnes veicināšana

Tiek apgalvots, ka aptuveni 95 % no incidentiem izraisa "sava veida cilvēciskā kļūda — ar nodomu vai bez tā"[53], tātad cilvēciskais faktors spēlē svarīgu lomu. Tādēļ ikviens ir atbildīgs par kiberdrošību. Tas nozīmē, ka jāmaina personīgā, uzņēmumu un valsts pārvaldes nostāja, lai ikviens apzinātos apdraudējumu un tā rīcībā būtu rīki un prasmes, kas ir nepieciešamas ātrai uzbrukumu atklāšanai un aktīvai aizsardzībai pret tiem. Cilvēkiem jāattīsta kiberhigiēnas paradumi, un uzņēmumiem un organizācijām jāievieš piemērotas, uz risku balstītas kiberdrošības programmas, kuras ir regulāri jāatjaunina, lai pielāgotos mainīgajai apdraudējuma situācijai.

Kiberdrošības direktīva ne tikai nosaka dalībvalstu pienākumus apmainīties ar informāciju par kiberuzbrukumiem ES līmenī, bet arī ieviest pārdomātas valstu kiberdrošības stratēģijas un sistēmas attiecībā uz tīkla un informācijas sistēmu drošību. Valstu pārvaldēm ES un valstu līmenī būtu jāturpina uzņemties vadošo lomu šo centienu virzīšanā uz priekšu.

Pirmkārt, dalībvalstīs būtu maksimāli jāpalielina kiberdrošības rīku pieejamība uzņēmumiem un privātpersonām. Jo īpaši būtu jāiegulda lielākas pūles, lai novērstu un mazinātu kibernoziedzības ietekmi uz galalietotājiem. Kā piemērs tam ir Eiropola darbs pie kampaņas "*NoMoreRansom*"[54], kas tika organizēta ciešā sadarbībā starp tiesībaizsardzības iestādēm un kiberdrošības uzņēmumiem, lai palīdzētu lietotājiem novērst inficēšanos ar izspiedējvīrusiem un atšifrēt datus, ja viņi ir kļuvuši par uzbrukuma upuriem. Šādas shēmas būtu jāizvērš arī pret citiem ļaunprogrammatūras veidiem citās jomās, un ES būtu jāizveido **vienots portāls, kas apkopotu visus šādus rīkus vienotā kontaktpunktā**, sniedzot konsultācijas lietotājiem par ļaunprogrammatūras novēršanu un atklāšanu un saites uz ziņošanas mehānismiem.

Otrkārt, dalībvalstīm būtu jāpaātrina **kiberdrošāku rīku izmantošana e-pārvaldes izstrādē** un pilnībā jāizmanto priekšrocības, ko sniedz kompetenču tīkls. Būtu jāveicina drošu identifikācijas līdzekļu ieviešana, pamatojoties uz ES regulējumu par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū, kas ir spēkā kopš 2016. gada un nodrošina paredzamu regulatīvo vidi drošai un vienotai elektroniskajai mijiedarbībai starp uzņēmumiem, privātpersonām un valsts sektora iestādēm[55].

---

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

[53] *IBM* "Kiberdrošības izlūkdatu rādītājs" 2014. gads, kas minēts Securitymagazine.com, 2014. gada 19. jūnijs.

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

[55] Regula (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū (*eIDAS* regula), kas tika pieņemta 2014. gada 23. jūlijā. Tāpat arī Eiropas Komisija nodrošina moduļus un rīkus *eID* un e-paraksta savietojamībai (piemēram, uzticamo sarakstu pārlūkus) Eiropas infrastruktūras savienošanas instrumenta programmas ietvaros.

Turklāt publiskajām iestādēm, jo īpaši tām, kuras sniedz pamatpakalpojumus, būtu jānodrošina to personāla apmācība ar kiberdrošību saistītās jomās.

Treškārt, dalībvalstīm būtu jānosaka kiberjautājumu izpratne kā prioritāte **izpratnes veicināšanas kampaņās**, tostarp kā mērķgrupu nosakot skolas, augstskolas, uzņēmējdarbības kopienu un pētniecības struktūras. Tiks palielināti komunikācijas centieni ES un dalībvalstu līmenī, lai kiberdrošības mēnesī, kas katru gadu notiek oktobrī un ko koordinē *ENISA,* sasniegtu plašāku auditoriju. Tikpat svarīga ir izpratnes veicināšana par tiešsaistes **dezinformācijas kampaņām un nepatiesām ziņām** sociālajos medijos, kas ir īpaši vērstas uz demokrātijas procesu un Eiropas vērtību graušanu. Lai arī primārā atbildība joprojām ir valsts līmenī – tostarp attiecībā uz Eiropas Parlamenta vēlēšanām –, ir pierādījies, ka zināšanu un pieredzes savstarpējai izmantošanai un apmaiņai Eiropas līmenī ir pievienotā vērtība attiecībā uz pasākumu mērķtiecīgu uzsākšanu[56].

Nozarei kopumā, bet jo īpaši digitālo pakalpojumu sniedzējiem un ražotājiem, arī ir svarīga loma. Tai ir jāatbalsta lietotāji (privātpersonas, uzņēmumi un valsts pārvalde) ar rīkiem, kas ļauj tiem pašiem uzņemties atbildību par savu darbību tiešsaistē, un tie skaidri jāinformē, ka kiberhigiēnas uzturēšana ir neatņemama daļa no piedāvājuma patērētājiem[57]. Lai atklātu un novērstu ievainojamību, nozarei būtu jācenšas ieviest iekšējos procesus, ar kuru palīdzību izpēta, kategorizē un novērš ievainojamības veidus neatkarīgi no tā, vai iespējamās ievainojamības avots atrodas konkrētā uzņēmuma iekšienē vai ārpus tā.

Galvenie pasākumi:

- direktīvas par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā pilnīga īstenošana;
- Eiropas Parlaments un Padome ātri pieņem regulu, kas nosaka jaunas pilnvaras *ENISA* un Eiropas satvaru sertifikācijai[58];
- Kopīga Eiropas Komisijas / nozares iniciatīva, lai noteiktu rūpības pienākuma principu produktu/programmatūras ievainojamības samazināšanai un "integrētās drošības" veicināšanai;
- plāna par reaģēšanu uz liela mēroga pārrobežu incidentiem ātra īstenošana;
- ietekmes novērtējuma uzsākšana, lai izpētītu iespēju 2018. gadā sagatavot Komisijas priekšlikumu par kiberdrošības zināšanu centru tīkla un Eiropas kiberdrošības pētniecības un zināšanu centra izveidi, balstoties uz tūlītēju izmēģinājuma posmu;
- palīdzības sniegšana dalībvalstīm to jomu apzināšanā, kurās no Eiropas Aizsardzības fonda varētu sniegt atbalstu kopējiem kiberdrošības projektiem;
- vienota Eiropas mēroga kontaktpunkta izveide, lai palīdzētu kiberuzbrukumu upuriem, sniegtu informāciju par jaunākajiem draudiem un apkopotu praktiskus padomus un kiberdrošības rīkus;
- dalībvalstu rīcība, integrējot kiberdrošību prasmju veidošanas programmās, e-pārvaldē un izpratnes veicināšanas kampaņās;
- nozares rīcība, nodrošinot ar kiberdrošību saistītu apmācību personālam un izmantojot "integrētās drošības" pieeju attiecībā uz saviem produktiem, pakalpojumiem un

[56] Piemērs tam ir Austrumu Stratēģiskās komunikācijas operatīvā grupa, kuru 2015. gadā izveidoja dalībvalstis un Augstā pārstāve, lai reaģētu uz notiekošajām Krievijas dezinformācijas kampaņām. Operatīvā grupa ir iesaistīta komunikācijas produktu un kampaņu izstrādē, kas vērsti uz ES politikas izskaidrošanu Austrumu partnerības reģionā.

[57] Vairāki ražotāji jau ir pieraduši pie "integrētās drošības" koncepcijas principiem, jo tie ir paredzēti dažos Eiropas tiesību aktos (piemēram, Direktīvā 2006/42/EK par mašīnām).

[58] COM(2017) 477.

procesiem.

3. EFEKTĪVAS ES SISTĒMAS IZVEIDE ATTURĒŠANAI NO KIBERNOZIEGUMIEM

Efektīva atturēšana nozīmē tādu pasākumu satvara izveide, kas būtu ticams un atturētu potenciālos kibernoziedzniekus un uzbrucējus no uzbrukumu veikšanas. Tik ilgi, kamēr kiberuzbrukumu veicēji — gan nevalstiski, gan valsts — baidīsies tikai no neizdošanās, viņiem nebūs motivācijas apturēt mēģinājumus. Efektīvāka tiesībaizsardzības iestāžu reakcija, koncentrējoties uz kriminālnoziedznieku atklāšanu, izsekojamību un kriminālvajāšanu, ir galvenais aspekts efektīvas atturēšanas nodrošināšanā. Turklāt ES ir nepieciešams atbalstīt dalībvalstis divējāda lietojuma kiberdrošības spēju attīstībā. Mēs sāksim mainīt notikumu gaitu saistībā ar kiberuzbrukumiem tikai tad, kad palielināsim iespējamību tikt pieķertam un sodītam par šo noziegumu veikšanu. Kiberuzbrukumi būtu nekavējoties jāizmeklē, un vainīgie būtu jāsauc pie atbildības, vai arī attiecīgi jārīkojas politiskā vai diplomātiskā līmenī. Lielas krīzes gadījumā, kura ir nozīmīga arī no starptautiskā un aizsardzības viedokļa, Augstā pārstāve varētu ierosināt Padomei piemērotas reakcijas variantus.

Viens solis ceļā uz to, lai uzlabotu krimināltiesisko reakciju uz kiberuzbrukumiem, tika jau sperts, pieņemot 2013. gada direktīvu par uzbrukumiem informācijas sistēmām[59]. Tajā tika noteikti minimālie noteikumi par kriminālpārkāpumu un sankciju definīciju uzbrukumu informācijas sistēmām jomā un operatīvie pasākumi sadarbības starp iestādēm uzlabošanai. Ar minēto direktīvu ir panākts ievērojams progress, nosakot krimināltbildību par kiberuzbrukumiem salīdzināmā līmenī visās dalībvalstīs, kas atvieglo pārrobežu sadarbību starp tiesībaizsardzības iestādēm, kuras izmeklē šādus pārkāpumus. Tomēr direktīvas potenciāls varētu tikt pilnībā izmantots, ja dalībvalstis pilnībā īstenotu visus tajā paredzētos noteikumus[60]. Komisija turpinās sniegt atbalstu dalībvalstīm direktīvas īstenošanā, un uzskata, ka pašlaik nav nepieciešams veikt tajā grozījumus.

3.1. Ļaunprātīgu personu identificēšana

Lai palielinātu mūsu iespējas saukt vainīgos pie atbildības, mums steidzami ir jāuzlabo savas spējas identificēt par kiberuzbrukumiem atbildīgās personas. Lielākais izaicinājums tiesībaizsardzības iestādēm ir kibernoziedzības izmeklēšanai noderīgas informācijas atrašana galvenokārt digitālas izsekošanas formā. Tādēļ ir nepieciešams palielināt mūsu tehnoloģiskās spējas veikt efektīvu izmeklēšanu, tostarp piesaistot Eiropola kibernoziedzības vienībai kiberdrošības ekspertus. Eiropols ir kļuvis par galveno dalībnieku, kas atbalsta dalībvalstis vairākjurisdikciju izmeklēšanā. Tam vajadzētu kļūt par specializēto zināšanu centru dalībvalstu tiesībaizsardzībā attiecībā uz izmeklēšanu tiešsaistē un kibernoziegumu tiesu ekspertīzi.

Plaši izplatītā prakse vienas IP adreses tvērumā reģistrēt vairākus lietotājus, dažkārt pat vairākus tūkstošus lietotāju, rada tehniskas grūtības izmeklēt ļaunprātīgu darbību tiešsaistē. Dažkārt rodas nepieciešamība pārbaudīt lielu skaitu lietotāju, lai identificētu vienu ļaunprātīgu personu, piemēram, tādos smagos noziegumos kā bērnu seksuālā izmantošana. Tādēļ ES mudinās ieviest jauno protokolu (*IPv6*), jo tas ļauj piešķirt vienai IP adresei vienu lietotāju, sniedzot nepārprotamas priekšrocības tiesībaizsardzības un kiberdrošības izmeklēšanā. Pirmais solis šajā virzienā būs tas, ka Komisija noteiks prasību pāriet uz *IPv6* visās

[59] Eiropas Parlamenta un Padomes Direktīva 2013/40/ES (2013. gada 12. augusts) par uzbrukumiem informācijas sistēmām.

[60] COM(2017) 474.

rīcībpolitikas jomās, tostarp attiecībā uz iepirkumiem un projektu un pētniecības finansējumu, kā arī sniegs atbalstu nepieciešamo mācību materiālu nodrošināšanai. Turklāt dalībvalstīm būtu jāapsver brīvprātīgu līgumu slēgšana ar interneta pakalpojumu sniedzējiem, lai virzītu pāreju uz *IPv6*.

Beļģija ir līderis pasaulē[61] *attiecībā uz ātrumu, kādā tā ievieš* IPv6*, arī pateicoties valsts un privātā sektora sadarbībai: attiecīgās ieinteresētās personas ir nolēmušas samazināt lietotāju skaitu vienai IP adresei līdz ne vairāk kā 16 lietotājiem, un tas notiek brīvprātīga pašregulējoša pasākuma ietvaros, kas motivē pāreju uz* IPv6[62].

Kopumā ir jāturpina veicināt atbildība par darbību tiešsaistē. Tas nozīmē tādu pasākumu veicināšanu, kas novērstu domēnu nosaukumu ļaunprātīgu izmantošanu nolūkā izplatīt nesankcionētus ziņojumus vai veiktu pikšķerēšanas uzbrukumus. Šajā nolūkā Komisija strādās, lai uzlabotu domēnu nosaukumu un *IP WHOIS*[63] sistēmu funkcionēšanu un tajos esošās informācijas pieejamību un precizitāti atbilstoši Piešķirto nosaukumu un numuru interneta korporācijas centieniem[64].

3.2. Tiesībaizsardzības reaģēšanas pastiprināšana

Efektīva kibernoziegumu **izmeklēšana** un **kriminālvajāšana** ir galvenais faktors, kas attur no kibernoziegumu veikšanas. Tomēr pašreizējā procesuālā sistēma ir labāk jāpielāgo interneta laikmetam[65]. Kiberuzbrukumu veikšanas ātrums var pārslogot mūsu procedūras, kā arī radīt konkrētu vajadzību pēc ātras pārrobežu sadarbības. Tādēļ, kā tika paziņots Eiropas Drošības programmas ietvaros, 2018. gada sākumā Komisija nāks klajā ar priekšlikumiem, lai **atvieglotu pārrobežu piekļuvi elektroniskajiem pierādījumiem**. Paralēli Komisija īsteno praktiskus pasākumus, lai uzlabotu pārrobežu piekļuvi elektroniskajiem pierādījumiem krimināllietu izmeklēšanā, kas ietver arī finansējumu pārrobežu sadarbības apmācībai, elektroniskas platformas izstrādi informācijas apmaiņai ES un tiesiskās sadarbības formu standartizēšanu dalībvalstīs.

Vēl viens šķērslis efektīvai kriminālvajāšanai ir atšķirīgās tiesu ekspertīzes procedūras, kuras izmanto elektronisko pierādījumu vākšanai kibernoziegumu izmeklēšanā dažādās dalībvalstīs. To varētu risināt, strādājot pie kopēju tiesu ekspertīzes standartu izveides. Turklāt tiesu ekspertīzes spējas ir jāpastiprina, lai sekmētu izsekojamību un attiecināmību. Viens no veidiem varētu būt tiesu ekspertīzes spēju attīstība Eiropolā, pielāgojot esošos budžeta un cilvēkresursus Eiropola Eiropas kibernoziedzības apkarošanas centrā, lai apmierinātu pieaugošo nepieciešamību pēc operatīvā atbalsta pārrobežu kibernoziegumu izmeklēšanā. Cits veids būtu iepriekš minētajā tehniskajā ievirzē attiecībā uz šifrēšanu pētīt, kā tās ļaunprātīga izmantošana rada būtiskas problēmas cīņā pret smagiem noziegumiem, tostarp terorismu un

---

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 Vaicājumu un atbilžu protokols, kuru plaši izmanto meklēšanai datubāzēs, kur atrodas dati par reģistrētiem lietotājiem vai tiem, kam piešķirts interneta resurss.

64 Piešķirto nosaukumu un numuru interneta korporācija (*ICANN*) ir bezpeļņas organizācija, kura ir atbildīga par vairāku ar interneta nosaukumvietām saistītu datubāzu uzturēšanas un ar tām saistīto procedūru koordinēšanu.

65 Piemēram, *Avalanche* robottīkla (virtuālais) centrālais komandas un kontroles serveris mainīja savus fiziskos serverus un domēnus ik pēc piecām minūtēm.

kibernoziegumiem. Komisija līdz 2017. gada oktobrim[66] darīs zināmus pašreizējo novērojumu rezultātus attiecībā uz **šifrēšanas lomu kriminālllietu izmeklēšanā**[67].

Ņemot vērā, ka internetam nav robežu, Eiropas Padomes piedāvātais starptautiskās sadarbības satvars **"Budapeštas Konvencija par kibernoziegumiem"**[68] sniedz dažādu valstu grupai iespēju izmantot optimālu tiesisko standartu dažādu valstu tiesību aktiem par kibernoziedzības apkarošanu. Pašlaik tiek izskatīta iespēja pievienot konvencijai protokolu[69], kas varētu nodrošināt arī iespēju rast risinājumu jautājumam par pārrobežu piekļuvi elektroniskajiem pierādījumiem starptautiskā kontekstā. Tā vietā, lai radītu jaunus starptautiskus juridiskos instrumentus attiecībā uz kibernoziedzības jautājumiem, ES aicina visas valstis izstrādāt piemērotus valstu tiesību aktus un censties sadarboties esošā starptautiskā regulējuma ietvaros.

Anonimizācijas rīku plašā pieejamība ļauj noziedzniekiem vieglāk paslēpties. **"Tumšais tīkls"**[70] ir pavēris jaunas iespējas noziedzniekiem piekļūt bērnu seksuālās izmantošanas materiāliem, narkotikām vai ieročiem, bieži vien ar niecīgu risku tikt pieķertiem[71]. Tas tagad ir arī galvenais kibernoziedzībā izmantoto rīku, piemēram, ļaunprogrammatūras un uzlaušanas rīku, avots. Kopā ar attiecīgajām ieinteresētājām personām Komisija analizēs valstu pieejas, lai rastu jaunus risinājumus. Eiropolam vajadzētu atvieglot un atbalstīt izmeklēšanu saistībā ar tumšo tīklu, novērtēt apdraudējumu un palīdzēt noteikt jurisdikciju un noteikt prioritāti augsta riska gadījumiem, un ES varētu būt vadošā loma starptautiskās darbības koordinēšanā[72].

Viena no kibernoziedzības jomām, kuras izplatība arvien pieaug, ir kredītkaršu datu vai citu elektronisku maksāšanas līdzekļu krāpnieciska izmantošana. Maksājumu dati, kurus iegūst, veicot kiberuzbrukumus tiešsaistes mazumtirgotājiem vai citiem likumīgiem uzņēmumiem, pēc tam tiek pārdoti tiešsaistē, un noziedznieki var tos izmantot krāpšanai[73]. Komisija nāk klajā ar priekšlikumu pastiprināt atturēšanas pasākumus, izmantojot **direktīvu par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem**[74]. Tās mērķis ir atjaunināt esošos noteikumus šajā jomā un stiprināt tiesībaizsardzības spēju apkarot šo noziedzības veidu.

---

[66] Astotais progresa ziņojums virzībā uz efektīvu un patiesu drošības savienību, 2017. gada 29. jūnijs (COM(2017) 354 *final*).

[67] Padomes prezidentūra, "Tieslietu un iekšlietu padomes 2016. gada 8. un 9. decembra sanāksmes rezultāti", Nr. 15391/16.

[68] Konvencija ir pirmais starptautiskais līgums par noziegumiem, kas pastrādāti internetā un citos datortīklos, un tajā īpaša uzmanība pievērsta autortiesību pārkāpumiem, ar datoru saistītai krāpšanai, bērnu pornogrāfijai un tīkla drošības pārkāpumiem. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. 2017. gadā 55 valstu valdības ir ratificējušas Eiropas Padomes Konvenciju par kibernoziegumiem vai pievienojušās tai.

[69] Darba uzdevums Budapeštas Konvencijas par kibernoziegumiem 2. papildu protokola projekta sagatavošanai, T-CY (2017)3.

[70] Tumšais tīkls sastāv no satura paralēlos tīklos, kuros izmanto internetu, bet ir nepieciešamas specifiskas programmatūras, konfigurācijas vai piekļuves atļauja. Tumšais tīkls ir neliela daļa no dziļā tīmekļa, kas ir meklētājprogrammās neindeksētā tīmekļa daļa.

[71] Vērā ņemams izņēmums ir nesenā divu lielāko kriminālā tumšā tīmekļa tirgu *AlphaBay* un *Hansa* aizturēšana: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[72] Eiropolam jau ir nozīmīga loma šajā jomā. Nesenu piemēru skatīt tīmekļa vietnē: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[73] Ieņēmumi no krāpšanas ir svarīgs organizētās noziedzības ienākumu avots, kas dod iespēju veikt citas krimināli sodāmas darbības, piemēram, terorismu, narkotiku tirdzniecību un cilvēku tirdzniecību.

[74] COM(2017) 489.

Ir jāuzlabo arī dalībvalstu tiesībaizsardzības iestāžu spējas izmeklēt kibernoziegumus, kā arī prokuroru un tiesnešu izpratne par tādiem noziegumiem un to izmeklēšanas iespējām, ko iespējamu dara kibertelpa. *Eurojust* un Eiropols dod ieguldījumu šā mērķa sasniegšanā un pastiprinātā koordinācijā, cieši sadarbojoties ar specializētām konsultantu grupām Eiropola Kibernoziedzības apkarošanas centrā un kibernoziedzības apkarošanas vienību vadītāju un kibernoziedzības jomā specializējušos prokuroru tīklu ietvaros. Komisija piešķirs finansējumu EUR 10,5 miljonu apmērā kibernoziedzības apkarošanai, galvenokārt tās **Iekšējās drošības fonda programmas policijai** ietvaros. Svarīgs elements ir apmācība, un Eiropas Kibernoziedzības apkarošanas apmācības un izglītības grupa ir izstrādājusi daudz noderīgu mācību materiālu. Ar Eiropas Savienības Tiesībaizsardzības apmācības aģentūras (*CEPOL*) atbalstu šie materiāli tiek plaši izmantoti tiesībaizsardzības profesionāļu apmācībā.

3.3. Valsts un privātā sektora sadarbība kibernoziedzības apkarošanā

Tradicionālo tiesībaizsardzības mehānismu efektivitāti ietekmē izaicinājumi, ko rada digitālā pasaule, kurai galvenokārt raksturīgas privātā īpašumā esošas infrastruktūras un daudz dažādu dalībnieku dažādās jurisdikcijās. Tā rezultātā sadarbība ar privāto sektoru, tostarp nozari un pilsonisko sabiedrību, ir ļoti svarīga valsts sektora iestādēm efektīvā noziedzības apkarošanā. Šajā kontekstā finanšu sektors arī ir svarīgs, un sadarbība ar to ir jāpastiprina. Piemēram, būtu jānostiprina finanšu izlūkošanas vienību[75] loma kibernoziedzības apkarošanā.

Dažas dalībvalstis jau ir veikušas galvenos pasākumus. Nīderlandē finanšu un tiesībaizsardzības iestādes cieši sadarbojas Elektroniskās noziedzības apkarošanas grupā, lai apkarotu krāpšanu tiešsaistē un kibernoziedzību. Vācijas Kibernoziedzības apkarošanas kompetences centrs darbojas kā operatīvais centrs tā dalībniekiem, lai apmainītos ar informāciju ciešā sadarbībā ar Vācijas federālo policiju un izstrādātu pasākumus, kas nodrošina aizsardzību pret kibernoziedzību. 16 dalībvalstīs[76] ir izveidoti kibernoziedzības apkarošanas izcilības centri, lai atvieglotu sadarbību starp tiesībaizsardzības iestādēm, akadēmiskajām aprindām un privātajiem partneriem labākās prakses, apmācības un spēju veidošanas attīstībai un apmaiņai.
Komisija atbalsta valsts un privātā sektora partnerības un sadarbības mehānismu izveidi tādu īpašu projektu kā "Tiešsaistes krāpniecības apkarošanas kibercentra un ekspertu tīkls"[77] ietvaros, kas īsteno informācijas apmaiņas modeli un standartu, lai analizētu un mazinātu elektroniskās noziedzības risku un krāpšanu tiešsaistē.

Kibernoziedzības kontekstā privātiem uzņēmumiem ir jāspēj apmainīties ar informāciju par konkrētiem incidentiem ar tiesībaizsardzības iestādēm, tostarp personas datiem, pilnībā ievērojot datu aizsardzības noteikumus. ES datu aizsardzības reforma, ko sāks piemērot 2018. gada maijā, nosaka kopīgu noteikumu kopumu, kurā paredzēti nosacījumi, ar kādiem tiesībaizsardzības iestādes un privātie uzņēmumi var sadarboties. Eiropas Komisija sadarbosies ar Eiropas Datu aizsardzības kolēģiju un attiecīgajām ieinteresētajām personām, lai apzinātu labāko praksi šajā jomā un attiecīgā gadījumā sniegtu norādes.

[75] Finanšu izlūkošanas vienības darbojas kā valsts līmeņa centri, kas saņem un analizē ziņojumus par aizdomīgiem darījumiem un citu informāciju, kura ir saistīta ar nelikumīgi iegūtu līdzekļu legalizāciju, saistītajiem predikatīvajiem nodarījumiem un terorisma finansēšanu, un izplata analīzes rezultātus.

[76] Austrija, Beļģija, Bulgārija, Kipra, Čehijas Republika, Igaunija, Francija, Vācija, Grieķija, Īrija, Lietuva, Polija, Rumānija, Slovēnija, Spānija un Apvienotā Karaliste.

[77] *EU-OF2CEN* iniciatīvas mērķis ir dot iespēju sistemātiskai, ES mēroga ar interneta krāpniecību saistītas informācijas apmaiņai starp bankām un tiesībaizsardzības dienestiem, lai novērstu maksājumus krāpniekiem un "naudas mūļiem" un lai veiktu izmeklēšanu un vainīgo kriminālvajāšanu. To līdzfinansē ES (Iekšējās drošības fonda programma policijai).

3.4. Spēcīgāka politiskā reakcija

Nesen pieņemtais **satvars vienotai ES diplomātiskai reakcijai uz ļaunprātīgām kiberdarbībām**[78] ("kiberdiplomātijas instrumentu kopums") nosaka veicamos pasākumus kopējās ārpolitikas un drošības politikas ietvaros, tostarp ierobežojošos pasākumus, kurus var izmantot, lai nostiprinātu ES reakciju uz darbībām, kas kaitē tās politiskajām, drošības un ekonomikas interesēm. Satvars ir svarīgs solis signalizējošo un reaģēšanas spēju veidošanā ES un dalībvalstu līmenī. Tas palielinās mūsu spēju signalizēt par ļaunprātīgām kiberdarbībām, lai ietekmētu potenciālo agresoru rīcību, tajā pašā laikā ņemot vērā nepieciešamību pēc samērīgas reakcijas. Attiecināmība uz valsts vai nevalstisko izpildītāju paliek suverēns politisks lēmums, kura pamatā ir izlūkdati no visiem avotiem. Pašlaik notiek satvara īstenošanas darbs ar dalībvalstīm, un tas tiks turpināts saskaņā ar plānu reaģēšanai uz liela mēroga kiberincidentiem[79]. *INTCEN*[80], cieši sadarbojoties ar dalībvalstīm un ES iestādēm, būtu jāapkopo, jāanalizē un jākopīgo informācija par situāciju, kas nepieciešama satvara pasākumu izmantošanai.

3.5. Kibernoziedzības atturēšanas veicināšana, izmantojot dalībvalstu aizsardzības spējas

Dalībvalstis jau strādā pie kiberaizsardzības spēju attīstības. Turklāt, ņemot vērā robežu saplūšanu starp kiberaizsardzību un kiberdrošību un kiberrīku un tehnoloģiju divējādo izmantošanu, kā arī lielās atšķirības starp dalībvalstu pieejām, ES ir izdevīgā situācijā, lai palīdzētu sekmēt militāro un civilo centienu sinerģiju[81].

Dalībvalstis ar attīstītākām kiberdrošības spējām, kas vēlas tās apkopot, var apsvērt iespēju ar Augstās pārstāves, Komisijas un Eiropas Aizsardzības aģentūras atbalstu iekļaut kiberaizsardzību pastāvīgās strukturētās sadarbības (*PESCO*) satvarā. Šo iespēju varētu papildināt iepriekšminētie centieni sekmēt ES nozares spējas un stratēģisko autonomiju. ES var sekmēt arī sadarbspēju, tostarp veicinot spēju attīstību, koordinējot apmācības un izglītību un divējāda lietojuma standartizācijas centienus.

Vienotais satvars būtu jāizmanto pilnībā, lai reaģētu uz hibrīddraudiem, kas bieži ietver kiberuzbrukumus, un tas būtu jādara jo īpaši ar ES Hibrīddraudu analīzes vienības un nesen Helsinkos izveidotā Eiropas Centra hibrīddraudu novēršanai palīdzību, kuru uzdevums ir veicināt stratēģisko dialogu un veikt izpēti un analīzi.

ES no jauna pievērsīs uzmanību 2014. gada ES kiberaizsardzības politikas satvaram[82] — rīkam, ar kura palīdzību var turpināt kiberdrošības un aizsardzības integrāciju kopējā drošības un aizsardzības politikā (KDAP). KDAP misiju un operāciju kibernoturība pati par sevi ir būtiska: tiks izstrādātas standartizētas procedūras un attīstītas tehniskās spējas, ar kurām varētu atbalstīt gan izvietotās civilās un militārās misijas un operācijas, gan arī to attiecīgās plānošanas un īstenošanas spēju struktūras un EĀDD informācijas tehnoloģiju pakalpojumu sniedzējus. Lai uzlabotu dalībvalstu sadarbību un labāk koordinētu ES centienus šajā jomā, Eiropas Aizsardzības aģentūra un EĀDD sadarbībā ar Komisijas dienestiem sekmēs dalībvalstu kiberaizsardzības politikas veidotāju iesaisti stratēģiskā līmenī. ES arī atbalstīs Eiropas kiberdrošības risinājumu izstrādi, kas ir daļa no tās centieniem Eiropas aizsardzības

[78] http://www.consilium.europa.eu/lv/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.
[79] C(2017) 6100.
[80] JOIN(2016) 018 *final*.
[81] ES izpratnē kibertelpa ir sauszemes, gaisa un jūras operāciju darbības sfēra. Kiberdrošības centieni ietver arī kosmosa resursu un ar tiem saistītās infrastruktūras uz zemes aizsardzību un noturības veidošanu.
[82] www.consilium.europa.eu/lv/workarea/downloadasset.aspx?id=40802190515.

tehniskā un rūpnieciskā pamata jomā. Tas ietver arī reģionālo izcilības kopu sekmēšanu kiberdrošības un aizsardzības jomā.

Ciešā sadarbībā ar EĀDD, dalībvalstīm un citām ES struktūrām Komisijas dienesti līdz 2018. gadam izveidos **kiberaizsardzības apmācību un izglītības platformu**, lai novērstu pašreizējo prasmju trūkumu kiberaizsardzībā. Tas papildinās Eiropas Aizsardzības aģentūras darbu šajā jomā, palīdzot novērst pašreizējo prasmju trūkumu kiberdrošībā un kiberaizsardzībā.

Galvenie pasākumi:

- Komisijas iniciatīva pārrobežu piekļuves elektroniskajiem pierādījumiem nodrošināšanai (2018. gada sākums);
- Eiropas Parlaments un Padome ātri pieņem ierosināto direktīvu par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem ;
- prasību attiecībā uz *IPv6* ieviešana ES iepirkumu, pētniecības un projektu finansēšanas jomā; brīvprātīgi nolīgumi starp dalībvalstīm un interneta pakalpojumu sniedzējiem, lai mudinātu pāriet uz *IPv6*;
- atjaunota/paplašināta Eiropola koncentrēšanās uz kibernoziegumu tiesu ekspertīzi un tumšā tīkla uzraudzību;
- satvara vienotai ES diplomātiskai reakcijai uz ļaunprātīgām kiberdarbībām īstenošana;
- palielināts finansiālais atbalsts valstu un starpvalstu projektiem krimināltiesību uzlabošanai kibertelpā;
- ar kiberdrošību saistītas izglītības platforma, lai novērstu pašreizējo prasmju trūkumu kiberdrošībā un kiberaizsardzībā, 2018. gadā.

4. STARPTAUTISKĀS SADARBĪBAS KIBERDROŠĪBAS JOMĀ STIPRINĀŠANA

Pamatojoties uz tādām ES pamatvērtībām un pamattiesībām kā vārda brīvība un tiesības uz privātumu un personas datu aizsardzību, kā arī atvērtas, brīvas un drošas kibertelpas nodrošināšana, ES starptautiskā kiberdrošības politika ir izstrādāta tā, lai reaģētu uz nepārtraukti pieaugošajiem izaicinājumiem nodrošināt globālo kiberstabilitāti un dotu ieguldījumu Eiropas stratēģiskajai autonomijai kibertelpā.

4.1. Kiberdrošība ārējās attiecībās

Pierādījumi liecina, ka cilvēki visā pasaulē ierindo citu valstu kiberuzbrukumus galveno valsts drošības apdraudējumu vidū[83]. Ņemot vērā apdraudējuma globālo raksturu, spēcīgu apvienību un partnerību veidošana un uzturēšana ar trešajām valstīm ir svarīga kiberuzbrukumu novēršanā un atturēšanā no tiem — un tas kļūst par arvien svarīgāku aspektu starptautiskajai stabilitātei un drošībai. ES noteiks prioritāti konfliktu novēršanas un kibertelpas stabilitātes nodrošināšanas stratēģiskā satvara izveidei tās divpusējā, reģionālā, daudzu ieinteresēto personu un daudzpusējā iesaistē.

ES stingri atbalsta pozīciju par to, ka starptautiskās tiesības, jo īpaši ANO Harta, attiecas uz kibertelpu. Kā papildinājumu saistošajiem starptautiskajiem tiesību aktiem ES atbalsta brīvprātīgas, nesaistošas normas, noteikumus un principus par atbildīgu valsts rīcību, ko ir skaidri formulējusi ANO Valdības ekspertu grupa[84]; tā arī mudina veikt reģionālās

[83] 2017. gada pavasaris, Globālās attieksmes aptauja, *Pew Research Centre.*
[84] A/68/98 un A/70/174.

uzticamības veicināšanas pasākumu izstrādi un īstenošanu gan Eiropas Drošības un sadarbības organizācijā, gan citos reģionos.

Divpusējā līmenī dialogi par kiberjautājumiem[85] tiks attīstīti tālāk un papildināti ar centieniem atvieglot sadarbību ar trešajām valstīm, lai nostiprinātu pienācīgas rūpības principus un valsts atbildību par notiekošo kibertelpā. Savās starptautiskajās saistībās ES noteiks prioritāti starptautiskās drošības jautājumiem kibertelpā, nodrošinot arī to, ka kiberdrošība nekļūst par ieganstu tirgus protekcionismam un pamattiesību un brīvību, tostarp vārda brīvības un informācijas pieejamības, ierobežošanai. Visaptveroša pieeja kiberdrošībai pieprasa cilvēktiesību ievērošanu, un ES turpinās uzturēt savas pamatvērtības globālā mērogā, pamatojoties uz ES Cilvēktiesību pamatnostādnēm par brīvību tiešsaistē[86]. Šajā ziņā ES uzsver visu ieinteresēto personu iesaistes interneta pārvaldībā nozīmi.

Komisija ir arī nākusi klajā ar priekšlikumu[87] ES eksporta kontroļu modernizēšanai, kas ietver kontroļu ieviešanu tādu kritisku kibernovērošanas tehnoloģiju eksportam, kas varētu izraisīt cilvēktiesību pārkāpumus vai tikt ļaunprātīgi izmantotas pret ES drošību; Komisija arī intensīvāk veidos dialogus ar trešām valstīm, lai sekmētu globālo konverģenci un atbildīgu rīcību šajā jomā.

4.2. Kiberdrošības spēju veidošana

Globālā kiberstabilitāte ir atkarīga no visu valstu vietējās un valsts līmeņa spējas novērst kiberincidentus un reaģēt uz tiem, kā arī veikt izmeklēšanu un kriminālvajāšanu kibernoziedzības gadījumos. Centienu stiprināt valsts noturību trešās valstīs atbalstīšana paaugstinās kiberdrošības līmeni pasaules mērogā un pozitīvi ietekmēs ES. Lai reaģētu uz strauji pieaugošajiem kiberdraudiem, ir nepieciešama apmācība, politikas un tiesību aktu izstrādes centieni, kā arī efektīvi funkcionējošas datorapdraudējumu reaģēšanas vienības un kibernoziedzības apkarošanas vienības visās pasaules valstīs.

Kopš 2013. gada ES ir līdere starptautiskās kiberdrošības spēju veidošanā, un tā sistemātiski sasaista šos centienus ar attīstības sadarbību. ES turpinās atbalstīt uz tiesībām balstītu spēju veidošanas modeli saskaņā ar *Digital4Development* pieeju[88]. Spēju veidošanas prioritāte tiks noteikta ES kaimiņvalstīm un jaunattīstības valstīm, kuras piedzīvo strauji augošu savienojamību un ātru draudu attīstību. ES centieni būs papildinājums ES attīstības programmai, ņemot vērā Ilgtspējīgas attīstības programmu 2030. gadam un kopējos centienus iestāžu spēju veidošanā.

Lai uzlabotu ES spēju mobilizēt kolektīvās zināšanas spēju veidošanas atbalstam, būtu jāizveido tam paredzēts ES kiberspēju veidošanas tīkls, kurā būtu iesaistīts EĀDD, dalībvalstu kiberdrošības iestādes, ES aģentūras, Komisijas dienesti, akadēmiskās aprindas un pilsoniskā sabiedrība. Tiks izstrādātas ES kiberspēju veidošanas pamatnostādnes, lai sniegtu labākas politiskās norādes un labāk noteiktu prioritātes ES centieniem attiecībā uz palīdzību trešām valstīm.

ES sadarbosies ar citiem līdzekļu devējiem šajā jomā, lai izvairītos no centienu pārklāšanās un veicinātu mērķtiecīgāku spēju veidošanu dažādos reģionos.

---

[85] ES 2017. gada septembrī bija divpusējas sarunas par kiberjautājumiem ar ASV, Ķīnu, Japānu, Korejas Republiku un Indiju.

[86] ES Cilvēktiesību pamatnostādnes par vārda brīvību tiešsaistē un bezsaistē.

[87] COM(2016) 616.

[88] SWD(2017) 157.

4.3. ES un NATO sadarbība

Pamatojoties uz jau sasniegto ievērojamo progresu, ES padziļinās ES un NATO sadarbību kiberdrošības, hibrīddraudu novēršanas un aizsardzības jomā, kā tas ir noteikts 2016. gada 8. jūlija kopīgajā deklarācijā[89]. Prioritātes cita starpā ir sadarbspējas sekmēšana ar saskaņotu kiberaizsardzības prasību un standartu palīdzību, sadarbības stiprināšana mācībās un praktiskajās nodarbībās un mācību prasību saskaņošana.

ES un NATO arī veicinās sadarbību kiberaizsardzības pētniecībā un inovācijās, pamatojoties uz pašreizējo tehnisko vienošanos par tādas informācijas apmaiņu starp attiecīgajām kiberdrošības iestādēm, kas saistīta ar kiberdrošību[90]. Nesen kopīgie centieni hibrīddraudu apkarošanā, jo īpaši sadarbība starp ES Hibrīddraudu analīzes vienību un NATO Hibrīddraudu analīzes nodaļu, būtu jāturpina, lai stiprinātu noturību un reaģēšanu uz kiberkrīzēm. ES un NATO sadarbība tiks turpināta, veicot kiberaizsardzības praktiskās nodarbības, kurās iesaistīsies EĀDD un citas ES struktūras, kā arī attiecīgās NATO iestādes, tostarp NATO Kopējais kiberaizsardzības izcilības centrs Tallinā. Pirmo reizi NATO un ES veiks paralēlas un koordinētas praktiskās nodarbības, reaģējot uz hibrīddraudu scenāriju, kurās NATO būs vadošā loma 2017. gadā, bet ES — 2018. gadā. Nākamajā ziņojumā par ES un NATO sadarbību, kas ir jāiesniedz attiecīgajām padomēm 2017. gada decembrī, tiks piedāvāta iespēja apsvērt turpmāku sadarbības paplašināšanu, nodrošinot kopējus, drošus un spēcīgus saziņas līdzekļus starp visām iesaistītajām iestādēm un struktūrām, tostarp *ENISA*.

Galvenie pasākumi:

- konfliktu novēršanas un kibertelpas stabilitātes nodrošināšanas stratēģiskā satvara uzlabošana;
- jauna spēju veidošanas tīkla izveide nolūkā atbalstīt trešo valstu spējas novērst kiberdraudus un ES Kiberdrošības spēju veidošanas pamatnostādņu izstrāde, lai labāk noteiktu ES centienu prioritātes;
- turpmāka ES un NATO sadarbība, tostarp dalība paralēlās un koordinētās praktiskā nodarbībās, un pastiprināta kiberdrošības standartu savietojamība.

5. NOBEIGUMS

ES sagatavotībai kiberjautājumu jomā ir centrālā loma digitālā vienotā tirgus un mūsu Drošības un aizsardzības savienības izveidē. Eiropas kiberdrošības pastiprināšana un reakcija uz civilo un militāro mērķu apdraudējumu ir absolūti nepieciešama.

Gaidāmais digitālais samits, kuru 2017. gada 29. septembrī organizē Igaunijas prezidentūra, dod iespēju demonstrēt kopējo apņemšanos likt kiberdrošību ES kā digitālas sabiedrības pamatā. Kopējo saistību ietvaros Komisija aicina dalībvalstis uzņemties saistības attiecībā uz to, kā tās paredz rīkoties jomās, kas ir to primārā atbildība. Šajās saistībās būtu jāietver kiberdrošības stiprināšana,

- pilnīgi un efektīvi īstenojot kiberdrošības direktīvu līdz 2018. gada 9. maijam, kā arī nodrošinot resursus, kas ir nepieciešami par kiberdrošību atbildīgajām valsts sektora iestādēm efektīvai savu uzdevumu veikšanai;
- piemērojot valstu pārvaldēm vienādus noteikumus, ņemot vērā to lomu sabiedrībā un ekonomikā kopumā;

[89] http://www.consilium.europa.eu/lv/press/press-releases/2016/07/08-eu-nato-joint-declaration/.

[90] *CERT-EU* un *NATO* datordrošības incidentu reaģēšanas spējas (*NCIRC*).

- nodrošinot ar kiberdrošību saistītas apmācības valsts pārvaldē;
- piešķirot prioritāti kiberdrošības situācijas izpratnes veicināšanai informatīvajās kampaņās un ietverot kiberdrošību akadēmiskās un arodapmācības mācību programmās;
- izmantojot iniciatīvas pastāvīgās strukturētās sadarbības (*PESCO*) un Eiropas Aizsardzības fonda ietvaros, lai atbalstītu kiberaizsardzības projektu izstrādi.

Šajā kopīgajā paziņojumā ir izklāstīts izaicinājumu tvērums un pasākumu kopums, ko ES var īstenot. Mums ir nepieciešama noturīga Eiropa, kas var efektīvi aizsargāt savus cilvēkus, iepriekš paredzot iespējamos kiberincidentus, nostiprinot aizsardzību tās struktūrās un darbībā, ātri atgūstoties no kiberuzbrukumiem un atturot to veicējus. Šajā paziņojumā ir ierosināti pārdomāti pasākumi, kas koordinētā veidā turpinās stiprināt ES kiberdrošības struktūras un spējas un nodrošinās pilnīgu sadarbību starp dalībvalstīm un attiecīgajām ES struktūrām, ievērojot to kompetences un atbildību. Tā īstenošana skaidri demonstrēs to, ka ES un dalībvalstis strādās kopā, lai ieviestu tādu kiberdrošības standartu, kas atbilst aizvien pieaugošajiem izaicinājumiem, ar ko pašlaik saskaras Eiropa.