EIROPAS
KOMISIJA

Briselē, 5.7.2016.
COM(2016) 410 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI

Kā nostiprināt Eiropas Kiberizturētspējas sistēmu

un sekmēt konkurētspējīgu un inovatīvu kiberdrošības nozari

1. IEVADS/KONTEKSTS

Kiberdrošības incidenti katru dienu rada ievērojamus ekonomiskus zaudējumus gan Eiropas uzņēmumiem, gan ekonomikai kopumā. Šādi incidenti mazina iedzīvotāju un uzņēmumu ticību digitālajai sabiedrībai. Komercnoslēpumu, komercinformācijas un personas datu zādzību, kā arī pakalpojumu, tostarp būtisku pakalpojumu, un infrastruktūras traucējumu rezultātā katru gadu rodas ekonomiskie zaudējumi simtiem miljardu eiro apmērā[1]. Tie var ietekmēt arī iedzīvotāju pamattiesības un sabiedrību kopumā.

2013. gada Eiropas Savienības kiberdrošības stratēģija[2] (ES kiberdrošības stratēģija) un tās galvenais rezultāts – Tīklu un informācijas drošības (TID) direktīva[3], kas drīzumā tiks pieņemta, un Direktīva 2013/40/ES par uzbrukumiem informācijas sistēmām ir līdz šim galvenie Eiropas Savienības politikas pasākumi šo kiberdrošības problēmu risināšanai. Bez tam ES rīcībā ir arī specializētas iestādes, piemēram, Eiropas Savienības Tīklu un informācijas drošības aģentūra (*ENISA*), Eiropola sastāvā esošais Eiropas Kibernoziedzības centrs (*EC3*) un datorapdraudējumu reaģēšanas vienība (*CERT-EU*). Nesen tika sāktas vairākas nozaru iniciatīvas (piemēram, enerģētikas un transporta jomā) nolūkā paaugstināt kiberdrošību dažādās svarīgās nozarēs.

Par spīti šiem atzīstamajiem sasniegumiem ES joprojām ir mazaizsargāta pret kiberincidentiem. Tie var apdraudēt digitālo vienoto tirgu un ekonomisko un sociālo dzīvi kopumā. Tiem var būt ne tikai ekonomiska ietekme. Hibrīddraudu gadījumā[4] kiberuzbrukumus var koordinēti īstenot kopā ar citām darbībām nolūkā destabilizēt valsti vai uzbrukt politiskām institūcijām.

Ņemot vērā iepriekš minēto, ES varētu būt sarežģīti risināt plaša mēroga kiberincidentu, kurā vienlaicīgi iesaistītas vairākas dalībvalstis. Sinerģijā ar paziņojumiem par hibrīddraudu apkarošanu un par Eiropas Drošības programmas īstenošanu[5] Komisija apsver rīcību mainīgajā kiberdrošības situācijā un izvērtē papildu pasākumus, kas var būt nepieciešami, lai uzlabotu ES kiberdrošības izturētspēju un reaģēšanu uz incidentiem.

Turklāt Komisija pievēršas arī kiberdrošības industriālajām spējām ES. Lai arī visu digitālo tehnoloģiju vērtību ķēdi nevar pārvaldīt Eiropā, ir nepieciešams vismaz saglabāt un attīstīt konkrētas būtiskas spējas. Tādu produktu piegāde un pakalpojumu sniegšana, kas nodrošina augstāko kiberdrošības līmeni, ir Eiropas kiberdrošības nozares iespēja, un tā varētu kļūt par spēcīgu priekšrocību konkurencē. Ir sagaidāms, ka pasaules kiberdrošības tirgus būs viens no visstraujāk augošajiem IKT nozares segmentiem[6]. Lai ES padarītu par šīs jomas vadošo spēlētāju, jābalstās uz spēcīgu datu drošības, tostarp personas datu drošības, kultūru un efektīvu reaģēšanu uz incidentiem. To uzskatīs par spēcīgu argumentu investēšanai ES,

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II; Center for Strategic and International Studies; 2014. gada jūnijs.*
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.
[6] Skatīt SWD(2016) 216.

tādējādi palīdzot sasniegt vērienīgos digitālā vienotā tirgus mērķus – veicināt izaugsmi un darbvietu radīšanu.

Ir nepieciešama stingra apņemšanās, lai sasniegtu iepriekš minēto, proti:

i) jāpastiprina sadarbība nolūkā palielināt gatavību un risināt kiberincidentus

Ir jāstiprina esošie un apstiprinātie sadarbības mehānismi, lai palielinātu ES izturētspēju un gatavību, tostarp iespējamai Eiropas mēroga kiberdrošības krīzei. Šiem sadarbības mehānismiem vajadzētu būt visaptverošiem un attiekties uz visu incidenta dzīves ciklu, sākot no prevencijas līdz kriminālprocesam. Efektīva dalībvalstu sadarbība un kritiskajiem operatoriem noteikto drošības prasību praktiska īstenošana no kiberdrošības nozares prasīs arī stabilus tehniskos risinājumus.

Tajā pašā laikā, lai visā ES nodrošinātu kritisko kiberobjektu izturētspēju, būs nepieciešami pastāvīgi centieni panākt starpnozaru sinerģiju un kiberdrošības prasības iekļaut visās attiecīgajās ES politikas jomās. Komisija izvērtēs nepieciešamību tuvākajā nākotnē atjaunināt 2013. gada ES kiberdrošības stratēģiju;

ii) jārisina problēmas, ar kurām saskaras Eiropas kiberdrošības vienotais tirgus

Digitālā vienotā tirgus (*DSM*) stratēģijā[7] ir norādīts, ka strauji mainīgajā tiešsaistes tīklu drošības tehnoloģiju un risinājumu jomā joprojām pastāv zināmi trūkumi. Vienlaikus tirgus pētījumi rāda, ka attiecībā uz kiberdrošības produktu piegādi un pakalpojumu nodrošināšanu ES iekšējais tirgus vēl aizvien ir ģeogrāfiski sadrumstalots[8]. Šajā paziņojumā ir izklāstīti vairāki uz tirgu orientēti politikas pasākumi šo vienotā tirgus trūkumu un problēmu risināšanai;

iii) jāsekmē industriālās spējas kiberdrošības jomā

ES kiberdrošības stratēģijā un *DSM* stratēģijā Komisija apņēmās veicināt plašāku ES kiberdrošības nozares produktu un pakalpojumu piedāvājumu. Tāpēc Komisija šobrīd pieņem arī lēmumu, ar kuru bruģēs ceļu noteikumiem par līgumisku publisko un privāto partnerību (*cPPP*) kiberdrošības jomā, ar ko centīsies sekmēt progresīvu Eiropas kiberdrošības pētījumu un inovāciju programmu nolūkā palielināt konkurētspēju.

2. SADARBĪBAS, ZINĀŠANU UN SPĒJU PACELŠANA JAUNĀ LĪMENĪ

ES kiberdrošības stratēģija un jo īpaši gaidāmā TID direktīva[9] pavērs iespējas uzlabot dalībvalstu savstarpējo sadarbību ES līmenī. Ņemot vērā pieaugošo ekonomiskās un sociālās dzīves digitalizāciju (ņemot vērā arī mākoņpakalpojumus, lietisko internetu un iekārtu savstarpējo komunikāciju), pārrobežu starpsavienojumu pieaugumu un strauji mainīgo ainu kiberdraudu jomā, ir ārkārtīgi svarīgi, lai direktīva tiktu īstenota ātri un efektīvi[10]. Šajā sakarā

[7] COM(2015) 192.
[8] Skatīt SWD(2016) 216.
[9] Ar TID direktīvu dalībvalstīm tiks noteikta prasība identificēt būtisko pakalpojumu operatorus tādās jomās kā enerģētika, transports, finanses un veselība, novērst kiberdrošības riskus un arī nodrošināt, ka konkrēti digitālo pakalpojumu sniedzēji veic atbilstošus pasākumus šādu risku novēršanai.
[10] Skatīt SWD(2016) 216.

ES jābūt gatavai iespējamai plaša mēroga kiberkrīzei[11], tostarp vienlaicīgiem uzbrukumiem kritiskām informācijas sistēmām vairākās dalībvalstīs[12].

Tāpēc, lai risinātu gan mazāka mēroga kiberincidentus (kas var izplatīties tālāk), gan arī iespējamus plaša mēroga kiberuzbrukumus vairākās dalībvalstīs, ir nepieciešams sadarboties ES līmenī. ES esošajos krīžu pārvarēšanas mehānismos jāintegrē kiberdrošības aspekti. Tāpat tai jānodrošina efektīva sadarbība un ātras informācijas apmaiņas mehānismi nozaru un dalībvalstu starpā, lai šādus incidentus risinātu un iegrožotu. Turklāt šiem mehānismiem vajadzētu darboties saskaņoti, tādējādi sniedzot ieguldījumu cīņā pret terorismu, organizēto noziedzību un kibernoziedzību. Šādi tiktu uzlabota arī ES spēja saskaņot savas darbības ar starptautiskajiem partneriem, efektīvi reaģējot uz globāliem apdraudējumiem un incidentiem.

2.1. Maksimāli efektīvs TID sadarbības mehānismu izmantojums un virzība uz *ENISA 2.0*

TID direktīvā prasīto valsts spēju būtisks elements ir datordrošības incidentu reaģēšanas vienības (*CSIRT*), kas ir atbildīgas par ātru reaģēšanu uz kiberdraudiem un kiberincidentiem. Tās veidos *CSIRT* tīklu, kura mērķis ir veicināt efektīvu operatīvo sadarbību konkrētu kiberdrošības incidentu gadījumā un dalīšanos ar informāciju par riskiem. Turklāt ar direktīvu tiks izveidota sadarbības grupa nolūkā atbalstīt un sekmēt stratēģisko sadarbību dalībvalstu starpā un veidot uzticēšanos starp tām.

Ņemot vērā kiberdraudu būtību un daudzveidību, Komisija aicina dalībvalstis pēc iespējas efektīvāk izmantot TID sadarbības mehānismus un uzlabot pārrobežu sadarbību attiecībā uz sagatavotību plaša mēroga kiberdrošības incidentam. Šādu papildu sadarbību nozīmīga kiberincidenta gadījumā uzlabotu tas, ja dažādajiem kiberekosistēmas elementiem būtu saskaņota pieeja sadarbībai krīzes situācijā. Šādu pieeju var noteikt plānā, kam būtu jānodrošina sinerģija un saskaņotība ar esošajiem krīžu pārvarēšanas mehānismiem[13]. Pēc tam to vajadzētu regulāri testēt kiberkrīzes un citās krīžu pārvarēšanas mācībās. Tajā būtu jāparedz, kāda loma būs tādām ES līmeņa struktūrām kā *ENISA, CERT-EU* un Eiropola sastāvā esošais Eiropas Kibernoziedzības centrs (*EC3*), un jāizmanto rīki, kas ir izstrādāti *CSIRT* tīkla ietvaros. Šādas sadarbības plānu Komisija 2017. gada pirmajā pusē iesniegs izskatīšanai sadarbības grupā, *CSIRT* tīklā un citu attiecīgo ieinteresēto personu starpā.

Šobrīd ES līmenī zināšanas un ekspertīze kiberdrošības jomā ir pieejami, bet tie ir izkliedēti un nestrukturēti. Lai atbalstītu TID sadarbības mehānismus, informācija būtu jāapkopo "informācijas centrā", lai visām dalībvalstīm tā būtu viegli pieejama pēc pieprasījuma. Šis "centrs" kļūtu par centrālo resursu, ļaujot ES institūcijām un dalībvalstīm attiecīgi apmainīties ar informāciju. Vieglāka piekļuve labāk strukturētai informācijai par kiberdrošības riskiem un iespējamajiem aizsardzības līdzekļiem palīdzētu dalībvalstīm palielināt savas spējas un saskaņot pieejas, tādējādi kopumā uzlabojot izturētspēju pret uzbrukumiem. Komisija, izmantojot *ENISA* un *CERT-EU* atbalstu un Kopīgā pētniecības centra zinātību, sekmēs šāda centra izveidi un nodrošinās tā ilgtspēju.

[11] Skatīt, piem., *ENISA* ziņojumu: *Common practices of EU-level crisis management and applicability to cyber crises*, 2016. gada aprīlis.
[12] Skatīt SWD(2016) 216.
[13] Jo īpaši integrētie krīzes situāciju politiskās reaģēšanas mehānismi, tostarp lēmums par noteikumiem attiecībā uz Komisijas veiktu solidaritātes klauzulas īstenošanu (2014. gada 24. jūlijs) un kopējās drošības un aizsardzības politikas lēmumu pieņemšanas procesi.

Turklāt ES līmenī būtu jāizveido pastāvīga augsta līmeņa padomdevēju grupa[14] kiberdrošības jautājumos; tā sastāvētu no nozares, akadēmisko aprindu, pilsoniskās sabiedrības un citu attiecīgu organizāciju ekspertiem un lēmumu pieņēmējiem. Šī grupa ļautu Komisijai atklātā un pārredzamā veidā iegūt ārēju ekspertīzi un ieguldījumu izmantošanai kiberdrošības stratēģijas politikas jomās un iespējamās regulējuma un citas sabiedriskās politikas darbībās. Tā papildinātu citas kiberdrošības struktūras un veidotu saites ar tām[15].

Turklāt Komisijai līdz 2018. gada 20. jūnijam ir jāveic *ENISA* novērtējums un līdz 2020. gada 19. jūnijam jāpieņem iespējamās izmaiņas *ENISA* pilnvarā vai arī tas jāpagarina[16]. Ņemot vērā pašreizējo kiberdrošības vidi, Komisijas mērķis ir iespējami agrāk veikt novērtēšanu un atkarībā no tās rezultātiem iespējami drīz nākt klajā ar priekšlikumu.

Izvērtējot iespējamo nepieciešamību grozīt *ENISA* pilnvaras, Komisija ņems vērā iepriekš izklāstītās kiberdrošības problēmas un kopējos centienus pastiprināt sadarbību un dalīšanos zināšanās. Šis process nodrošinās iespēju izvērtēt iespējamu aģentūras spēju un potenciāla palielināšanu, lai dalībvalstīm ilgtspējīgā veidā sniegtu atbalstu kiberdrošības izturētspējas sasniegšanā. Turklāt, izvērtējot *ENISA* pilnvaras, būtu jāņem vērā aģentūras jaunās atbildības jomas saskaņā ar TID direktīvu, jaunie politikas mērķi atbalstīt kiberdrošības nozari (*DSM* stratēģija un jo īpaši *cPPP*), mainīgās kritisko nozaru nodrošināšanas vajadzības un jaunās problēmas, kas saistītas ar pārrobežu incidentiem, tostarp saskaņotu reaģēšanu uz kiberkrīzēm.

Komisija veiks šādus pasākumus:

- 2017. gada pirmajā pusē iesniegs izskatīšanai sadarbības plānu plaša mēroga kiberincidentu risināšanai ES līmenī;
- veicinās "informācijas centra" izveidi, lai atbalstītu informācijas apmaiņu ES struktūru un dalībvalstu starpā;
- izveidos augsta līmeņa padomdevēju grupu kiberdrošības jautājumos, un
- līdz 2017. gada beigām pabeigs *ENISA* novērtēšanu. Šajā novērtējumā būs apskatīta nepieciešamība grozīt vai paplašināt *ENISA* pilnvaras, cenšoties iespējami drīz izstrādāt iespējamo priekšlikumu.

2.2. Pastiprināti centieni saistībā ar izglītību, apmācību un mācībām kiberdrošības jomā

Atbilstošas prasmes un apmācība, kas saistīta gan ar kiberdrošības incidentu novēršanu, gan ar to risināšanu un to ietekmes mazināšanu, ir daži no galvenajiem aspektiem kiberdrošības izturētspējas sasniegšanā.

Šobrīd *ENISA,* Eiropas Kibernoziedzības apkarošanas apmācības un izglītības grupai (*ECTEG*) sadarbībā ar Eiropola sastāvā esošo Eiropas Kibernoziedzības centru un Eiropas Policijas akadēmijai (*CEPOL*) ir svarīga loma spēju, tostarp kibernoziedzības kriminālistikas,

[14] Uz Komisijas ekspertu grupām attiecas horizontālie noteikumi, kas noteikti Komisijas Lēmumā C(2016)3301.
[15] Piemēram, TID platforma, *cPPP* kiberdrošības jomā un nozaru platformas, piemēram, Enerģētikas ekspertu platforma kiberdrošības jautājumos (*EECSP*). Tai vajadzētu veidot saikni arī ar austa līmeņa apaļā galda diskusiju, kas minēta paziņojumā par Eiropas rūpniecības digitalizāciju: COM(2016) 180.
[16] Regula (ES) Nr. 526/2013, ar ko atceļ Regulu (EK) Nr. 460/2004.

veidošanas atbalstā, izstrādājot rokasgrāmatas un organizējot apmācības un kiberdrošības mācības.

Tajā pašā laikā kibertelpa strauji attīstās, un tajā būtiska nozīme ir divējāda lietojuma spējām. Tāpēc, lai palielinātu ES izturētspēju un spējas reaģēt uz incidentiem, ir nepieciešams attīstīt civilmilitāro sadarbību un sinerģiju apmācību un mācību jomā.

Nolūkā apmierināt šīs vajadzības, kā arī turpināt ar TID direktīvas un ES kiberaizsardzības politikas satvara[17] pieņemšanu aizsākto Komisijas dienesti sadarbosies ar dalībvalstīm, Eiropas Ārējās darbības dienestu (EĀDD), *ENISA* un citām attiecīgajām ES struktūrām[18], lai izveidotu tādu izglītības, mācību un apmācības platformu kiberdrošības jomā, kas veicinās civilās un aizsardzības jomas apmācību sinerģiju.

Komisija veiks šādus pasākumus:

- cieši sadarbosies ar dalībvalstīm, *ENISA*, EĀDD un citām attiecīgajām ES struktūrām nolūkā izveidot apmācības platformu kiberdrošības jomā.

2.3. Starpnozaru atkarības un galvenās publiskās tīkla infrastruktūras izturētspēja

Novērtējot plaša mēroga kiberincidenta risku un ietekmi, svarīgs faktors ir pārrobežu un starpnozaru atkarību apmērs. Nopietns kiberincidents vienā nozarē vai vienā dalībvalstī var tieši vai netieši ietekmēt citas nozares vai dalībvalstis vai izplatīties uz tām.

Pārrobežu un starpnozaru sadarbība veicina informācijas un zinātības apmaiņu, tādējādi palielinot sagatavotību un izturētspēju. Lai labāk izprastu savstarpējo atkarību, Komisija ir atbalstījusi darbību dažādās nozarēs, īstenojot Eiropas programmu kritiskās infrastruktūras aizsardzībai[19].

Vienlaikus nepieciešamais priekšnoteikums starpnozaru risku risināšanai ir katras atsevišķās nozares spēja identificēt kiberincidentus, sagatavoties tiem un reaģēt uz tiem. Komisija novērtēs kiberincidentu radītos riskus savstarpēji ļoti atkarīgās nozarēs gan pašās valstīs, gan ārpus to robežām, jo īpaši nozarēs, uz kurām attiecas TID direktīva, ņemot vērā arī norises starptautiskajā līmenī[20]. Pēc šī novērtējuma Komisija apsvērs, vai šādās kritiskās nozarēs ir nepieciešami turpmāki īpaši noteikumi un/vai norādījumi par sagatavotību kiberriskiem.

Gatavojoties kiberincidentiem un reaģējot uz tiem, Eiropas līmenī svarīga nozīme var būt nozaru informācijas apmaiņas un analīzes centriem (*ISAC*)[21] un attiecīgajām *CSIRT*. Lai nodrošinātu efektīvu informācijas plūsmu par mainīgajiem draudiem un sekmētu reaģēšanu uz kiberincidentiem, *ISAC* būtu jāmudina iesaistīties TID direktīvā paredzētajā *CSIRT* tīklā un sadarboties ar Eiropola sastāvā esošo Eiropas Kibernoziedzības centru, *CERT-EU*, kā arī ar attiecīgajām tiesībaizsardzības struktūrām.

[17] Eiropas Savienības Ārlietu padome pieņēma 2014. gada 18. novembrī, Doc. 15585/14.
[18] Piemēram, Eiropas Drošības un aizsardzības koledža, *EC3*, *CEPOL* un Eiropas Aizsardzības aģentūra.
[19] SWD(2013) 318.
[20] Piemēram, Eiropas Aviācijas drošības aģentūras pieņemtais kiberdrošības ceļvedis, kiberdrošības ceļvedis, Starptautiskās Civilās aviācijas organizācijas un Starptautiskā Jūrniecības organizācijas izstrādātie kiberdrošības ceļveži.
[21] Skatīt, piemēram, Eiropas Enerģētikas *ISAC* (http://www.ee-isac.eu).

Informācijas apmaiņai ieinteresēto personu starpā un ar iestādēm visa kiberrisku dzīves cikla laikā ir nepieciešama dalībnieku pārliecība, ka viņiem netiks piemērota atbildība. Komisija ir ņēmusi vērā vairākas šādas bažas, kas attur uzņēmumus no dalīšanās ar vērtīgu izlūkinformāciju par draudiem ar pārējiem uzņēmumiem, citām nozarēm vai ar iestādēm, sevišķi pārrobežu mērogā. Komisija centīsies risināt un mazināt šīs bažas, lai uzlabotu informācijas apmaiņu par kiberdraudiem.

Uzticami ziņošanas kanāli, kas nodrošina konfidencialitāti, arī ir svarīgi, lai uzņēmumus iedrošinātu ziņot par komercnoslēpumu kiberzādzībām. Tas ļautu uzraudzīt un izvērtēt Eiropas rūpniecībai (kā rezultātā samazinās pārdošanas apjomi un darbvietu skaits) un pētniecības struktūrām nodarīto kaitējumu. Tas arī palīdzētu izstrādāt pareizu atbildes politiku. Ar *ENISA*, Eiropas Savienības Intelektuālā īpašuma biroja (*EUIPO*) un Eiropola sastāvā esošā *EC3* atbalstu Komisija dialogā ar privātajām ieinteresētajām personām izveidos uzticamus kanālus brīvprātīgai ziņošanai par komercnoslēpumu kiberzādzībām. Tas ļautu ES līmenī vākt anonīmus un apkopotus datus. Ar šiem datiem varētu dalīties ar dalībvalstīm, lai papildinātu diplomātiskos centienus un izpratnes veidošanas darbības nolūkā palīdzēt aizsargāt ES nemateriālos aktīvus pret kiberuzbrukumiem.

Lai sniegtu atbalstu nozaru kiberdrošībai, Komisija veicinās arī kiberdrošības integrēšanu dažādu ES nozaru tādu politiku izstrādē, kurās tas ir nepieciešams.

Visbeidzot, publiskā sektora iestādēm ir liela nozīme svarīgo interneta infrastruktūru integritātes pārbaudē nolūkā konstatēt problēmas, informēt par šiem tīkliem atbildīgo pusi un vajadzības gadījumā sniegt atbalstu zināmo ievainojamību novēršanā. Valstu regulatīvās iestādes varētu izmantot *CSIRT* spējas, lai regulāri skenētu publisko tīkla infrastruktūru. Pamatojoties uz minēto, tās varētu mudināt operatorus novērst trūkumus un risināt ievainojamības, kas konstatētas šo skenēšanu laikā.

Tāpēc Komisija analizēs nepieciešamos juridiskos un organizatoriskos nosacījumus tam, lai valstu regulatīvajām iestādēm sadarbībā ar valstu kiberdrošības iestādēm ļautu pieprasīt *CSIRT* veikt regulāras publiskās tīkla infrastruktūras ievainojamību pārbaudes. Valstu *CSIRT* būtu jāmudina sadarboties *CSIRT* tīklā jautājumos par paraugpraksi tīklu monitorēšanā, tādējādi veicinot plaša mēroga incidentu novēršanu.

Komisija veiks šādus pasākumus:

- veicinās nozaru informācijas apmaiņas un analīzes centru sadarbības veidošanos Eiropas līmenī, atbalstīs to sadarbību ar *CSIRT* un centīsies novērst šķēršļus, kas tirgus dalībniekus kavē dalīties informācijā;
- pētīs stratēģiskos/sistēmiskos riskus, ko izraisa kiberincidenti ļoti atkarīgās nozarēs gan pašās valstīs, gan ārpus to robežām;
- izvērtēs papildu noteikumu un/vai norādījumu par kritisko nozaru sagatavotību kiberriskiem nepieciešamību un vajadzības gadījumā apsvērs tos;
- sadarbībā ar *ENISA, EUIPO* un *EC3* izveidos uzticamus kanālus, kas būs paredzēti brīvprātīgai ziņošanai par komercnoslēpumu kiberzādzībām;
- veicinās kiberdrošības pasākumu integrēšanu Eiropas nozaru politikās, un
- analizēs nepieciešamos nosacījumus tam, lai valstu iestādēm ļautu pieprasīt *CSIRT*

veikt regulāras galveno tīkla infrastruktūru pārbaudes.

3. EIROPAS KIBERDROŠĪBAS VIENOTĀ TIRGUS PROBLĒMU RISINĀŠANA

Eiropai ir nepieciešami augstas kvalitātes un sadarbspējīgi kiberdrošības produkti un risinājumi par pieejamu cenu. Tomēr IKT drošības produktu piegāde un pakalpojumu sniegšana vienotā tirgū vēl aizvien ir ģeogrāfiski sadrumstalota. No vienas puses, tas apgrūtina Eiropas uzņēmumu konkurētspēju valstu, Eiropas un globālā līmenī, no otras puses, tas sašaurina tādu derīgu un izmantojamu kiberdrošības tehnoloģiju izvēli, kas iedzīvotājiem un uzņēmumiem ir pieejamas[22].

Kiberdrošības nozare Eiropā lielā mērā attīstījusies, pateicoties valstu valdību pieprasījumam, tostarp aizsardzības nozares vajadzībām. Lielākā daļa Eiropas aizsardzības jomas līgumslēdzēju ir izveidojuši kiberdrošības nodaļas[23]. Vienlaikus ir radušies neskaitāmi inovatīvi MVU gan specializētos tirgos/tirgus nišās (piemēram, kriptogrāfijas sistēmu tirgos), gan arī jau attīstītos tirgos (piemēram, pretvīrusu programmu tirgos) ar jauniem uzņēmējdarbības modeļiem.

Tomēr uzņēmumiem ir grūtības pāraugt vietējā valsts tirgus robežas. Neuzticēšanās citās valstīs izstrādātiem risinājumiem ir būtisks faktors, kas skaidri izkristalizējās Komisijas uzsāktajās konsultācijās[24]. Līdz ar to daudzi iepirkumi vēl aizvien notiek attiecīgajās dalībvalstīs un daudzi uzņēmumi nespēj panākt apjomradītus ietaupījumus, kas ļautu tiem kļūt konkurētspējīgākiem gan iekšējā tirgū, gan globāli.

Sadarbspējīgu risinājumu (tehnisko standartu), pieeju (procesu standartu) un ES līmeņa sertifikācijas mehānismu trūkums citu trūkumu starpā ir tas, kas ietekmē kiberdrošības vienoto tirgu. Šajā sakarā kiberdrošība tika atzīta par vienu no IKT standartizācijas prioritātēm digitālajā vienotajā tirgū[25].

Sakarā ar ierobežotām kiberdrošības uzņēmumu izaugsmes perspektīvām vienotajā tirgū daudzi uzņēmumi apvienojas vai arī tos iegādājas investori no trešām valstīm[26]. Lai gan šī tendence norāda uz Eiropas uzņēmēju spējām kiberdrošības inovāciju jomā, pastāv risks, ka tas var novest pie Eiropas zinātības un ekspertīzes zaudēšanas un pie intelektuālā darbaspēka emigrācijas.

Ir nepieciešami steidzami pasākumi, lai veicinātu integrētāka kiberdrošības produktu un pakalpojumu vienotā tirgus izveidi, kas veicinās praktiskāku un cenas ziņā izdevīgāku risinājumu ieviešanu.

Šķēršļus, kas kavē uzticības veidošanos Eiropas rūpniecības nozares un institucionālo dalībnieku starpā, var pārvarēt, veicinot sadarbību inovāciju dzīves cikla agrīnā posmā: pašā kiberdrošības nozarē, piegādātāju un pircēju starpā un starpnozaru līmenī, iesaistot nozares, kas jau ir vai varētu kļūt par kiberdrošības risinājumu patērētājiem.

[22] Skatīt SWD(2016) 216.
[23] Skatīt SWD(2016) 216.
[24] Skatīt SWD(2016) 215.
[25] COM(2016) 176/2.
[26] Skatīt SWD(2016) 216.

Vienlaikus Eiropā aizvien svarīgāka kļūst divējāda lietojuma produktu, pakalpojumu un tehnoloģiju izstrāde. Arvien lielāks skaits risinājumu tiek pārnesti no civilā uz aizsardzības nozares tirgu[27]. Gaidāmajā Eiropas Aizsardzības rīcības plānā Komisija ir iecerējusi identificēt pasākumus, lai vēl vairāk veicinātu civilmilitāro sinerģiju Eiropas līmenī.

3.1. Sertificēšana un marķēšana

Lai palielinātu uzticēšanos produktiem un pakalpojumiem un uzlabotu to drošību, svarīgs aspekts ir sertificēšana. Minētais attiecas arī uz tādām jaunām sistēmām, kuras plaši izmanto digitālās tehnoloģijas un kurām ir nepieciešams augsts drošības līmenis, piemēram, tīklam pieslēgtām un bezvadītāja automašīnām, elektroniskām veselības sistēmām, rūpnieciskas automatizācijas vadības sistēmām (*IACS*) vai viedtīkliem.

Rodas valstu iniciatīvas, kuru mērķis ir noteikt augsta līmeņa kiberdrošības prasības IKT komponentiem tradicionālajā infrastruktūrā, tostarp sertifikācijas prasības. Lai arī šīs iniciatīvas ir svarīgas, tās var sadrumstalot vienoto tirgu un radīt sadarbspējas problēmas. Tikai dažās dalībvalstīs pastāv efektīvas IKT produktu drošības sertificēšanas shēmas[28]. Tāpēc IKT piegādātājam var būt jāiziet vairāki sertificēšanas procesi, lai produktu pārdotu vairākās dalībvalstīs. Vissliktākajā gadījumā IKT produktu vai pakalpojumu, kas izstrādāts tā, lai tas atbilstu vienas dalībvalsts kiberdrošības prasībām, nedrīkst laist tirgū citā dalībvalstī.

Lai izveidotu funkcionējošu vienoto tirgu kiberdrošības jomā, ar iespējamo IKT produktu un pakalpojumu sertificēšanas satvaru būtu jācenšas sasniegt šādus mērķus: i) aptvert plašu IKT sistēmu, produktu un pakalpojumu loku; ii) nodrošināt piemērošanu visās 28 dalībvalstīs, un iii) aptvert visus kiberdrošības līmeņus; vienlaikus ņemot vērā norises starptautiskajā līmenī.

Šajā nolūkā Komisija izveidos tādu īpašu darba grupu IKT produktu un pakalpojumu drošības sertificēšanas jomā, kas sastāvēs no dalībvalstu un nozares ekspertiem. Tās mērķis būs sadarbībā ar *ENISA* un Kopīgo pētniecības centru līdz 2016. gada beigām izstrādāt ceļvedi, kurā būtu izpētītas iespējas šāda Eiropas IKT drošības sertificēšanas satvara priekšlikuma izstrādei līdz 2017. gada beigām. Šajā sakarā Komisija ņems vērā arī Regulu (EK) Nr. 2008/765 un sertificēšanas noteikumus, kas ietverti Vispārīgajā datu aizsardzības regulā 2016/679[29].

Process ietvers plašu apspriešanos un ietekmes novērtējumu. Tas ļaus Komisijai izskatīt dažādas iespējas IKT produktu un pakalpojumu sertificēšanas satvara izveidei. Komisija izskatīs arī IKT drošības sertificēšanu infrastruktūras nozarēs (piemēram, aviācijā, dzelzceļā, autobūvē) un īpašos izmantošanai gatavu tehnoloģiju sertificēšanas un validēšanas mehānismos (piemēram, rūpnieciskas automatizācijas vadības sistēmu kiberdrošība[30],

[27] Divējāda lietojuma preču eksporta nozare 2013. gadā jau veidoja aptuveni 20 % kopējā ES eksporta (vērtības). Tas ietver ES iekšējo tirdzniecību.

[28] Skatīt SWD(2016) 216 vecāko ierēdņu grupai informācijas sistēmu jautājumos (Padomes 1992. gada 31. maija Lēmums 92/242/EEK) un citas spēkā esošas shēmas, piemēram, *Commercial Product Assurance* Apvienotajā Karalistē un *Certification Sécuritaire de Premier Niveau* Francijā.

[29] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulā (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti paredzēti gan rīcības kodeksi, kas paredzēti, lai veicinātu datu aizsardzības noteikumu atbilstīgu piemērošanu, kā arī sertificēšanas mehānismi, kas attiecas uz visiem datu aizsardzības principiem, tostarp uz personas datu apstrādes drošību.

[30] Skatīt *ERNCIP* tematiskā grupa "Rūpniecisko kontroles sistēmu kiberdrošība", pieejama vietnē https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

lietišķais internets, mākoņpakalpojumi). Tā risinās arī iepriekš minētās Eiropas IKT drošības sertificēšanas shēmas ietvaros konstatētās nepilnības.

Sertificēšana iespēju robežās balstīsies un starptautiski atzītiem standartiem un tiks izstrādāta sadarbībā ar starptautiskiem partneriem.

Komisija arī izpētīs iespējas, kā IKT drošības sertificēšanu vislabāk integrēt turpmākajos nozaru tiesību aktos, arī attiecībā uz drošības aspektiem.

Papildus iespējamajiem regulējuma variantiem Komisija arī izpētīs iespēju izveidot komerciāli orientētu, brīvprātīgu un viegli izpildāmu Eiropas marķēšanas sistēmu IKT produktu drošībai. Tās mērķis papildus sertificēšanai būs uzlabot kiberdrošības aspektu saprotamību komerciālos produktos, lai palielinātu to konkurētspēju vienotajā tirgū un globālā mērogā. Pienācīga uzmanība tiks veltīta pašreizējām nozaru un horizontālajām iniciatīvām, ko nozare uzsākusi, – gan no piedāvājuma, gan no pieprasījuma puses.

Valsts pārvaldes iestādes būs cieši iesaistītas, lai publiskajos iepirkumos varētu izmantot vienotās specifikācijas un sertifikācijas atsauces. Komisija arī uzraudzīs un ziņos, kā attiecīgās sertifikācijas prasības tiek izmantotas publiskajos iepirkumos valstu līmenī, jo īpaši attiecībā uz nozaru sistēmām (enerģētikas, transporta, veselības, valsts pārvaldes u. c. sistēmām).

Komisija veiks šādus pasākumus:

- līdz 2016. gada beigām izstrādās ceļvedi virzībā uz iespējamu Eiropas IKT drošības sertificēšanas satvara priekšlikumu, kurš jāiesniedz līdz 2017. gada beigām un kurā jāizvērtē atvieglota Eiropas kiberdrošības marķēšanas satvara izpildāmība un ietekme;
- izpētīs IKT drošības sertificēšanas nepieciešamību un attiecīgā gadījumā novērsīs trūkumus tajā esošo nozares sertificēšanas/validēšanas mehānismu ietvaros;
- attiecīgā gadījumā iekļaus IKT produktu drošības sertifikācijas integrēšanu turpmākajos nozares tiesību aktu priekšlikumos;
- veicinās valsts pārvaldes iestāžu iesaisti, lai atvieglotu sertificēšanas un vienoto specifikāciju izmantošanu publiskajos iepirkumos, un
- uzraudzīs attiecīgu sertifikācijas prasību izmantošanu publiskajos un uzņēmumu iepirkumos un pēc trīs gadiem ziņos par tirgus stāvokli.

3.2. Lielākas investīcijas Eiropas kiberdrošībā un atbalsts MVU

Lai gan Eiropā notiek kiberdrošības inovāciju uzplaukums, ES vēl aizvien nav pietiekami attīstītas kultūras investīcijām kiberdrošībā. Šajā jomā ir daudz inovatīvu MVU, bet tie bieži vien nav spējīgi paplašināt savu darbību. Cita starpā tam par iemeslu ir tāda viegli pieejama finansējuma trūkums, kas palīdzētu attīstīties agrīnajos posmos. Uzņēmumiem Eiropā ir arī ierobežota piekļuve riska kapitālam, kā arī tiem pieejamais tirgvedības budžets, kas paredzēts to pamanāmības uzlabošanai vai dažādu standartizācijas un atbilstības prasību kopumu izpildei, ir neatbilstošs.

Vienlaikus kiberdrošības tirgus spēlētāju sadarbība ir visai fragmentāra, un ir nepieciešami turpmāki centieni, lai palielinātu ekonomikas koncentrēšanos un radītu jaunas vērtības ķēdes[31].

Lai Eiropā palielinātu investīcijas kiberdrošībā un atbalstītu MVU, ir nepieciešams atvieglināt piekļuvi finansējumam. Jāatbalsta arī globāli konkurētspējīgu kiberdrošības kopu un izcilības centru izveide digitālai izaugsmei labvēlīgās reģionālās ekosistēmās. Šis atbalsts jāsasaista ar lietpratīgas specializācijas stratēģiju īstenošanu un citiem ES instrumentiem, lai Eiropas kiberdrošības nozare tos labāk izmantotu.

Komisijas pieeja būs palielināt kiberdrošības kopienas izpratni par finansēšanas iespējām Eiropas, valstu un reģionālā līmenī (saistībā gan ar horizontāliem instrumentiem, gan arī ar īpašiem uzaicinājumiem[32]), izmantojot esošos instrumentus un kanālus, piemēram, Eiropas Biznesa atbalsta tīklu.

Komisija šos centienus papildinās, sadarbībā ar Eiropas Investīciju banku (EIB) un Eiropas Investīciju fondu (EIF) izpētot veidus, kā atvieglināt piekļuvi finansējumam. Šim nolūkam varētu izmantot kapitāla un kvazikapitāla investīcijas, aizdevumus, garantiju piešķiršanu projektiem vai kontragarantijas starpniekiem, piemēram, Eiropas Stratēģisko investīciju fonda ietvaros izveidojot Kiberdrošības investīciju platformu[33].

Turklāt Komisija kopā ar ieinteresētajām dalībvalstīm un reģioniem pievērstos arī kiberdrošības lietpratīgas specializācijas platformas izveidei[34]. Tā palīdzētu saskaņot un plānot kiberdrošības stratēģijas un izveidot stratēģisku sadarbību ar ieinteresētajām personām reģionālajās ekosistēmās. Šai pieejai būtu arī jāpalīdz atraisīt esošo Eiropas strukturālo un investīcijas fondu potenciālu kiberdrošības nozares vajadzībām.

Runājot vispārīgāk, Komisija veicinās integrētās drošības pieeju. Tā centīsies nodrošināt, ka kiberdrošības prasības tiek pastāvīgi ņemtas vērā ikvienā gadījumā, kad tiek veiktas lielas investīcijas infrastruktūrā, kam ir digitālā komponente un ko līdzfinansē no Eiropas fondu līdzekļiem. Šim nolūkam tā pakāpeniski ieviesīs attiecīgas prasības publisko iepirkumu un programmu noteikumos.

Komisija veiks šādus pasākumus:

- izmantos esošos MVU atbalsta rīkus, lai kiberdrošības kopienā palielinātu izpratni par esošiem finansēšanas mehānismiem;
- vēl vairāk paplašinās ES rīku un instrumentu izmantošanu, lai palīdzētu inovatīviem MVU izpētīt potenciālo sinerģiju starp civilo un aizsardzības kiberdrošības tirgu[35];

[31] Skatīt SWD(2016) 216.

[32] Skatīt, piemēram, 2016. gada daudznozaru uzaicinājumu iesniegt priekšlikumus Eiropas Infrastruktūras savienošanas instrumenta programmas ietvaros, 2016. gada *COSMO* uzaicinājumus saistībā ar Kopu internacionalizācijas programmu.

[33] Eiropas Stratēģisko investīciju fonda ietvaros atsevišķus projektus var atbalstīt vai nu tieši, vai netieši, izmantojot investīciju platformas. Šādas platformas var palīdzēt finansēt mazākus projektus un sasaistīt līdzekļus no dažādiem avotiem, paverot iespējas diversificētām investīcijām uz ģeogrāfiska vai nozariska pamata.

[34] Skatīt lietpratīgas specializācijas instrumentus (*RIS3*): http://s3platform.jrc.ec.europa.eu/.

[35] Piemēram, Eiropas Biznesa atbalsta tīkls un ar aizsardzību saistītu reģionu Eiropas tīkls sniegs reģioniem jaunas iespējas izpētīt pārrobežu sadarbību divējāda lietojuma produktu jomā, tostarp kiberdrošības jomā, un MVU – meklēt sadarbības partnerus.

- sadarbībā ar EIB un EIF izpētīs iespēju atvieglināt piekļuvi investīcijām, piemēram, izmantojot īpaši paredzētu kiberdrošības investīciju platformu vai citus rīkus;
- izstrādās kiberdrošības lietpratīgas specializācijas platformu, lai sniegtu atbalstu dalībvalstīm un reģioniem, kas ir ieinteresēti investēt kiberdrošības nozarē (*RIS3*), un
- attiecībā uz tādām apjomīgām investīcijām infrastruktūrā, kurām ir digitālā komponente un kuras līdzfinansē no ES fondu līdzekļiem, veicinās integrētās drošības pieeju.

4. EIROPAS KIBERDROŠĪBAS NOZARES STIMULĒŠANA UN VEICINĀŠANA, IZMANTOJOT INOVĀCIJAS – KIBERDROŠĪBAS *cPPP* IZVEIDE

Lai veicinātu Eiropas kiberdrošības nozares konkurētspēju un inovētspēju, tiks parakstīta līgumiska publiskā un privātā sektora partnerība (*cPPP*) kiberdrošības jomā. Ar šīs *cPPP* palīdzību tiks sakopoti rūpnieciskie un publiskie resursi, lai pētniecībā un inovācijā nodrošinātu izcilību.

cPPP mērķis ir veidot uzticību dalībvalstu un nozares starpā, veicinot sadarbību pētniecības un inovācijas procesa agrīnā posmā. Tās mērķis ir arī palīdzēt saskaņot pieprasījumu un piegādi. Tam vajadzētu palīdzēt nozares dalībniekiem uzzināt no galalietotājiem un nozarēm, kas ir nozīmīgi kiberdrošības risinājumu patērētāji (piemēra, enerģētika, veselība, transports, finanses), kādas būs to prasības nākotnē. Tas sekmēs viņu iesaisti vienoto savas nozares digitālās drošības, privātuma un datu aizsardzības prasību definēšanā.

Kiberdrošības *cPPP* palīdzēs arī maksimāli izmantot pieejamos līdzekļus. Tas tiks panākts, pirmkārt, izmantojot labāku saskaņošanu ar dalībvalstīm. Otrkārt, vairāk uzmanības tiks pievērsts atsevišķām tehniskām prioritātēm, lai kiberdrošības nozarei palīdzētu panākt tehnoloģiskus sasniegumus un pārvaldīt galvenās nākotnes kiberdrošības tehnoloģijas. Šajā sakarā atvērtā pirmkoda programmatūras un atvērto standartu izstrāde var palīdzēt veicināt uzticēšanos, pārredzamību un revolucionāras inovācijas, un tāpēc tiem arī vajadzētu būtu daļai no *cPPP* ietvaros veiktajām investīcijām.

Kiberdrošības *cPPP* ietvaros veiktais darbs gūs labumu arī no sinerģijas ar citiem Eiropas projektiem, īpaši tiem, kas pievēršas drošības aspektiem. To vidū ir nākotnes rūpnīcas, energoefektīvas ēkas, *5G* un lielo datu tehnoloģiju *PPP*[36] un citas nozaru *PPP*[37], kā arī lietiskā interneta iniciatīva[38]. Turklāt tiks veicināta cieša sasaiste ar Eiropas atvērto zinātnes mākoni un Eiropas superdatošanas iniciatīvu kvantu kibertehnoloģijās (piemēram, kvantu atslēgu inovācijā, kvantu datošanas pētniecībā).

Kiberdrošības *cPPP* sakņojas pamatprogrammā "Apvārsnis 2020"[39], kas ir ES pētniecības un inovācijas pamatprogramma laikposmam no 2014. līdz 2020. gadam. Tā piesaistīs finansējumu no diviem programmas pīlāriem: vadošā loma pamattehnoloģiju un rūpniecisko

[36] Publiskā un privātā partnerība *5G* infrastruktūras jomā un lielo datu tehnoloģiju publiskā un privātā partnerība.
[37] Piemēram, publiskā un privātā partnerība *SESAR* vai pārejas uz dzelzceļu jomā.
[38] Lietiskā interneta inovāciju alianse (*AIOTI*).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

tehnoloģiju jomā (*LEIT-ICT*) un sabiedrības problēmu risināšana – droša sabiedrība (*SC7*). Kopējais *cPPP* budžets sasniegs EUR 450 miljonus ar trīskāršu finanšu sviras faktoru nozares pusē. Arī citās pamatprogrammas "Apvārsnis 2020" daļās būtu jāpievēršas kiberdrošībai un būtu ar to jāsaskaņo (piemēram, "Apvāršņa 2020" enerģētikas, transporta un sabiedrības veselības problēmu risināšanas un izcilības daļās). Tas palīdzēs sasniegt kiberdrošības *cPPP* mērķus. Šai saskaņošanai būtu jānotiek arī jau pašā nozaru stratēģiju izstrādes posmā.

cPPP tiks īstenota pārredzami, izmantojot atvērtu un elastīgu pārvaldību, kas pielāgota strauji mainīgajai kiberdrošības videi. Tajā tiks ņemta vērā dalībvalstu vajadzība apspriest, kā izmaiņas tehnoloģijās ietekmē drošu valsts un pārrobežu infrastruktūras izmantošanu. Tāpat partnerības rezultātam jābūt ilgtspējīgam vairāku gadu garumā, lai nodrošinātu, ka tās mērķi ir sasniedzami.

cPPP atbalstīs Eiropas Kiberdrošības organizācija (*ECSO*), kuras dalībnieku kopums atspoguļos Eiropas kiberdrošības tirgus daudzveidību. Tā ietvers arī valstu, reģionālās un vietējās pārvaldes iestādes, pētniecības centrus, akadēmiskās aprindas un citas ieinteresētās personas.

Komisija veiks šādus pasākumus:

- ar nozari parakstīs līgumisku publiskā un privātā sektora partnerību kiberdrošības jomā, lai tā sāktu darboties 2016. gada trešajā ceturksnī;
- pamatprogrammas "Apvārsnis 2020" ietvaros 2017. gada pirmajā ceturksnī izsludinās uzaicinājumus iesniegt priekšlikumus saistībā ar kiberdrošības *cPPP*, un
- nodrošinās kiberdrošības *cPPP* saskaņošanu ar attiecīgajām nozaru stratēģijām, "Apvāršņa 2020" instrumentiem un nozaru *PPP*.

5. NOSLĒGUMS

Šajā paziņojumā ir izklāstīti pasākumi, kuru mērķis ir stiprināt Eiropas kiberizturētspējas sistēmu un veicināt konkurētspējīgu un inovētspējīgu kiberdrošības nozari Eiropā saskaņā ar ES kiberdrošības stratēģijā un digitālā vienotā tirgus stratēģijā izklāstīto. Komisija aicina Eiropas Parlamentu un Padomi atbalstīt šo pieeju.