Eiropas Savienības
Padome

Briselē, 2020. gada 16. decembrī
(OR. en)

14133/20

Starpiestāžu lieta:
2020/0305(NLE)

CYBER 280	**RECH 529**
JAI 1118	**COMPET 642**
JAIEX 121	**IND 273**
EJUSTICE 107	**COTER 115**
COSI 254	**ENFOPOL 350**
DATAPROTECT 154	**COPS 485**
COPEN 387	**MI 578**
TELECOM 269	**IXIM 139**
PROCIV 99	**POLMIL 201**
CSC 367	**HYBRID 48**
CIS 65	**CSCI 96**
RELEX 1019	**POLGEN 234**

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2020. gada 16. decembris
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretārs *Jeppe TRANHOLM-MIKKELSEN*
K-jas dok. Nr.:	JOIN(2020) 18 final
Temats:	KOPĪGS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI ES kiberdrošības stratēģija digitālajai desmitgadei

Pielikumā ir pievienots dokuments JOIN(2020) 18 *final*.

Pielikumā: JOIN(2020) 18 *final*

EIROPAS
KOMISIJA

SAVIENĪBAS AUGSTAIS
PĀRSTĀVIS ĀRLIETĀS UN
DROŠĪBAS POLITIKAS
JAUTĀJUMOS

Briselē, 16.12.2020.
JOIN(2020) 18 final

KOPĪGS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

ES kiberdrošības stratēģija digitālajai desmitgadei

KOPĪGS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

ES kiberdrošības stratēģija digitālajai desmitgadei

I. IEVADS: KIBERDROŠA DIGITĀLĀ PĀRVEIDE SAREŽĢĪTĀ DRAUDU VIDĒ

Kiberdrošība ir svarīga eiropiešu drošības daļa. Neatkarīgi no tā, vai runa ir par savienotām ierīcēm, elektrotīkliem, bankām, gaisa kuģiem, valsts pārvaldi vai slimnīcām, cilvēki ir pelnījuši, lai viss, ko tie izmanto vai apmeklē, būtu garantēti pasargāts no kiberdraudiem. ES ekonomika, demokrātija un sabiedrība kā vēl nekad agrāk ir atkarīgas no drošiem un uzticamiem digitālajiem rīkiem un savienojamības. Tādēļ kiberdrošībai ir izšķirīga nozīme noturīgas, zaļas un digitālas Eiropas veidošanā.

Transporta, enerģētikas un veselības, telesakaru, finanšu, drošības, demokrātisko procesu, kosmosa un aizsardzības nozares ir lielā mērā atkarīgas no tīklu un informācijas sistēmām, kas arvien biežāk ir savstarpēji savienotas. Starpnozaru savstarpējā atkarība ir ļoti augsta, jo tīklu un informācijas sistēmu darbība savukārt ir atkarīga no stabilas elektroapgādes. Savienoto ierīču pasaulē jau šobrīd ir vairāk nekā cilvēku, un tiek prognozēts, ka līdz 2025. gadam to skaits pieaugs līdz 25 miljardiem[1], turklāt ceturtā daļa no tām atradīsies Eiropā. Covid-19 pandēmija, kuras laikā 40 % ES strādājošo pārgāja uz tāldarbu, ir paātrinājusi darba modeļu digitalizāciju un, visticamāk, atstās paliekošas sekas uz mūsu ikdienu[2]. Šādi palielinās neaizsargātība pret kiberuzbrukumiem[3]. Patērētājiem bieži vien tiek piegādātas savienotās preces ar zināmām vājajām vietām, kas vēl vairāk palielina ar ļaunprātīgām kiberdarbībām saistītu uzbrukumu iespējas[4]. ES rūpniecības vide ir aizvien vairāk digitalizēta un savienota, kas nozīmē arī to, ka kiberuzbrukumi var daudz smagāk nekā jebkad ietekmēt nozares un ekosistēmas.

Draudu ainu vēl vairāk pasliktina ģeopolitiskais saspīlējums attiecībā uz globālu un atvērtu internetu un tehnoloģiju kontroli visā piegādes ķēdē[5]. Šo saspīlējumu atspoguļo pieaugošais skaits valstu, kas ir ieviesušas digitālās robežas. Interneta ierobežojumi apdraud globālu un atvērtu kibertelpu, kā arī tiesiskumu, pamattiesības, brīvību un demokrātiju — ES pamatvērtības. Kibertelpa arvien biežāk tiek izmantota politiskiem un ideoloģiskiem

[1] Pēc telesakaru arodasociācijas *GSMA* aplēsēm; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). Starptautiskā Datu korporācija paredz, ka būs 42,6 miljardi savienotu iekārtu, sensoru un kameru; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] 2020. gada jūnijā rīkotā aptaujā 47 % no uzņēmumu vadītājiem plānoja atļaut darbiniekiem pilnībā strādāt attālināti arī pēc tam, kad būs iespējams atgriezties darbvietā; 82 % bija iecerējuši atļaut tāldarbu vismaz daļu no laika; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Viena no līdz šim kaitnieciskākajām ļaunprogrammatūrām, ko dēvē par *Mirai*, izveidoja vairāk nekā 600 000 ierīču robottīklu, kas traucēja vairāku lielu tīmekļa vietņu darbību Eiropā un ASV.

[5] Ieskaitot elektronikas komponentus, datu analītiku, mākoņpakalpojumus, ātrākus un viedākus 5G un turpmākos tīklus, šifrēšanu, mākslīgo intelektu (MI), kā arī jaunas datošanas un uzticamas datu apstrādes paradigmas kā blokķēdes, "no mākoņdatošanas līdz perifērijai" un kvantisko datošanu.

mērķiem, un efektīvas daudzpusējas attiecības kavē pieaugoša starptautiskā polarizācija. Hibrīddraudi apvieno dezinformācijas kampaņas ar kiberuzbrukumiem infrastruktūrai, ekonomikas procesiem un demokrātiskajām institūcijām, un tie var nodarīt fizisku kaitējumu, ļaut prettiesiski piekļūt personas datiem, nolaupīt rūpniecisko vai valsts noslēpumu, sēt neuzticību un vājināt sociālo kohēziju. Šīs darbības kaitē starptautiskajai drošībai un stabilitātei, kā arī kibertelpas sniegtajiem ekonomiskās, sociālās un politiskās attīstības ieguvumiem.

Ļaunprātīga vēršanās pret kritisko infrastruktūru ir nozīmīgs globāls risks[6]. Interneta uzbūve ir decentralizēta — tam nav centrālas struktūras, bet ir daudzu ieinteresēto personu īstenota pārvaldība. Tas ir spējis uzturēt eksponenciālu datplūsmas apjoma pieaugumu, vienlaikus būdams pastāvīgs mērķis ļaunprātīgiem mēģinājumiem to traucēt[7]. Vienlaikus arvien lielāka ir paļaušanās uz globālā un atvērtā interneta pamatfunkcijām, piemēram, domēnu nosaukumu sistēmu (DNS), un interneta pamatpakalpojumiem, kas nepieciešami sakariem, tīmekļa mitināšanai, lietotnēm un datiem. Šie pakalpojumi arvien vairāk koncentrējas dažu privātu uzņēmumu rokās[8]. Līdz ar to Eiropas ekonomika un sabiedrība nav pasargāta no traucējošiem ģeopolitiskiem vai tehniskiem notikumiem, kas skar interneta pamatresursus vai vienu vai vairākus no šiem uzņēmumiem. Pandēmijas izraisītais interneta lietošanas apjoma pieaugums un izmaiņu tendences vēl vairāk ir atklājuši, cik neaizsargātas ir no šīs digitālās infrastruktūras atkarīgās piegādes ķēdes.

Bažas par drošību ir svarīgs faktors, kas attur no tiešsaistes pakalpojumu izmantošanas[9]**.** Aptuveni divas piektdaļas ES lietotāju ir piedzīvojuši ar drošību saistītas problēmas, bet trīs piektdaļas nejūtas spējīgi aizsargāties no kibernoziegumiem[10]. Trešdaļa lietotāju pēdējo trīs gadu laikā ir saņēmusi krāpnieciskas e-pasta vēstules vai tālruņa zvanus, kuros ir lūgts sniegt personisku informāciju, bet 83 % nekad nav ziņojuši par kibernoziegumiem. Katru astoto uzņēmumu ir skāruši kiberuzbrukumi[11]. Vairāk nekā puse uzņēmumu un iedzīvotāju personālo datoru, kas reiz tikuši inficēti ar ļaunprogrammatūru, tā paša gada laikā tiek inficēti atkārtoti[12]. Datu aizsardzības pārkāpumos katru gadu tiek zaudēti simtiem miljonu ierakstu; viena pārkāpuma radītās vidējās izmaksas uz vienu uzņēmumu

---

[6] Pasaules Ekonomikas foruma 2020. gada ziņojums par riskiem pasaulē.

[7] Ekonomiskās sadarbības un attīstības organizācija ziņo, ka pandēmijas rezultātā interneta datplūsmas apjoms ir pieaudzis par 60 %; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Eiropas Elektronisko sakaru regulatoru iestāde un Komisija regulāri publicē ziņojumus par interneta jaudas stāvokli koronavīrusa ierobežošanas pasākumu laikā. *ENISA* ziņojumā ir minēts, ka 2019. gada 3. ceturksnī, salīdzinot ar 2018. gada 3. ceturksni, izkliedētās pakalpojumatteices (*DDoS*) uzbrukumu kopējais skaits ir pieaudzis par 241 %. *DDoS* uzbrukumi kļūst aizvien intensīvāki — 2020. gada februārī notika visu laiku apjomīgākais uzbrukums, kura datplūsma sasniedza 2,3 terabitus sekundē. 2020. gada augustā "*CenturyLink* atvienojumā" ASV interneta pakalpojumu sniedzēja maršrutēšanas problēma izraisīja pasaules tīmekļa datplūsmas samazināšanos par 3,5 %; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

[8] *Internet Society*. "The Global Internet Report: Consolidation in the Internet Economy"; https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/

[9] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG.

[10] 2020. gada Digitālās ekonomikas un sabiedrības indekss; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[11] *Eurostat* paziņojums presei "ICT security measures taken by vast majority of enterprises in the EU", 6/2020, 2020. gada 13. janvāris. "Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare and transportation"; PEF, 2020. gada ziņojums par riskiem pasaulē.

[12] Avots: *Comparitech*.

2018. gadā pieauga, pārsniedzot 3,5 miljonus EUR[13]. Kiberuzbrukuma ietekmi bieži vien nevar izolēt, un tas var izraisīt ķēdes reakciju ekonomikā un sabiedrībā, ietekmējot miljoniem cilvēku[14].

Gandrīz visu veidu noziegumu izmeklēšanai piemīt digitāls komponents. Tiek ziņots, ka 2019. gadā ir trīskāršojies gadā novēroto incidentu skaits. Eksistē aptuveni 700 miljonu jaunu ļaunprogrammatūras paraugu, kas ir visbiežāk izmantotais kiberuzbrukuma īstenošanas veids[15]. Tiek lēsts, ka 2020. gadā kibernoziedzība pasaules ekonomikai ir nodarījusi 5,5 triljonus EUR lielus zaudējumus, kas ir divreiz vairāk nekā 2015. gadā[16]. Tā ir lielākā saimnieciskās bagātības pāreja vēsturē, kas pārsniedz pasaules narkotiku tirdzniecības apmērus. Viena ievērojama incidenta — 2017. gada "WannaCry" izspiedējprogrammatūras uzbrukuma — nodarītās izmaksas pasaules ekonomikai tika lēstas vairāk nekā 6,5 miljardu EUR apmērā[17].

Digitālo pakalpojumu un finanšu nozare ir starp biežākajiem kiberuzbrukumu mērķiem, kuru vidū ir arī publiskais sektors un ražošanas nozare, tomēr uzņēmumu un personu kibergatavība un informētība joprojām ir zema[18], un darba tirgū valda ievērojams kiberdrošības prasmju deficīts[19]. 2019. gadā notika gandrīz 450 kiberdrošības incidenti, kuros bija iesaistīta Eiropas kritiskā infrastruktūra, piemēram, finanšu un enerģētikas nozarēs[20]. Pandēmija ir īpaši smagi skārusi veselības aprūpes organizācijas un speciālistus. Tehnoloģijām kļūstot nenošķiramām no fiziskās pasaules, kiberdraudi apdraud vismazāk aizsargāto personu dzīvību un labklājību[21]. Vairāk nekā divas trešdaļas uzņēmumu, jo īpaši MVU, kiberdrošībā tiek uzskatīti par "iesācējiem", un Eiropas uzņēmumi tiek uzskatīti par vājāk sagatavotiem nekā Āzijas un Amerikas uzņēmumi[22]. Tiek lēsts, ka Eiropā aptuveni 291 000 kiberdrošības speciālistu vakanču nav aizpildītas. Kiberdrošības ekspertu pieņemšana darbā un apmācība ir lēns process, kas noved pie organizāciju kiberdrošības risku palielināšanās[23].

---

[13] *Ponemon* institūta 2020. gada ziņojums par datu aizsardzības pārkāpumu izmaksām, balstoties uz 524 nesenu pārkāpumu analīzi 17 valstīs un 17 nozarēs; https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[14] Kopīgā pētniecības centra (KPC) ziņojums "Cybersecurity, our digital anchor"; https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor

[15] Avots: AV-TEST, https://www.av-test.org/en/statistics/malware/.

[16] KPC. "Cybersecurity – Our Digital Anchor".

[17] Avots: *Cyence*.

[18] Arī uzņēmumu, jo īpaši MVU, informētība par komercnoslēpumu kiberzādzībām joprojām ir zema; *PwC* pētījums par rūpnieciskās spiegošanas apmēru un ietekmi un par komercnoslēpumu zādzībām, kas veiktas, izmantojot kibervidi: "Dissemination report on measures to tackle and prevent cyber-theft of trade secrets", 2018.

[19] Sk.: *ENISA*. "Threat Landscape 2020" un "Verizon Data Breach Investigations Report 2020"; https://enterprise.verizon.com/resources/reports/dbir/

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f.

[21] Izspiedējprogrammatūra ir izmantota, lai uzbruktu slimnīcām un medicīniskajām kartēm, piemēram, Rumānijā (2020. gada jūnijā), Diseldorfā (2020. gada septembrī) un uzņēmumā "Vastaamo" (2020. gada oktobrī).

[22] *PwC*. "The Global State of Information Security 2018"; *ESI Thoughtlab*. "The Cybersecurity Imperative", 2019.

[23] ES Kiberdrošības aģentūra. "Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database", 2019. gada decembris.

ES trūkst kiberdraudu situācijas kolektīvas apzināšanās. Tas tā ir tādēļ, ka valstu iestādes sistemātiski neapkopo un nedalās, piemēram, ar privātajā sektorā pieejamo informāciju, kas varētu palīdzēt izvērtēt ES situāciju kiberdrošības jomā. Dalībvalstis ziņo tikai par nelielu daļu no incidentiem, un informācijas koplietošana nav nedz sistemātiska, nedz visaptveroša[24], un kiberuzbrukumi var būt tikai viens no aspektiem, kā izpaužas mērķtiecīgi un ļaunprātīgi uzbrukumi pret Eiropas sabiedrībām. Savstarpējā operatīvā palīdzība starp dalībvalstīm patlaban ir ļoti ierobežota, un starp dalībvalstīm un ES iestādēm, aģentūrām un struktūrām nav ieviests operatīvs mehānisms liela mēroga pārrobežu kiberincidentu un krīžu gadījumiem[25].

Tādēļ, lai cilvēki uzticētos, izmantotu un gūtu labumu no inovācijas, savienojamības un automatizācijas, kā arī lai tiktu aizsargātas pamattiesības un brīvības, ieskaitot tiesības uz privāto dzīvi un personas datu aizsardzību, un vārda un informācijas brīvību, ir ļoti svarīgi uzlabot kiberdrošību. Kiberdrošība ir neatņemama daļa no tīkla savienojamības, kā arī globālā un atvērtā interneta, kam jābūt 21. gadsimta 20. gadu ekonomikas un sociālās pārejas pamatā. Tā palīdz veidot vairāk labāku darbvietu, elastīgāku darbu, efektīvāku un ilgtspējīgāku transportu un lauksaimniecību, kā arī vieglāku un taisnīgāku piekļuvi veselības aprūpei. Tā ir arī svarīga pārejai uz tīrāku enerģiju saskaņā ar Eiropas zaļo kursu[26], izmantojot pārrobežu tīklus un viedskaitītājus, kā arī lai izvairītos no nevajadzīgas datu glabāšanas dublēšanās. Visbeidzot, tā ir svarīga starptautiskajai drošībai un stabilitātei, kā arī pasaules ekonomikas, demokrātijas un sabiedrības attīstībai. Tādēļ valdībām, uzņēmumiem un indivīdiem digitālie rīki ir jāizmanto atbildīgi, domājot par drošību. Informētībai par kiberdrošību, kā arī tās higiēnai ir jābūt pamatā ikdienas darbību digitālajai pārveidei.

ES jaunā kiberdrošības stratēģija digitālajai desmitgadei ir svarīga daļa no Eiropas digitālās nākotnes veidošanas[27], Komisijas Eiropas atveseļošanas plāna[28], Drošības savienības stratēģijas 2020.–2025. gadam[29], ES ārpolitikas un drošības politikas globālās stratēģijas[30] un Eiropadomes stratēģiskās programmas 2019.–2024. gadam[31]. Tajā ir izklāstīts, kā ES aizsargās iedzīvotājus, uzņēmumus un iestādes no kiberdraudiem un kā tā sekmēs starptautisko sadarbību un ieņems vadošo lomu globāla un atvērta interneta nodrošināšanai.

II. DOMĀT GLOBĀLI, RĪKOTIES EIROPEISKI

Šīs stratēģijas mērķis ir nodrošināt globālu un atvērtu internetu ar spēcīgiem aizsardzības mehānismiem, lai mazinātu apdraudējumus Eiropas iedzīvotāju drošībai, pamattiesībām un brīvībām. Sekojot ar iepriekšējām stratēģijām panāktajam progresam, tajā ir ietverti konkrēti priekšlikumi **trīs galveno instrumentu — regulatīvo, ieguldījumu un politikas instrumentu** — izvietošanai, lai sekmētu **trīs ES rīcības jomas — 1) noturību, tehnoloģisko suverenitāti un līderību, 2) novēršanas, atturēšanas un reaģēšanas operatīvo spēju veidošanu un 3) globālas un atvērtas kibertelpas attīstīšanu**. ES ir apņēmusies atbalstīt šo stratēģiju ar vēl **nepieredzētiem ieguldījumiem ES digitālās**

[24] Dalībvalstīm saskaņā ar Tīklu un informācijas sistēmu drošības direktīvas (Direktīva (ES) 2016/1148) 10. panta 3. punktu katru gadu ir jāiesniedz sadarbības grupai kopsavilkuma ziņojums par saņemtajiem paziņojumiem.
[25] *CSIRT* tīkla dalībnieku savstarpējai palīdzībai ir ieviestas standarta operāciju procedūras.
[26] "Eiropas zaļais kurss", COM(2019) 640 final.
[27] "Eiropas digitālās nākotnes veidošana", COM(2020) 67 final.
[28] "Eiropas lielā stunda: jāatjaunojas un jāsagatavo ceļš nākamajai paaudzei", COM(2020) 456 final.
[29] ES Drošības savienības stratēģija 2020.–2025. gadam, COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en.
[31] https://www.consilium.europa.eu/lv/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#.

pārkārtošanās procesā tuvāko septiņu gadu laikā — iespējams, četrkāršojot līdzšinējo apjomu, — kā daļu no jaunas tehnoloģiskās un rūpnieciskās rīcībpolitikas un atveseļošanas darba programmas[32].

Izmantojot stimulus, pienākumus un etalonrādītājus, kiberdrošību ir nepieciešams integrēt visos minētajos digitālajos ieguldījumos, jo īpaši tādās nozīmīgās tehnoloģijās kā mākslīgais intelekts (MI), šifrēšana un kvantiskā datošana. Šādi varētu tikt stimulēta Eiropas kiberdrošības nozares izaugsme un sniegta nepieciešamā pārliecība, kas ļautu atteikties no mantotām sistēmām. Eiropas Aizsardzības fonds (EAF) atbalstīs Eiropas kiberaizsardzības risinājumus kā daļu no Eiropas aizsardzības tehnoloģiskā un rūpnieciskā pamata. Kiberdrošība ir iekļauta mūsu partneru atbalstam paredzētajos ārējās finansēšanas instrumentos, jo īpaši Kaimiņattiecību, attīstības sadarbības un starptautiskās sadarbības instrumentā. Tehnoloģiju ļaunprātīgas izmantošanas novēršana, kritiskās infrastruktūras aizsardzība un piegādes ķēžu integritātes nodrošināšana arī ļauj ES ievērot ANO normas, noteikumus un principus par valstu atbildīgu uzvedību[33].

1. NOTURĪBA, TEHNOLOĢISKĀ SUVERENITĀTE UN LĪDERĪBA

ES kritiskā infrastruktūra un būtiskie sabiedriskie pakalpojumi arvien vairāk kļūst savstarpēji atkarīgi un digitalizēti. Visām ar internetu savienotajām precēm ES (vai tie būtu automatizēti transportlīdzekļi, ražošanas vadības sistēmas vai sadzīves tehnikas ierīces), kā arī piegādes ķēdēm, kas dara tās pieejamas, ir jābūt jau sākotnēji drošām, noturīgām pret kiberincidentiem, kā arī tām pēc vājo vietu atklāšanas ātri jāpiemēro ielāpi. Tas ir ļoti svarīgi, lai ES privātajam un publiskajam sektoram sniegtu iespēju izvēlēties starp visdrošāko infrastruktūru un pakalpojumiem. Nākamā desmitgade ir ES iespēja vadīt drošu tehnoloģiju izstrādi visā piegādes ķēdē. Ir jāpiesaista visi nepieciešamie regulatīvie, ieguldījumu un politikas instrumenti, lai nodrošinātu noturību un attīstītākas rūpnieciskās un tehnoloģiskās spējas kiberdrošībā. Sākotnēji kiberdroši rūpnieciskie procesi, operācijas un ierīces var mazināt riskus, samazināt izmaksas uzņēmumiem un plašākai sabiedrībai, tādējādi uzlabojot noturību.

1.1. Noturīga infrastruktūra un kritiski svarīgi pakalpojumi

Kiberdrošības vienotā tirgus centrā atrodas ES **noteikumi par tīklu un informācijas drošību (TID)**. Komisija ierosina veikt šo noteikumu reformu ar pārskatītu TID direktīvu, lai uzlabotu **visu to attiecīgo publisko un privāto sektoru kibernoturību, kuri veic ekonomikai un sabiedrībai svarīgas funkcijas[34].** Pārskatīšanu ir nepieciešams veikt, lai mazinātu iekšējā tirgus nesakritības, saskaņojot darbības jomu, prasības drošībai un ziņošanai par incidentiem, valstu uzraudzību un izpildi, kā arī kompetento iestāžu spējas.

Reformēta TID direktīva kalpos par pamatu konkrētākiem noteikumiem, kas ir nepieciešami arī stratēģiski svarīgām nozarēm, ieskaitot enerģētiku, transportu un veselības aprūpi. Lai nodrošinātu saskaņā ar Drošības savienības stratēģiju 2020.–2025. gadam izziņoto

[32] Ieguldījumiem visā digitālo tehnoloģiju piegādes ķēdē, ar kuriem sekmē digitālo pārkārtošanos vai risina no tās izrietošās problēmas, vajadzētu būt vismaz 20 % (kas atbilst 134,5 miljardiem EUR) no 672,5 miljardu EUR lielā Atveseļošanas un noturības mehānisma, ko veido dotācijas un aizdevumi. ES finansējums, kas 2021.–2027. gada daudzgadu finanšu shēmā saskaņā ar programmu "Digitālā Eiropa" paredzēts kiberdrošībai un saskaņā ar programmu "Apvārsnis Eiropa" — kiberdrošības pētniecībai, kopā varētu sasniegt 2 miljardus EUR, ko papildinās dalībvalstu un nozares ieguldījumi, un īpašu uzmanību paredzēts veltīt MVU atbalstam.

[33] https://undocs.org/A/70/174.

[34] [*iekļaut atsauci uz TID priekšlikumu*]

konsekvento pieeju, reformētā direktīva tiek ierosināta vienlaikus ar kritiskās infrastruktūras noturības tiesību aktu pārskatīšanu[35]. Energotehnoloģijas, kas ietver digitālos komponentus, un ar tām saistīto piegādes ķēžu drošība ir svarīgas būtisku sabiedrisku pakalpojumu nepārtrauktībai un kritiski svarīgas energoinfrastruktūras stratēģiskajai kontrolei. Tādēļ Komisija ierosinās pasākumus, ieskaitot "tīkla kodeksu", ar ko tiks paredzēti pārrobežu elektroenerģijas plūsmu kiberdrošības noteikumi un kas būtu jāpieņem līdz 2022. gada beigām. Arī finanšu sektoram ir jāstiprina digitālās darbības noturība un jānodrošina spēja izturēt visu veidu ar IKT saistītus traucējumus un apdraudējumus, kā ir ierosinājusi Komisija[36]. Komisija transporta jomā papildināja ES aviācijas drošības tiesību aktus ar noteikumiem par kiberdrošību[37] un turpinās centienus uzlabot kibernoturību visos transporta veidos. Svarīgs Eiropas Demokrātijas rīcības plāna komponents ir **demokrātisko procesu un iestāžu** kibernoturības stiprināšana, lai aizsargātu un veicinātu brīvas vēlēšanas, demokrātisku diskursu un mediju plurālismu[38]. Visbeidzot, lai panāktu nākotnes kosmosa programmas infrastruktūras un pakalpojumu drošību, Komisijas turpinās padziļināt *Galileo* kiberdrošības stratēģiju attiecībā uz globālās navigācijas satelītu sistēmas nākamās paaudzes pakalpojumiem un citiem jaunajiem kosmosa programmas komponentiem[39].

1.2. Eiropas kibervairoga veidošana

Izplatoties savienojamībai un pieaugot kiberuzbrukumu izsmalcinātībai, svarīgu lomu (tajā skaitā nozaru līmenī) pilda informācijas apmaiņas un analīzes centri (*ISAC*), jo tie ļauj dažādām ieinteresētajām personām apmainīties ar informāciju par kiberdraudiem[40]. Turklāt tīkli un datorsistēmas ir pastāvīgi jāuzrauga un jāanalizē, lai reāllaikā atklātu ielaušanos un anomālijas. Tādēļ daudzi privātie uzņēmumi, publiskās organizācijas un valstu iestādes ir izveidojuši datordrošības incidentu reaģēšanas vienības (*CSIRT*) un drošības operāciju centrus (DOC).

Drošības operāciju centriem ir liela loma ierakstu apkopošanā[41] un to uzraudzītajos sakaru tīklos notiekošo aizdomīgo notikumu izolēšanā. Tie to dara, identificējot signālus un modeļus, kā arī no lielā izvērtējamo datu apjoma izgūstot zināšanas par apdraudējumiem. Tie ir palīdzējuši atklāt ļaundabīgu izpildāmprogrammu darbības, kas savukārt ir palīdzējis ierobežot kiberuzbrukumus. Darbs, kas jāpaveic šajos centros, ir smags un notiek straujā tempā, tādēļ nenovērtējamu atbalstu praktiķiem var sniegt MI, jo īpaši mašīnmācīšanās paņēmieni[42].

---

[35] [iekļaut atsauci uz *priekšlikumu* direktīvai par kritiski svarīgo struktūru noturību]

[36] Priekšlikums regulai par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 un (ES) Nr. 909/2014 (COM(2020) 595 final).

[37] Komisijas Īstenošanas regula (ES) 2019/1583.

[38] Paziņojums "Eiropas Demokrātijas rīcības plāns", COM(2020) 790. Saskaņā ar šo plānu Eiropas vēlēšanu sadarbības tīkls un dalībvalstu vēlēšanu tīkli atbalstīs kopīgu ekspertu grupu izveidošanu cīņai pret vēlēšanu apdraudējumiem, ieskaitot kiberdraudus; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en

[39] Tie ietver jaunu valdības satelītsakaru iniciatīvu (*GOVSATCOM*) un kosmosa atkritumus (*SST*)

[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

[41] Tā, lai tos kā pierādījumus varētu izmantot tiesībaizsardzības iestādes un tiesas.

[42] Avots: *Ponemon* pētniecības institūta aptauja "Improving the Effectiveness of the SOC, 2019"; attiecībā uz pētījumiem par MI izmantošanu drošības operāciju centros sk., piem.: Khraisat, A., Gondal, I., Vamplew, P. *et al. Survey of intrusion detection systems: techniques, datasets and challenges, Cybersecur 2*, 20 (2019).

Komisija ierosina veidot **ES mēroga drošības operāciju centru tīklu**[43], kā arī atbalstīt esošo centru uzlabošanu un jaunu centru izveidi. Tā arī atbalstīs šajos centros strādājošo darbinieku mācības un prasmju uzlabošanu. Balstoties uz vajadzību analīzi, kas tiktu veikta kopā ar attiecīgajām iesaistītajām personām un ko atbalstītu ES Kiberdrošības aģentūra (*ENISA*), tā varētu piešķirt vairāk nekā 300 miljonus EUR, lai atbalstītu publisko un privāto, kā arī pārrobežu sadarbību, veidojot valstu un nozaru tīklus, iesaistot arī MVU, un balstoties uz attiecīgiem pārvaldības, datu koplietošanas un drošības noteikumiem.

Dalībvalstis tiek mudinātas sniegt līdzieguldījumu šajā projektā. Šādā gadījumā centri varētu efektīvāk koplietot un korelēt atklātos signālus un veidot kvalitatīvus draudu izlūkdatus, kas tālāk tiktu koplietoti ar *ISAC* un valstu iestādēm, tādējādi ļaujot pilnvērtīgāk apzināties situāciju. Mērķis būtu pakāpeniski savienot iespējami daudzus centrus Savienībā, lai veidotu kopīgas zināšanas un apmainītos ar labāko pieredzi. Šiem centriem tiks piešķirts atbalsts, lai tie uzlabotu incidentu atklāšanas, analīzes un reaģēšanas ātrumu, izmantojot vismodernākās MI un mašīnmācīšanās spējas un papildinot tās ar superdatošanas infrastruktūru, ko Savienībā izstrādājis Eiropas augstas veiktspējas datošanas kopuzņēmums[44].

Šis tīkls, izmantojot pastāvīgu kopdarbību un sadarbību, laikus brīdinās iestādes un visas ieinteresētās personas, tostarp kopējo kibervienību (sk. 2.1. iedaļu), par kiberdrošības incidentiem. **Tas kalpos kā reāls ES kiberdrošības vairogs**, nodrošinot uzticamu "sargtorņu" tīklu, kas spēs atklāt iespējamos draudus, pirms tie nodarījuši liela mēroga kaitējumu.

1.3. Īpaši droša sakaru infrastruktūra

Eiropas Savienības valdības satelītsakari[45] kā kosmosa programmas komponents nodrošinās drošas un izmaksu ziņā efektīvas kosmosā bāzētas saziņas spējas, lai nodrošinātu ES un tās dalībvalstu, tostarp valsts drošības jomas pārstāvju un ES iestāžu, struktūru un aģentūru, pārvaldīto drošības un drošuma ziņā kritiski svarīgo misiju un operāciju darbību.

Dalībvalstis ir apņēmušās sadarboties ar Komisiju, lai izvietotu drošu kvantu sakaru infrastruktūru (KSI) Eiropai[46]. KSI nodrošinās valstu iestādēm jaunu veidu, kā pārsūtīt konfidenciālu informāciju, izmantojot sevišķi drošu šifrēšanas veidu, kas ļauj aizsargāties pret kiberuzbrukumiem un ir veidots, izmantojot Eiropas tehnoloģijas. Tai būs divas galvenās sastāvdaļas: esošie sauszemes šķiedras sakaru tīkli, kas valsts un pārrobežu līmenī sasaista stratēģiskos objektus, un sasaistīti kosmiskie pavadoņi, kas aptver visu ES, ieskaitot tās aizjūras teritorijas[47]. Šī iniciatīva par jaunu un drošāku šifrēšanas veidu izstrādi un

[43]Sīkāka šo centru pārvaldības, darbības principu un finansēšanas kārtība, kā arī kārtība, kādā tie papildinās esošās struktūras, piemēram, digitālās inovācijas centrus, tiks izstrādāta vēlāk.

[44]https://ec.europa.eu/digital-single-market/lveurohpc-joint-undertaking.

[45]*GOVSATCOM* ir daļa no Savienības kosmosa programmas.

[46]*EuroQCI* deklarāciju ir parakstījusi lielākā daļa dalībvalstu, un tās izstrādei un infrastruktūras izvietošanai ir jānotiek 2021.–2027. gadā, izmantojot programmu "Apvārsnis Eiropa" un "Digitālā Eiropa", kā arī Eiropas Kosmosa aģentūras finansējumu ar attiecīgu pārvaldības kārtību; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

[47]Kosmosa komponentu ir nepieciešams attīstīt, lai sasniegtu attālinātus punkta-punkta savienojumus (> 1000 km), ko nav iespējams nodrošināt ar sauszemes infrastruktūru. Izmantojot kvantu mehānikas īpašības, KSI sākotnēji ļaus dalībniekiem droši apmainīties ar nejauši ģenerētām slepenām atslēgām ziņojumu šifrēšanai un atšifrēšanai. Tā arī ietvers testēšanas un atbilstības nodrošināšanas infrastruktūras izvietošanu, lai izvērtētu Eiropas kvantu sakaru ierīču un sistēmu atbilstību KSI infrastruktūrai, kā arī veiktu to sertificēšanu un validēšanu pirms to iekļaušanas KSI. Tā tiks izstrādāta tā, lai atbalstītu papildu lietotnes pēc tam, kad tās būs

izvietošanu, kā arī jaunu paņēmienu izstrādi kritiski svarīgas informācijas un datu aktīvu aizsardzībai var palīdzēt aizsargāt sensitīvu informāciju un attiecīgi — kritisko infrastruktūru.

No šī viedokļa, kā arī ejot vēl tālāk, Komisija izvērtēs iespējamo vairākorbītu drošā savienojuma sistēmu. Balstoties uz *GOVSATCOM* un KSI, tā integrēs mūsdienīgas tehnoloģijas (kvantisko datošanu, 5G, MI, perifērdatošanu), ievērojot visstingrāko kiberdrošības regulējumu, lai atbalstītu sākotnēji drošus pakalpojumus, piemēram, uzticamu, drošu un izmaksu ziņā efektīvu savienojamību un šifrētus sakarus kritiski svarīgām valdības darbībām.

1.4. Nākamās paaudzes platjoslas mobilo sakaru tīklu nodrošināšana

ES iedzīvotājiem un uzņēmumiem, kas lieto sarežģītas un novatoriskas lietotnes, kuras ļauj izmantot **5G un turpmāko paaudžu tīkli**, ir jāspēj izmantot visaugstākos drošības standartus. Dalībvalstis, sadarbojoties ar Komisiju un izmantojot *ENISA* atbalstu, 2020. gada janvārī ir izveidojušas ES 5G rīkkopu[48] — visaptverošu un objektīvu uz risku balstītu pieeju 5G kiberdrošībai, kas ir balstīta uz iespējamo mazināšanas plānu izvērtēšanu un visefektīvāko pasākumu identificēšanu. Turklāt ES konsolidē spējas 5G jomā un ārpus tās, lai izvairītos no atkarības un sekmētu ilgtspējīgas un daudzveidīgas piegādes ķēdes izveidi.

Komisija 2020. gada decembrī publicēja ziņojumu par to, kāda ietekme bijusi 2019. gada 26. marta Ieteikumam par 5G tīklu kiberdrošību[49]. Tas liecināja, ka kopš vienošanās par rīkkopu ir panākts ievērojams progress un ka vairums dalībvalstu ievēro grafiku, lai tuvākajā laikā pabeigtu īstenot ievērojamu rīkkopas daļu, lai gan šajā ziņā pastāv zināmas atšķirības un nenovērstas nepilnības, kas jau ir identificētas 2020. gada jūlijā publicētajā progresa ziņojumā[50].

Eiropadome 2020. gada oktobrī aicināja ES un dalībvalstis "pilnībā izmantot 5G kiberdrošības rīkkopu" un "piemērot attiecīgos ierobežojumus augsta riska piegādātājiem saistībā ar tiem galvenajiem aktīviem, kas ES koordinētajos riska novērtējumos definēti kā kritiski un sensitīvi, balstoties uz kopējiem objektīviem kritērijiem"[51].

ES un dalībvalstīm turpmāk būtu jānodrošina, ka identificētie riski ir pietiekami un koordinēti tikuši mazināti, jo īpaši attiecībā uz mērķi — mazināt saskarsmi ar augsta riska piegādātājiem un izvairīties no atkarības no šiem piegādātājiem valsts un Savienības līmenī, un ka tiek ņemta vērā jebkura jauna nozīmīga notikumu attīstība vai risks. Dalībvalstis tiek aicinātas pilnībā izmantot rīkkopu, veicot ieguldījumus digitālajā spējā un savienojamībā.

Pamatojoties uz ziņojumu par 2019. gada ieteikuma ietekmi, Komisija mudina dalībvalstis paātrināt darbu pie galveno rīkkopas pasākumu īstenošanas, lai to pabeigtu līdz 2021. gada otrajam ceturksnim. Tā arī aicina dalībvalstis turpināt uzraudzīt panākto progresu un nodrošināt pieeju tālāku saskaņošanu. Lai atbalstītu šo procesu, ES līmenī būs vērojama tiekšanās uz trim galvenajiem mērķiem: nodrošināt riska mazināšanas pieeju tālāku

---

sasniegušas nepieciešamo tehnoloģisko briedumu. Pašreizējais *OpenQKD* izmēģinājuma projekts (https://openqkd.eu/) ir šīs testēšanas un atbilstības infrastruktūras priekštecis.

[48]Paziņojums "Droša 5G ieviešana ES — ES rīkkopas īstenošana", COM (2020) 50.

[49] Komisijas ziņojums par ietekmi, kādu radījis Komisijas 2019. gada 26. marta Ieteikums par 5G tīklu kiberdrošību, 2020. gada 15. decembris.

[50]TID sadarbības grupas 2020. gada 24. jūlija ziņojums par rīkkopas īstenošanu.

[51]EUCO 13/20, Eiropadomes ārkārtas sanāksme (2020. gada 1. un 2. oktobrī) — secinājumi.

konverģenci ES, atbalstīt zināšanu pastāvīgu apmaiņu un spēju veidošanu, kā arī sekmēt piegādes ķēžu noturību un citus ES stratēģiskās drošības mērķus. Konkrētas ar šiem pamatmērķiem saistītas darbības ir izklāstītas šī paziņojuma īpašā pielikumā.

Komisija turpinās cieši sadarboties ar dalībvalstīm, lai ar *ENISA* atbalstu sasniegtu šos mērķus un darbības (sk. pielikumu).

ES 5G rīkkopas pieeja ir arī izraisījusi interesi trešās valstīs, kas patlaban izstrādā pieejas savu sakaru tīklu nodrošināšanai. Komisijas dienesti kopā ar Eiropas Ārējās darbības dienestu un ES delegāciju tīklu ir gatavi sniegt pasaules iestādēm papildu informāciju par tās visaptverošo, objektīvo un uz risku balstīto pieeju, ja tāda tiks lūgta.

1.5. Drošu lietu internets

Ikvienai savienotai lietai piemīt vājās vietas, kuru izmantošana var radīt plašas iedarbības sekas. Iekšējā tirgus noteikumi ietver aizsardzību pret nedrošiem produktiem un pakalpojumiem. Komisija jau strādā pie tā, lai nodrošinātu **pārredzamus drošības risinājumus un sertifikāciju atbilstīgi Kiberdrošības aktam** un stimulētu drošus produktus un pakalpojumus, nepasliktinot to veiktspēju[52]. Tā 2021. gada pirmajā ceturksnī pieņems pirmo Savienības mainīgo darba programmu (kas tiks aktualizēta ne retāk kā reizi trijos gados), lai ļautu nozarei, valstu iestādēm un standartizācijas struktūrām savlaicīgi sagatavoties gaidāmajām Eiropas kiberdrošības sertifikācijas shēmām[53]. Izplatoties lietu internetam, ir nepieciešams stiprināt izpildāmus noteikumus, lai gan nodrošinātu kopējo noturību, gan stiprinātu kiberdrošību.

Komisija apsvērs visaptverošu pieeju, tajā skaitā iespējamus **jaunus horizontālus noteikumus, kā uzlabot visu iekšējā tirgū laisto savienoto produktu un ar tiem saistīto pakalpojumu kiberdrošību**[54]. Šie noteikumi varētu ietvert **jaunu rūpības pienākumu savienoto ierīču ražotājiem**, lai tie risinātu programmatūras vājās vietas, ieskaitot programmatūras un drošības atjauninājumu turpmāku nodrošināšanu, kā arī personas un citu sensitīvu datu dzēšanu to kalpošanas laika beigās. Ar šiem noteikumiem tiktu stiprināta iniciatīva par "tiesībām atjaunināt novecojušu programmatūru", kas sākotnēji tika piedāvāta Aprites ekonomikas rīcības plānā un papildina pašreizējos pasākumus, kuri attiecas uz īpašiem produktu veidiem, piemēram, obligātas prasības konkrētu bezvadu produktu laišanai tirgū (pieņemot deleģēto aktu saskaņā ar Radioiekārtu direktīvu[55]), kā arī mērķi no 2022. gada jūlija īstenot mehānisko transportlīdzekļu kiberdrošības noteikumus visiem jaunu

[52] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 atcelšanu (Kiberdrošības akts). Kiberdrošības akts sekmē IKT sertifikāciju ES līmenī, paredzot Eiropas kiberdrošības sertifikācijas satvaru, ar ko izveido brīvprātīgas Eiropas kiberdrošības sertifikācijas shēmas, lai Savienībā IKT produktiem, IKT pakalpojumiem un IKT procesiem nodrošinātu pietiekami augstu kiberdrošības līmeni, kā arī mazinātu Savienības iekšējā tirgus sadrumstalotību attiecībā uz kiberdrošības sertifikācijas shēmām. Vienlaikus kiberdrošības "reitingus" veidojošie uzņēmumi bieži vien atrodas ārpus ES, kur to pārredzamība un pārraudzība ir ierobežota; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[53] To paredz Kiberdrošības akta 47. panta 5. punkts.

[54] Padomes secinājumos izteikts aicinājums apsvērt horizontālu tiesību aktu attiecībā uz savienoto ierīču kiberdrošību; 13629/20, 2020. gada 2. decembris.

[55] Direktīva 2014/53/ES

veidu transportlīdzekļiem[56]. Turklāt tie balstītos uz ierosināto produktu vispārējās drošības noteikumu pārskatīšanu, kas tieši nerisina kiberdrošības jautājumu[57].

1.6. Lielāka globālā interneta drošība

Interneta funkcionalitāti un integritāti visā pasaulē nodrošina pamatprotokolu un atbalstošās infrastruktūras kopums[58]. Šis kopums ietver DNS, kā arī tās hierarhisko un deleģēto zonu sistēmu, hierarhiski sākot ar saknes zonu un 13 DNS saknes serveriem[59], uz kuriem balstās viss globālais tīmeklis. Komisija plāno izstrādāt **ES finansētu ārkārtas situāciju plānu rīcībai ekstremālu scenāriju gadījumā, kas ietekmētu globālās DNS sakņu sistēmas integritāti un pieejamību**. Tā sadarbosies ar *ENISA*, dalībvalstīm, abiem ES DNS saknes servera operatoriem[60] un daudzu ieinteresēto personu kopienu, lai izvērtētu, kāda ir šo dalībnieku loma interneta globālas pieejamības garantēšanā jebkuros apstākļos.

Lai klients piekļūtu interneta resursam, kuram ir konkrēts domēna nosaukums, tā pieprasījums (parasti — pēc vienotā resursu vietrāža jeb URL), vēršoties pie DNS serveriem, ir jāpārveido vai "jāatrisina", lai iegūtu IP adresi. Tomēr ES iedzīvotāji un organizācijas arvien vairāk paļaujas uz dažiem publiskiem domēnu nosaukumu atrisinātājiem, kurus uztur trešo valstu struktūras. Šāda DNS atrisināšanas konsolidācija dažu uzņēmumu rokās[61] padara pašu atrisināšanas procesu neaizsargātu tādu notikumu gadījumā, kas ietekmē vienu nozīmīgu pakalpojumu sniedzēju, kā arī apgrūtina ES iestādēm iespēju vērsties pret iespējamiem ļaunprātīgiem kiberuzbrukumiem un nozīmīgiem ģeopolitiskiem un tehniskiem incidentiem[62].

Lai mazinātu ar tirgus koncentrāciju saistītās drošības problēmas, Komisija mudinās attiecīgās ieinteresētās personas, ieskaitot ES uzņēmumus, interneta pakalpojumu sniedzējus un pārlūkprogrammu izstrādātājus pieņemt DNS atrisinātāju dažādošanas stratēģiju. Komisija arī plāno sekmēt drošu interneta savienojamību, atbalstot publiska **Eiropas DNS atrisinātāja pakalpojuma** izstrādi. Iniciatīva "DNS4EU" piedāvās alternatīvu Eiropas pakalpojumu, ar ko piekļūt globālajam internetam. *DNS4EU* būs pārredzama, atbildīs jaunākajiem standartiem un noteikumiem attiecībā uz drošību, datu aizsardzību un privātumu (integrētu aizsardzību un

---

[56] Atbilst 2020. gada jūnijā pieņemtajiem ANO noteikumiem; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[57] Produktu vispārējās drošības pašreizējo noteikumu (Direktīva 2001/95/EK) pārskatīšana; ir paredzēti arī ierosināti pielāgoti noteikumi par ražotāju atbildību digitālajā kontekstā ES atbildības tiesiskā regulējuma ietvaros.

[58] "Atklātā interneta publiskais kodols, proti, tā galvenie protokoli un infrastruktūra, kas ir globāls sabiedrisks labums, nodrošina interneta būtiskākās funkcijas kopumā un ir tā normālas darbības pamats. *ENISA* būtu jāatbalsta atklātā interneta publiskā kodola drošība un tā funkcionēšanas stabilitāte, tostarp — bet ne tikai — attiecībā uz galvenajiem protokoliem (jo īpaši DNS, BGP un IPv6), domēnu nosaukumu sistēmas darbību (piemēram, visu augstākā līmeņa domēnu darbība) un sakņu zonas darbību"; Kiberdrošības akta 23. apsvērums.

[59] https://www.iana.org/domains/root/servers.

[60] i.root serveri, ko darbina *Netnod* (Zviedrija), un k.root serveri, ko darbina *RIPE NCC* (Nīderlande).

[61] "Consolidation in the DNS resolver market – how much, how fast how dangerous?" ( ), "Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services" ( ).

[62] Ir arī pierādījumi, kas liecina, ka DNS datus var izmantot profilēšanai, kas ietekmē privātumu un datu aizsardzības tiesības.

aizsardzību pēc noklusējuma), kā arī veidos daļu no Eiropas datu un mākoņpakalpojumu industriālās alianses[63].

Komisija, sadarbojoties ar dalībvalstīm un nozari, **paātrinās svarīgu interneta standartu, ieskaitot IPv6**[64], **kā arī plaši atzītu interneta drošības standartu un DNS, maršrutēšanas un e-pasta drošības labās prakses**[65] **apgūšanu**, neizslēdzot regulatīvus pasākumus, piemēram, Eiropas turpināmības klauzulu attiecībā uz IPv4, kas vadītu tirgu, ja netiktu panākts pietiekams progress ceļā uz to pieņemšanu. ES būtu jāveicina (kā tas tiek darīts, piemēram, stratēģijā "ES un Āfrika"[66]) šo standartu īstenošana partnervalstīs kā paņēmiens, ar kuru atbalstīt globāla un atvērta interneta attīstību un pretoties slēgtiem, uz kontroli balstītiem interneta modeļiem. Visbeidzot, Komisija apsvērs nepieciešamību pēc mehānisma, ar kuru sistemātiskāk uzraudzīt un vākt apkopotus datus par interneta datplūsmu, kā arī sniegt ieteikumus attiecībā uz iespējamajiem traucējumiem[67].

1.7. Pastiprināta klātbūtne tehnoloģiju piegādes ķēdē

ES plānotais finanšu atbalsts kiberdrošai digitālajai pārveidei saskaņā ar 2021.–2027. gada daudzgadu finanšu shēmu sniedz tai unikālu iespēju apvienot aktīvus, lai saskaņā ar tās vērtībām un prioritātēm stiprinātu tās industriālo stratēģiju[68] un līdera lomu digitālo tehnoloģiju un kiberdrošības jomā visā digitālajā piegādes ķēdē (ieskaitot datus un mākoņpakalpojumus, nākamās paaudzes procesoru tehnoloģijas, sevišķi drošu savienojamību un 6G tīklus). Publiskā sektora intervencei ir jāizmanto instrumenti, ko piedāvā ES publiskā iepirkuma regulējums un svarīgi projekti visas Eiropas interesēs. Papildus tam tā var iespējot privātus ieguldījumus, izmantojot publiskās un privātās partnerības (tostarp balstoties uz pieredzi, kas gūta saistībā ar līgumisko publisko un privāto partnerību attiecībā uz kiberdrošību un tās īstenošanu Eiropas Kiberdrošības organizācijā), MVU vai industriālo aliansu atbalsta riska kapitālu, tehnoloģisko spēju stratēģijas.

Īpaša uzmanība tiks veltīta arī tehniskā atbalsta instrumentam[69] un tam, kā MVU (jo īpaši pārskatītās TID direktīvas darbības jomā neietilpstošie) vislabāk varētu izmantot jaunākos kiberdrošības līdzekļus, tajā skaitā izmantojot īpašas darbības digitālās inovācijas centros programmā "Digitālā Eiropa". Mērķis ir panākt, ka dalībvalstis veic līdzīga apmēra ieguldījumus, ko nozare līdzfinansē saskaņā ar partnerību, kas kopīgi ar dalībvalstīm tiek pārvaldīta ierosinātajā **Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centrā un Nacionālo koordinācijas centru tīklā (*CCCN*)**. *CCCN*, uzklausot nozares un akadēmiskās vides viedokļus, būtu jāieņem svarīga loma ES kiberdrošības tehnoloģiskās suverenitātes attīstīšanā, veidojot spējas nodrošināt sensitīvu infrastruktūru, piemēram, 5G, tādējādi mazinot atkarību no pārējās pasaules vissvarīgāko tehnoloģiju ziņā.

---

[63] Kopīgs paziņojums "Nākamās paaudzes mākoņpakalpojumu veidošana ES uzņēmumiem un publiskajam sektoram"; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[64] IPv6 ieviešana patlaban ir iegājusi tālākā attīstības posmā, ņemot vērā būtisko IPv4 adrešu piedāvājuma deficītu un izmaksu pieaugumu. Tomēr IPv6 izvietošana ES nav notikusi vienveidīgi.

[65] Šie standarti ir, piemēram, *DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE*, kā arī maršrutēšanas normas un labākā prakse, piemēram, Savstarpējās maršrutēšanas drošības normas (*MANRS*).

[66] Kopīgs paziņojums "Ceļā uz visaptverošu stratēģiju ar Āfriku", 9.3.2020., JOIN(2020) 4 final.

[67] Šāds "interneta novērošanas centrs" varētu ietilpt Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra darbības jomā; priekšlikums Regulai, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu, COM(2018) 630 final.

[68] Paziņojums "Jauna Eiropas industriālā stratēģija", COM(2020) 102 final.

[69] https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=COM:2020:0409:FIN .

Komisija plāno atbalstīt (iespējams — *CCCN* ietvaros) īpašas kiberdrošības maģistra studiju programmas izstrādi un veicināt vienotu Eiropas kiberdrošības pētniecības un inovācijas ceļvedi pēc 2020. gada. Ar *CCCN* starpniecību veiktie ieguldījumi balstītos arī uz sadarbību pētniecības un izstrādes jomā, ko īstenotu kiberdrošības izcilības centru tīkli, apvienojot Eiropas labākās pētniecības komandas un nozari, lai izstrādātu un īstenotu vienotas pētniecības programmas atbilstīgi Eiropas kiberdrošības organizācijas ceļvedim[70]. Komisija turpinās izmantot *ENISA* un Eiropola paveikto pētniecības darbu, kā arī programmas "Apvārsnis Eiropa" ietvaros turpinās atbalstīt atsevišķus interneta inovatorus, kas izstrādā privātumu uzlabojošas un drošas saziņas tehnoloģijas, balstoties uz atvērtā pirmkoda programmatūru un aparatūru, kā tas pašlaik notiek Nākamās paaudzes interneta iniciatīvā.

1.8. Kiberlietpratīgs ES darbaspēks

ES centieni celt darbaspēka kvalifikāciju, attīstīt, piesaistīt un noturēt labākos kiberdrošības talantus un ieguldīt pasaules līmeņa pētniecībā un inovācijā ir svarīgs komponents vispārējā aizsardzībā pret kiberdraudiem. Šai jomai ir liels potenciāls. Tādēļ ir jāvelta īpaša uzmanība daudzveidīgāku talantu attīstīšanai, piesaistei un noturēšanai. Pārskatītais rīcības plāns digitālās izglītības jomā uzlabos informētību par kiberdrošību iedzīvotāju, jo īpaši bērnu un jauniešu, un organizāciju, jo īpaši MVU, vidū[71]. Tas arī stimulēs sieviešu dalību zinātnes, tehnoloģijas, inženierzinātņu un matemātikas (*STEM*) izglītībā, kā arī IKT darbvietu prasmju pilnveidē un digitālo prasmju pārkvalifikācijā. Turklāt Komisija kopā ar Eiropola ES Intelektuālā īpašuma biroju, *ENISA*, dalībvalstīm un privāto sektoru izstrādās informētības rīkus un norādījumus par to, kā uzlabot ES uzņēmumu noturību **pret intelektuālā īpašuma kiberzādzībām**[72].

Arī izglītībai — ieskaitot profesionālo izglītību un apmācību (PIA), informētību un mācības — būtu jāuzlabo kiberdrošības un kiberaizsardzības prasmes ES līmenī. Šajā nolūkā attiecīgajiem ES dalībniekiem, piemēram, *ENISA*, Eiropas Aizsardzības aģentūrai (EAA) un Eiropas Drošības un aizsardzības koledžai (EDAK)[73], būtu jācenšas panākt to veikto attiecīgo darbību sinerģija.

Stratēģiskās iniciatīvas

ES būtu jānodrošina:

- pārskatītās TID direktīvas pieņemšana;
- drošu lietu interneta regulatīvie pasākumi;
- ka 2021.–2027. gadā ar *CCCN* starpniecību tiek panākts, ka ieguldījumi kiberdrošībā (jo īpaši, izmantojot programmu "Digitālā Eiropa", "Apvārsnis Eiropa" un atveseļošanas mehānismu) sasniedz līdz 4,5 miljardiem EUR publisko un privāto ieguldījumu veidā;
- MI atbalstītu drošības operāciju centru ES tīkls un sevišķi droša sakaru infrastruktūra, kas izmanto kvantu tehnoloģijas;

[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies.
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_lv.
[72] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2187.
[73] Izmantojot kiberjomas izglītības, apmācības, mācību un izvērtēšanas platformu (*ETEE*).

- plaša kiberdrošības tehnoloģiju apgūšana, digitālās inovācijas centros paredzot īpašu atbalstu MVU;
- ES DNS atrisinātāja pakalpojuma izstrāde kā droša un atvērta alternatīva ES pilsoņiem, uzņēmumiem un valsts pārvaldei, lai piekļūtu internetam, un
- 5G rīkkopas īstenošanas pabeigšana līdz 2021. gada otrajam ceturksnim (sk. pielikumu).

2. NOVĒRŠANAS, ATTURĒŠANAS UN REAĢĒŠANAS OPERATĪVO SPĒJU VEIDOŠANA

Kiberincidenti neatkarīgi no tā, vai tās ir nejaušas vai tīšas noziedznieku, valsts un nevalstisko dalībnieku darbības, var nodarīt ļoti lielu kaitējumu. To mērogs un sarežģītība, kas bieži ietver trešo personu pakalpojumu, aparatūras un programmatūras ļaunprātīgu izmantošanu mērķa kompromitēšanai, ļoti apgrūtina pretošanos ES kolektīvo apdraudējumu videi, ja netiek sistemātiski un visaptveroši koplietota informācija un nenotiek sadarbība vienotai reaģēšanai. ES mērķis, **pilnībā īstenojot regulatīvos rīkus, piesaistīšanu un sadarbību**, ir sniegt dalībvalstīm atbalstu šo valstu iedzīvotāju, viņu ekonomisko un valsts drošības interešu aizsardzībai, pilnībā ievērojot pamattiesības un brīvības, kā arī tiesiskumu. Vairākas kopienas, ko veido tīkli, ES iestādes, struktūras un aģentūras, kā arī dalībvalstu iestādes, atbild par kiberdraudu novēršanu, atturēšanu, kavēšanu, kā arī reaģēšanu uz tiem, izmantojot to attiecīgos instrumentus un iniciatīvas[74]. Šīs kopienas ir: i) TID iestādes, piemēram, *CSIRT*, un reaģēšanas spējas katastrofu gadījumos, ii) tiesībaizsardzības un tiesu iestādes, iii) kiberdiplomātija un iv) kiberaizsardzība.

2.1. Kopēja kibervienība

Kopēja kibervienība kalpotu kā virtuāla un fiziska platforma, kurā sadarbotos dažādas ES kiberdrošības kopienas un kas būtu orientēta uz operatīvo un tehnisko koordināciju cīņai pret nopietniem pārrobežu kiberincidentiem un apdraudējumiem.

Kopējā kibervienība būtu svarīgs solis ceļā uz **Eiropas kiberdrošības krīzes pārvarēšanas satvara** pabeigšanu. Kā izklāstīts Komisijas priekšsēdētājas politiskajās pamatnostādnēs[75], vienībai būtu jāļauj dalībvalstīm, ES iestādēm, struktūrām un aģentūrām pilnībā izmantot esošās struktūras, resursus un spējas, kā arī sekmēt domāšanas veidu "**vajadzība pēc apmaiņas**". Tā sniegtu iespēju konsolidēt līdz šim panākto progresu 2017. gada Ieteikuma par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm ("Plāns")[76]

[74]Ieskaitot Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) atbalstu operatīvajai sadarbībai un krīzes pārvarēšanai, *CSIRT* tīklu, Kiberkrīžu kontaktpersonu organizācijas tīklu (*CyCLONe*, kas saskaņā ar pārskatīto TID direktīvu kļūs par *EU-CyCLONe*), TID sadarbības grupu, "rescEU", Eiropas Kibernoziedzības apkarošanas centru un Eiropola Kopīgo kibernoziedzības apkarošanas darba grupu un tiesībaizsardzības iestāžu ārkārtas reaģēšanas protokolu, ES Izlūkošanas un situāciju centru (*EU INTCEN*) un kiberdiplomātijas instrumentu kopumu, Vienoto izlūkdatu analīzes procedūru (*SIAC*); Pastāvīgās strukturētās sadarbības (*PESCO*) satvara kiberjomas projektus, jo īpaši "Kiberdrošības ātrās reaģēšanas vienības un savstarpēja palīdzība kiberdrošības jomā" (*CRRT*).

[75]"Eiropas Savienība, kas tiecas uz augstākiem mērķiem: Mana programma Eiropai", Eiropas Komisijas priekšsēdētāja amata kandidātes Urzulas fon der Leienas politikas pamatnostādnes nākamajai Eiropas Komisijai (2019–2024).

[76]Ieteikums par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm, 13.9.2017., C(2017) 6100 final.

īstenošanā. Tā arī sniegtu iespēju vēl vairāk stiprināt sadarbību attiecībā uz Plāna arhitektūru un izmantotu progresu, kas jo īpaši sasniegts TID sadarbības grupā un *CyCLONe* tīklā.

Šādi būtu iespējams risināt **divas galvenās nepilnības**, kas patlaban palielina ievainojamību un rada neefektivitāti reaģēšanā uz pārrobežu draudiem un incidentiem, kas skar Savienību. Pirmkārt, civilās, diplomātiskās, tiesībaizsardzības un aizsardzības kiberdrošības **kopienām** vēl nav kopējas telpas, kurā attīstīt strukturētu sadarbību un sekmēt operatīvo un tehnisko sadarbību. Otrkārt, attiecīgās kiberdrošības jomas ieinteresētās personas vēl nav spējušas pilnībā izmantot operatīvās sadarbības un savstarpējās palīdzības **potenciālu** esošajos tīklos un kopienās. Tas attiecas arī uz to, ka trūkst platformas, kas ļautu īstenot operatīvo sadarbību ar privāto sektoru. Vienībai būtu jāuzlabo un jāpaātrina koordinācija, kā arī jāļauj ES stāties pretī un reaģēt uz liela mēroga kiberincidentiem un krīzēm.

Kopējā kibervienība nebūtu papildu atsevišķa struktūra, kā arī neietekmētu valsts kiberdrošības iestāžu un ES dalībnieku kompetenci un pilnvaras. Vienība darbotos tikai kā atbalsta mehānisms, kurā dalībnieki varētu izmantot cits cita atbalstu un zinātību, jo īpaši gadījumos, kad dažādām kiberkopienām ir nepieciešams cieši sadarboties. Vienlaikus nesenie notikumi ir apliecinājuši, ka ES ir nepieciešams celt mērķu vērienīgumu un uzlabot gatavību saskarties ar kiberdraudu ainu un realitāti. ES dalībnieki (Komisija, ES aģentūras un struktūras) būs gatavi būtiski palielināt resursus un spējas kā daļu no ieguldījuma KKV, lai uzlabotu savu gatavību un noturību.

Ar kopējo kibervienību tiktu sasniegti trīs galvenie mērķi. Pirmkārt, tā nodrošinātu visu kiberdrošības kopienu **gatavību**; otrkārt, daloties ar informāciju, tiktu nodrošināta pastāvīga un kopīga situācijas **apzināšanās**; treškārt, tā stiprinātu koordinētu **reaģēšanu** un atgūšanos. Lai sasniegtu šos mērķus, vienībai būtu jābalstās uz skaidri noteiktiem **blokiem un mērķiem**, piemēram, garantētu **drošu un ātru informācijas koplietošanu**, dalībnieku **sadarbības** uzlabošanu, tostarp attiecībā uz dalībvalstu un attiecīgo ES struktūru mijiedarbību, strukturētu **partnerattiecību veidošanu ar uzticamu nozares** bāzi, kā arī koordinētas pieejas sekmēšanu **sadarbībā ar ārējiem partneriem**. Lai to panāktu, balstoties uz valsts un ES līmenī pieejamo spēju plānošanu, vienība varētu sekmēt sadarbības satvara izstrādi.

Lai kopējā kibervienība kļūtu par ES kiberdrošības operatīvās sadarbības centrmezglu, Komisija sadarbosies ar dalībvalstīm un attiecīgām ES iestādēm, struktūrām un aģentūrām, ieskaitot *ENISA*, *CERT-EU* un Eiropolu, sekmējot **pakāpenisku un iekļaujošu pieeju** un pilnībā ievērojot visu iesaistīto pušu kompetenci un pilnvaras. Atbilstīgi šai pieejai vienība varētu veicināt turpmāku sadarbību starp konkrētas kiberkopienas dalībniekiem, ja tie to uzskatīs par nepieciešamu.

Kopējās kibervienības īstenošanai tiek ierosināti četri galvenie pasākumi:

- *definēt*, plānojot valsts un ES līmenī pieejamās spējas;
- *sagatavot*, izveidojot strukturētas sadarbības un palīdzības satvaru;
- *izvietot*, īstenojot satvaru un izmantojot dalībnieku sniegtos resursus, lai kopējā kibervienība uzsāktu darbu;
- *paplašināt*, stiprinot koordinētas reaģēšanas spējas un uzklausot nozares un partneru viedokļus.

Balstoties uz rezultātiem pēc apspriešanās ar dalībvalstīm, ES iestādēm, struktūrām un aģentūrām[77], Komisija, piedaloties Augstajam pārstāvim atbilstīgi tā kompetencei, līdz 2021. gada februārim iepazīstinās ar **kopējās kibervienības definēšanas, sagatavošanas, izvietošanas un paplašināšanas** procesu, starpposma mērķrādītājiem un grafiku.

2.2. Cīņa pret kibernoziedzību

Mūsu atkarība no tiešsaistes rīkiem ir ģeometriskā progresijā paplašinājusi kibernoziedznieku uzbrukumu iespējas un novedusi pie situācijas, kurā gandrīz visu veidu noziegumu izmeklēšanai piemīt digitāls elements. Turklāt svarīgas mūsu sabiedrības daļas apdraud kiberjomas dalībnieki un personas, kas izmanto kiberrīkus nelikumīgu darbību plānošanai un veikšanai. Tādēļ pastāv cieša saikne ar ES kopējo drošības politiku, ko atspoguļo 2020. gada Drošības savienības stratēģijas un ES terorisma apkarošanas programmas[78] kiberelementi.

Efektīva cīņa pret kibernoziegumiem ir svarīgs kiberdrošības garantēšanas faktors: atturēšanu nav iespējams panākt tikai ar noturību, bet ir nepieciešama arī pārkāpēju atklāšana un kriminālvajāšana. Līdz ar to ir svarīgi sekmēt kiberdrošības dalībnieku un tiesībaizsardzības iestāžu sadarbību un informācijas apmaiņu. Šim nolūkam ES līmenī jau ir izveidota cieša sadarbība starp Eiropolu un *ENISA*, kuras ietvaros šīs struktūras ir organizējušas kopīgas konferences un darbseminārus, kā arī sniegušas Komisijai, dalībvalstīm un citām ieinteresētām personām kopīgus ziņojumus par kiberdraudiem un tehnoloģiskajām problēmām. Komisija turpinās atbalstīt šo integrēto pieeju, lai nodrošinātu saskaņotu un efektīvu reaģēšanu, balstoties uz visaptverošu informācijas ainu.

ES un valstu iestādēm būtu jāpaplašina un jāuzlabo tiesībaizsardzības iestāžu spēja izmeklēt kibernoziegumus kā svarīgs šīs reaģēšanas elements, pilnībā ievērojot pamattiesības un cenšoties panākt nepieciešamo līdzsvaru starp dažādām tiesībām un interesēm. ES būtu jāspēj apkarot kibernoziedzību, pilnībā īstenojot mērķim piemērotus tiesību aktus, īpašu uzmanību veltot cīņai pret seksuālu vardarbību pret bērniem internetā un digitālajai izmeklēšanai, tostarp noziedzībai "tumšajā tīklā". Tiesībaizsardzības iestādēm jābūt pilnībā aprīkotām digitālās izmeklēšanas veikšanai. Šim nolūkam Komisija ierosinās tiesībaizsardzības iestāžu digitālo spēju uzlabošanas rīcības plānu, sniedzot tām nepieciešamās prasmes un rīkus. Eiropols arī turpinās attīstīt savu zinātības centra funkciju, lai atbalstītu valstu tiesībaizsardzības iestādes cīņā pret kibernoziegumiem un kiberatkarīgiem noziegumiem, palīdzot definēt kopējus kriminālistikas standartus (izmantojot Eiropola inovācijas laboratoriju un centru). Ir nepieciešams, lai dalībvalsts attiecīgi īstenotu visas minētās darbības, un tās tiek mudinātas izmantot iekšējās drošības fonda valstu programmas un ierosināt programmas, atsaucoties uzaicinājumiem iesniegt priekšlikumus tematiskā mehānisma ietvaros.

Komisija izmantos visus pieejamos līdzekļus, ieskaitot pārkāpumu procedūras, lai nodrošinātu, ka tiek pilnībā transponēta un īstenota 2013. gada Direktīva par uzbrukumiem informācijas sistēmām[79], ieskaitot tās noteikumu, kas paredz dalībvalstu pienākumu sniegt statistiku. Ar to labāk novērsīs domēna nosaukumu ļaunprātīgu izmantošanu, tostarp

[77]Dalībvalstu (tajā skaitā Blue OLEx20 gaitā, kur bija pulcējušies valstu kiberdrošības iestāžu vadītāji), ES iestāžu, struktūru un aģentūru apspriešanās no 2020. gada jūlija līdz novembrim.
[78]Paziņojums "ES terorisma apkarošanas programma: paredzēt, novērst, aizsargāt, reaģēt", 9.12.2020., COM(2020) 795 final.
[79]Direktīva 2013/40/ES par uzbrukumiem informācijas sistēmām.

attiecīgos gadījumos — nelikumīga satura izplatīšanai, un centīsies panākt precīzu reģistrācijas datu pieejamību, turpinot kontaktēties ar Piešķirto nosaukumu un numuru interneta korporāciju (*ICANN*) un citām interneta pārvaldības sistēmas ieinteresētajām personām, jo īpaši *ICANN* valdības padomdevējas komitejas sabiedrības drošības darba grupā. Pārskatītās TID direktīvas priekšlikums attiecīgi paredz uzturēt precīzas un pilnīgas domēna nosaukumu un to reģistrācijas datu jeb "*WHOIS* datu" bāzes, kā arī nodrošināt likumīgu piekļuvi šiem datiem, ciktāl tas ir svarīgi DNS drošības, stabilitātes un noturības nodrošināšanai.

Komisija arī turpinās darbu pie tā, lai nodrošinātu attiecīgus kanālus un precizētu noteikumus, kā iegūt pārrobežu piekļuvi elektroniskajiem pierādījumiem kriminālizmeklēšanā (nepieciešami 85 % izmeklēšanu, 65 % no visiem pieprasījumiem tiek iesniegti pakalpojumu sniedzējiem citā jurisdikcijā), sekmējot "e-pierādījumu paketes" un praktisku pasākumu pieņemšanu un vēlāku īstenošanu[80]. Eiropas Parlamentam un Padomei ir svarīgi ātri pieņemt priekšlikumus par e-pierādījumiem, lai praktiķiem nodrošinātu efektīvu rīku. E-pierādījumiem ir jābūt lasāmiem, tādēļ Komisija turpinās darbu pie tiesībaizsardzības spēju atbalsta digitālās izmeklēšanas jomā, tostarp attiecībā uz šifrēšanu, ar ko sastopas kriminālizmeklētāji, vienlaikus pilnībā saglabājot tās funkciju — aizsargāt pamattiesības un kiberdrošību.

2.3. ES kiberdiplomātijas instrumentu kopums

ES ir izmantojusi **kiberdiplomātijas instrumentu kopumu**[81], lai novērstu ļaunprātīgas kiberdarbības, atturētu no to veikšanas, kavētu tās un reaģētu uz tām. Pēc tam, kad 2019. gada maijā tika ieviests tiesiskais regulējums mērķtiecīgiem ierobežojošiem pasākumiem pret kiberuzbrukumiem[82], ES 2020. gada jūlijā šim režīmam pakļāva sešas fiziskas personas un trīs struktūras, kas ir atbildīgas par kiberuzbrukumiem, kas skar ES un tās dalībvalstis, vai ir tajos iesaistītas[83]. 2020. gada oktobrī tika minētas vēl divas personas un viena struktūra[84]. Ļaunprātīgas kiberdarbības, ieskaitot lēni iedarbīgas darbības, ir jāapkaro, izmantojot

[80]COM(2018) 225 un 226; C(2020) 2779 final. Konkrēti, projekts *SIRIUS* nesen saņēma papildu finansējumu no partnerības instrumenta, lai uzlabotu likumīgu pārrobežu piekļuvi e-pierādījumiem kriminālizmeklēšanā (nepieciešami 85 % no smagu noziegumu izmeklēšanām, bet 65 % no visiem pieprasījumiem tiek iesniegti pakalpojumu sniedzējiem citā jurisdikcijā) un izveidotu saderīgus starptautiskus noteikumus.

[81] https://www.consilium.europa.eu/lv/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/.

[82]Padomes Lēmums (KĀDP) 2019/797 (2019. gada 17. maijs) par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (OV L 129 I, 17.5.2019., 13. lpp.) un Padomes Regula (ES) 2019/796
(2019. gada 17. maijs) par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (OV L 129 I, 17.5.2019., 1. lpp.).

[83] Padomes Lēmums (KĀDP) 2020/1127 (2020. gada 30. jūlijs), ar ko groza Lēmumu (KĀDP) 2019/797 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (ST/9564/2020/INIT) (OV L 246, 30.7.2020., 12.–17. lpp.); un Padomes Īstenošanas regula (ES) 2020/1125 (2020. gada 30. jūlijs), ar ko īsteno Regulu (ES) 2019/796 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (ST/9568/2020/INIT) (OV L 246, 30.7.2020., 4.–9. lpp.).

[84] Padomes Lēmums (KĀDP) 2020/1537 (2020. gada 22. oktobris), ar ko groza Lēmumu (KĀDP) 2019/797 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (OV L 351 I, 22.10.2020., 5.–7. lpp.); un Padomes Īstenošanas regula (ES) 2020/1536 (2020. gada 22. oktobris), ar ko īsteno Regulu (ES) 2019/796 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (OV L 351 I, 22.10.2020., 1.–4. lpp.).

efektīvu un visaptverošu kopēju ES diplomātisko reakciju, kas ietver visus ES līmenī pieejamos pasākumus.

Straujai un efektīvai ES diplomātiskajai reakcijai ir nepieciešama noturīga un kopēja situācijas apzināšanās un spēja ātri izstrādāt kopēju ES nostāju. Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos sekmēs un atvieglos **dalībvalstu ES kiberizlūkošanas darba grupas** izveidi ES Izlūkošanas un situāciju centrā (*INTCEN*), lai sekmētu izlūkdienestu stratēģisku sadarbību attiecībā uz kiberdraudiem un darbībām. Šis darbs papildus atbalstīs ES situācijas apzināšanos un lēmumu pieņemšanu attiecībā uz kopēju diplomātisko reakciju. Darba grupai ir jāsadarbojas ar esošajām struktūrām[85], tostarp, ja nepieciešams, ar hibrīdās un ārvalstu iejaukšanās draudiem plašākā nozīmē strādājošajām struktūrām, lai apkopotu un izvērtētu situācijas apzināšanos.

Lai stiprinātu spējas novērst, atturēt, kavēt ļaunprātīgu uzvedību kibertelpā un reaģēt uz to, Augstais pārstāvis, piedaloties Komisijai atbilstīgi tās kompetencei, ES iesniegs priekšlikumu sīkāk definēt tās **kiberatturēšanas pozīciju**. Pamatojoties uz darbu, kas līdz šim paveikts kiberdiplomātijas instrumentu kopuma satvarā, pozīcijai būtu jāsekmē atbildīga valstu uzvedība un sadarbība kibertelpā, īpaši norādot, kā pretoties kiberuzbrukumiem, kam ir visbūtiskākā ietekme, jo īpaši tiem, kas ietekmē mūsu kritisko infrastruktūru, demokrātiskās institūcijas un procesus[86], kā arī uzbrukumiem piegādes ķēdēm un kiberiespējotām intelektuālā īpašuma zādzībām. Pozīcijā būtu jāizklāsta, kā ES un dalībvalstis varētu izmantot politiskos, ekonomiskos, diplomātiskos, juridiskos un stratēģiskās komunikācijas instrumentus pret ļaunprātīgām kiberdarbībām, kā arī jārisina jautājums, kā ES un dalībvalstis varētu uzlabot spējas noteikt ļaunprātīgu kiberdarbību veicējus. Papildus tam Augstais pārstāvis plāno kopā ar Padomi un Komisiju izvērtēt **papildu pasākumus kiberdiplomātijas instrumentu kopuma ietvaros**, ieskaitot iespēju paredzēt papildu ierobežojošus pasākumus, kā arī izvērtēt **kvalificēta vairākuma balsošanu (KVB) attiecībā uz iekļaušanu pret kiberuzbrukumiem vērstā horizontālo sankciju režīma sarakstā**. ES arī būtu jāpieliek papildu pūles, lai **stiprinātu sadarbību ar starptautiskajiem partneriem**, ieskaitot NATO, nolūkā virzīt vienotu izpratni par drošības apdraudējuma ainu, izstrādāt sadarbības mehānismus un identificēt uz sadarbību vērstu diplomātisko reakciju.

Augstais pārstāvis, piedaloties Komisijai, ierosinās arī atjaunināt **kiberdiplomātijas instrumentu kopuma īstenošanas nostādnes[87]**, tostarp ņemot vērā lēmumu pieņemšanas procesa efektivitātes celšanu, un turpina regulāri organizēt mācības par kiberdiplomātijas instrumentu kopumu un vērtēt to. ES arī būtu tālāk **jāintegrē kiberdiplomātijas instrumentu kopums ES krīzes mehānismos**, jācenšas panākt sinerģija ar centieniem pretoties hibrīddraudiem, dezinformācijai un ārvalstu intervencei saskaņā ar kopīgo regulējumu hibrīddraudu apkarošanai[88] un Eiropas Demokrātijas rīcības plānu. Šajā sakarā ES būtu jāpārdomā kiberdiplomātijas instrumentu kopuma mijiedarbība ar LES 42. panta 7. punkta un LESD 222. panta iespējamo izmantošanu[89].

[85] Piemēram, ES vienoto izlūkdatu analīzes procedūru (*SIAC*) un, ja nepieciešams, attiecīgajiem saskaņā ar *PESCO* satvaru izveidotajiem projektiem, kā arī 2018. gada agrīnās brīdināšanas sistēmu (ABS), kas ir izveidota, lai atbalstītu ES kopējo pieeju cīņā pret dezinformāciju.
[86] Jo īpaši cenšoties panākt sinerģiju ar Eiropas Demokrātijas rīcības plāna iniciatīvām.
[87] 13007/17
[88] https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:52016JC0018&from=LV.
[89] Attiecīgi — savstarpējās aizsardzības klauzula un solidaritātes klauzula.

2.4. Kiberaizsardzības spēju stiprināšana

ES un dalībvalstīm ir jāuzlabo spējas novērst kiberdraudus un uz tiem reaģēt atbilstīgi no 2016. gada ES globālās stratēģijas izrietošajam ES mērķu vērienīgumam[90]. Šajā nolūkā Augstais pārstāvis sadarbībā ar Komisiju iepazīstinās ar **kiberaizsardzības politikas satvara (KPS) pārskatīšanu**, lai vēl vairāk uzlabotu ES[91] dalībnieku, kā arī dalībvalstu savstarpējo koordināciju un sadarbību, tostarp attiecībā uz kopējās drošības un aizsardzības politikas (KĀDP) misijām un operācijām. KPS informācija ir jāizmanto gaidāmajā stratēģiskajā kompasā[92], nodrošinot kiberdrošības un kiberaizsardzības tālāku integrāciju plašākā drošības un aizsardzības darba programmā.

2018. gadā ES identificēja kibertelpu kā operāciju jomu[93]. ES Militārās komitejas gaidāmajā "**Militārajā redzējumā un stratēģijā par kibertelpu kā operāciju jomu**" būtu sīkāk jādefinē, ka kibertelpa kā operāciju joma ļauj veikt ES KDAP militārās misijas un operācijas. **Militārais *CERT* tīkls**[94], kuru veido Eiropas Aizsardzības aģentūra (EAA), vēl vairāk palīdzēs paplašināt dalībvalstu savstarpējo sadarbību. Turklāt, lai nodrošinātu kosmosa programmas pārziņā esošās kritiski svarīgās kosmosa infrastruktūras kiberdrošību, tiks stiprināta Eiropas Savienības Kosmosa programmas aģentūra un jo īpaši *Galileo* drošības uzraudzības centrs, kā arī tā pilnvaras attiecinātas uz citiem kritiski svarīgiem kosmosa programmas aktīviem.

ES un dalībvalstīm jānodrošina turpmāks stimuls **vismodernāko kiberaizsardzības spēju attīstīšanai**, izmantojot dažādu ES rīcībpolitiku un instrumentus, jo īpaši KPS, un attiecīgos gadījumos jābalstās uz EAA darbu. Tam nepieciešams liels uzsvars uz svarīgu tehnoloģiju, piemēram, MI, šifrēšanas un kvantiskās datošanas, izstrādi un izmantošanu. Atbilstīgi 2018. gada ES spēju veidošanas prioritātēm[95] un balstoties uz pirmā pilnā koordinētā ikgadējā pārskata par aizsardzību (*CARD*) ziņojuma secinājumiem[96], ES būtu vēl vairāk jāveicina sadarbība starp dalībvalstīm **kiberaizsardzības pētniecības, inovācijas un spēju veidošanas** jautājumos, mudinot dalībvalstis pilnībā izmantot **pastāvīgās strukturētās sadarbības (*PESCO*)**[97] un **EAF**[98] potenciālu.

Gaidāmajā **Komisijas rīcības plānā par civilās, aizsardzības un kosmosa nozares sinerģiju**, kas tiks prezentēts 2021. gada pirmajā ceturksnī, būs ietvertas darbības, ar kurām

---

[90] Padomes secinājumi (14149/16) par ES globālās stratēģijas īstenošanu drošības un aizsardzības jomā.
[91] Jo īpaši EĀDD, ieskaitot ES Militāro štābu (ESMŠ), Eiropas Drošības un aizsardzības koledža (EDAK), Komisija un ES aģentūras, jo īpaši Eiropas Aizsardzības aģentūra (EAA).
[92] Padomes 2020. gada 17. jūnija secinājumi par drošību un aizsardzību (8910/20)
[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/lv/pdf.
[94] ES militārā *CERT* tīkla izveide ir atbilde uz 2018. gada kiberaizsardzības politikas satvarā identificētu mērķi, un tās nolūks ir sekmēt ES dalībvalstu militāro *CERT* aktīvu mijiedarbību un savstarpēju informācijas apmaiņu.
[95] 2018. gada jūnijā dalībvalstis EAA valdē vienojās vadīt sadarbību aizsardzības jomā ES līmenī.
[96] 2020. gada novembrī EAA valdē apstiprinājuši aizsardzības ministri.
https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card).
[97] Patlaban darbojas vairāki ar kiberjomu saistīti *PESCO* projekti, jo īpaši ar kiberdraudiem un kiberincidentiem saistītas reaģēšanas informācijas apmaiņas platforma, Kiberdrošības ātrās reaģēšanas vienības un savstarpēja palīdzība kiberdrošības jomā, ES Kiberlietu akadēmija un inovācijas centrs un Kibertelpas un informācijas telpas koordinācijas centrs (***CIDCC***).
[98] Komisija EAF ietvaros jau ir identificējusi iespējas veikt uz sadarbību vērstas kiberaizsardzības pētniecības un izstrādes darbības, kuru mērķis ir stiprināt aizsardzības nozares sadarbību, inovācijas spējas un konkurētspēju.

papildus tiks atbalstīta sinerģija programmu, tehnoloģijas, inovācijas un jaunuzņēmumu līmenī atbilstīgi attiecīgo programmu pārvaldībai[99].

Turklāt ir jāattīsta attiecīgas sinerģijas un saskarnes starp kiberaizsardzības iniciatīvām, kas uzsāktas citos satvaros, ieskaitot ar kiberjomu saistītos dalībvalstu *PESCO* kopdarbības projektos[100], kā arī ar ES kiberdrošības struktūrām, lai atbalstītu informācijas koplietošanu un savstarpēju atbalstu.

Stratēģiskās iniciatīvas

Eiropas Savienībai būtu:

- jāpabeidz Eiropas kiberdrošības krīzes pārvarēšanas satvars un jānosaka kopējās kibervienības izveides process, starpposma mērķrādītāji un grafiks;
- jāturpina īstenot kibernoziedzības darba programma Drošības savienības stratēģijas ietvaros;
- jāmudina un jāatvieglo tādas dalībvalstu kiberizlūkošanas darba grupas izveide, kas pastāvētu pie *EU INTCEN*;
- jāvirza ES kiberatturēšanas pozīcija, lai novērstu un kavētu ļaunprātīgas kiberdarbības, atturētu no tām un reaģētu uz tām;
- jāpārskata kiberaizsardzības politikas satvars;
- jāsekmē ES "Militārā redzējuma un stratēģijas par kibertelpu kā operāciju jomu" izstrāde KDAP militārajām misijām un operācijām;
- jāatbalsta civilās, aizsardzības un kosmosa nozares sinerģija un
- jāstiprina kritiski svarīgas kosmosa infrastruktūras kiberdrošība kosmosa programmas ietvaros.

3. GLOBĀLAS UN ATVĒRTAS KIBERTELPAS ATTĪSTĪŠANA

ES būtu jāturpina sadarboties ar starptautiskajiem partneriem, lai sekmētu tiesiskumā, cilvēktiesībās, pamatbrīvībās un demokrātiskajās vērtībās balstītu kibertelpas politisko modeli un redzējumu, kas pasaulē panāktu sociālo, ekonomisko un politisko attīstību un sekmētu drošības savienību. Lai kibertelpa saglabātos globāla, atvērta, stabila un droša, ir svarīgi sadarboties starptautiski. Šim nolūkam ES būtu jāturpina darbs ar trešām valstīm, starptautiskajām organizācijām, kā arī daudzu ieinteresēto personu kopienu, lai izstrādātu un īstenotu saskanīgu un holistisku starptautisko kiberpolitiku, paturot prātā, ka jauno tehnoloģiju ekonomiskie aspekti, iekšējā drošība un ārpolitikas, drošības un aizsardzības politika arvien biežāk ir savstarpēji savienoti. ES kā spēcīgs ekonomikas un tirdzniecības bloks, kas ir dibināts uz svarīgu demokrātisku vērtību, tiesiskuma ievērošanas un pamattiesību pamata, atrodas arī unikālā pozīcijā, lai ieņemtu vadošo lomu starptautisku normu un standartu noteikšanā un popularizēšanā.

[99] Piemēram, "Apvārsnis Eiropa", "Digitālā Eiropa" un EAF.
[100] https://pesco.europa.eu/.

3.1. ES līderība kibertelpas standartu, normu un satvara jomā

Starptautisko standartu noteikšanas uzlabošana

Lai popularizētu un aizstāvētu savu redzējumu par kibertelpu starptautiski, ES ir **jāpastiprina iesaistīšanās un līderība starptautiskajos standartu noteikšanas procesos, kā arī jāuzlabo pārstāvība starptautiskajās un Eiropas standartu noteikšanas struktūrās un citās standartu izstrādes organizācijās**[101]. Tā kā digitālās tehnoloģijas strauji attīstās, starptautisko standartu nozīme tradicionālo regulatīvo centienu papildināšanā tādās jomās kā MI, mākoņpakalpojumi, kvantiskā datošana un kvantu sakari ir arvien lielāka. Trešās valstis arvien biežāk starptautisko standartu veidošanu izmanto, lai sekmētu savus politiskos un ideoloģiskos mērķus, kas bieži vien neatbilst ES vērtībām. Turklāt pieaug risks, ka radīsies konkurējošas starptautiskās standartizācijas sistēmas, izraisot sadrumstalotību.

Ir svarīgi veidot starptautiskos standartus jauno tehnoloģiju un interneta arhitektūras kodola jomās atbilstīgi ES vērtībām, lai nodrošinātu, ka internets arī turpmāk saglabājas globāls un atvērts, tehnoloģijas ir orientētas uz cilvēkiem un vērstas uz privātumu, kā arī tās tiek izmantotas likumīgi, droši un ētiski. ES kā daļu no gaidāmās standartu noteikšanas stratēģijas būtu jānosaka **starptautiskās standartu noteikšanas mērķi** un jāīsteno proaktīva un koordinēta saziņa to popularizēšanai starptautiskajā līmenī. Būtu jācenšas panākt ciešāku sadarbību un pienākumu sadali ar līdzīgi domājošiem partneriem un Eiropas ieinteresētajām personām.

Sekmēt valstu atbildīgu uzvedību kibertelpā

ES turpina sadarboties ar starptautiskajiem partneriem, lai sekmētu un veicinātu globālu, atvērtu, stabilu un drošu kibertelpu, kurā **tiek ievērotas starptautiskās tiesības, jo īpaši Apvienoto Nāciju Organizācijas (ANO) Statūti**[102]**,** kā arī **brīvprātīgas, nesaistošas normas, noteikumi un principi par valstu atbildīgu uzvedību**[103]. Pasliktinoties efektīvām daudzpusējām diskusijām par starptautisko drošību kibertelpā, pastāv skaidra vajadzība pēc tā, lai ES un dalībvalstis uzņemtos proaktīvāku lomu apspriedēs ANO un citos attiecīgajos starptautiskajos forumos. ES atrodas vislabākajā situācijā, lai **sekmētu, koordinētu un konsolidētu dalībvalstu nostājas starptautiskajos forumos**, un tai būtu **jāizstrādā ES nostāja par starptautisko tiesību piemērošanu kibertelpā**. Augstais pārstāvis kopā arī dalībvalstīm arī plāno ANO virzīt iekļaujošo, uz vienprātību balstīto priekšlikumu par politisku apņemšanos attiecībā uz **rīcības programmu, kā sekmēt valstu atbildīgu uzvedību kibertelpā (RP)**[104]. Balstoties uz ANO Ģenerālās asamblejas apstiprināto esošo tiesību aktu kopumu[105], RP piedāvā platformu sadarbībai un labākās prakses apmaiņai ANO,

[101] Piemēram, Starptautiskajā Standartizācijas organizācijā (ISO), Starptautiskajā Elektrotehnikas komisijā (*IEC*), Starptautiskajā Telesakaru savienībā (*ITU*), Eiropas Standartizācijas komitejā (*CEN*), Eiropas Elektrotehnikas standartizācijas komitejā (*CENELEC*), Eiropas telesakaru standartu institūtā (ETSI), Interneta tehniskajā uzdevumgrupā (*IETF*), Trešās paaudzes partnerības projektā (*3GPP*) un Elektroinženieru un elektronikas inženieru institūtā (*IEEE*).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/.

[103] Tas ir atspoguļots attiecīgajos ziņojumos, ko iesniegušas valdības ekspertu grupas informācijas un telesakaru nozaru attīstības jautājumos starptautiskās drošības jomā (*UNGGE*) un apstiprinājusi ANO ĢA, jo īpaši 2015., 2013. un 2010. gada ziņojumos.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

[105] Tas ir atspoguļots attiecīgajos ziņojumos, ko iesniegušas valdības ekspertu grupas informācijas un telesakaru nozaru attīstības jautājumos starptautiskās drošības jomā (*UNGGE*) un apstiprinājusi ANO ĢA, jo īpaši 2015., 2013. un 2010. gada ziņojumos.

kā arī ierosina izveidot mehānismu, kā ieviest praksē atbildīgas valstu uzvedības normas un sekmēt spēju veidošanu. Turklāt Augstais pārstāvis plāno stiprināt un mudināt valstu savstarpējo **uzticības veicināšanas pasākumu** īstenošanu, tostarp apmaiņu ar labāko praksi reģionālajā un daudzpusējā līmenī, kā arī sniedzot ieguldījumu starpreģionu sadarbībā.

Lielāka starptautiskā savienojamība nedrīkstētu novest pie cenzūras, masveidīgas novērošanas, datu privātuma pārkāpumiem un represijām pret pilsonisko sabiedrību, akadēmisko vidi un iedzīvotājiem. ES ir jāsaglabā vadošā loma **cilvēktiesību un pamatbrīvību** aizsardzībā un sekmēšanā tiešsaistē. Šajā nolūkā ES būtu jāsekmē tālāka atbilstība starptautiskajām cilvēktiesībām un standartiem[106], kā arī jāievieš praksē tās Rīcības plāns cilvēktiesību un demokrātijas jomā 2020.–2024. gadam[107] un jāsekmē cilvēktiesību nostādnes par vārda brīvību tiešsaistē un bezsaistē[108], **sniedzot jaunu impulsu ES instrumentu praktiskajai piemērošanai**. ES ir jāpieliek pastāvīgas pūles, lai **aizsargātu cilvēktiesību aizstāvjus, pilsonisko sabiedrību un akadēmisko vidi, kas strādā pie tādiem jautājumiem kā kiberdrošība, datu privātums, novērošana un cenzūra tiešsaistē**. Šim nolūkam ES ir jāsniedz papildu praktiskie norādījumi, jāsekmē labākā pieredze un jāpastiprina centieni novērst jauno tehnoloģiju ļaunprātīgu izmantošanu, jo īpaši, nepieciešamības gadījumā izmantojot diplomātiskos pasākumus un veicot šo tehnoloģiju eksporta kontroli. ES ir jāturpina arī cīnīties par vismazāk aizsargāto sabiedrības locekļu aizsardzību tiešsaistē, ierosinot tiesību aktus, lai labāk aizsargātu bērnus no seksuālas vardarbības un izmantošanas, kā arī Bērnu tiesību stratēģiju.

Budapeštas Konvencija par kibernoziegumiem

ES turpina atbalstīt trešās valstis, kas vēlas pievienoties **Eiropas Padomes Budapeštas Konvencijai par kibernoziegumiem**, un strādā pie tā, lai tiktu pabeigts **Budapeštas Konvencijas otrais papildprotokols**, kurā ir ietverti pasākumi un aizsardzības pasākumi, lai uzlabotu starptautisko sadarbību starp tiesībaizsardzības iestādēm un tiesu iestādēm, kā arī starp iestādēm un pakalpojumu sniedzējiem citās valstīs, kurā Komisija piedalās sarunās ES vārdā[109]. Pašreizējā iniciatīva attiecībā uz jaunu ANO līmeņa tiesību aktu par kibernoziedzību riskē saasināt atšķirības un palēnināt tik ļoti nepieciešamās valstu reformas un ar tām saistītos spēju veidošanas centienus, kas varētu kavēt efektīvu starptautisko sadarbību cīņā pret kibernoziegumiem: ES neredz nepieciešamību pēc jauna ANO līmeņa tiesību akta par kibernoziedzību. ES turpina iesaistīties **daudzpusējā informācijas apmaiņā par kibernoziegumiem**, lai, izmantojot iekļaušanu un pārredzamību, kā arī ņemot vērā pieejamās zināšanas, nodrošinātu cilvēktiesību un pamatbrīvību ievērošanu nolūkā panākt pievienoto vērtību visiem.

3.2. Sadarbība ar partneriem un daudzu ieinteresēto personu kopiena

ES būtu **jāstiprina un jāpaplašina kiberdialogi ar trešām valstīm**, lai veicinātu tās vērtības un redzējumu attiecībā uz kibertelpu, apmainītos ar labāko praksi un censtos efektīvāk sadarboties. ES būtu arī jāizveido **strukturēta informācijas apmaiņa ar reģionālajām organizācijām**, piemēram, Āfrikas Savienību, *ASEAN* Reģionālo forumu, Amerikas valstu organizāciju un Eiropas Drošības un sadarbības organizāciju. Tajā pašā laikā ES būtu

[106] Jo īpaši ANO Statūtiem un Vispārējai cilvēktiesību deklarācijai.
[107] https://www.consilium.europa.eu/lv/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/.
[108] https://www.consilium.europa.eu/media/28348/142549.pdf.
[109] Padomes 2019. gada jūnija lēmums (ref 9116/19)

jācenšas atrast kopīgu pamatu ar citiem partneriem, kur tas ir iespējams un ir šādas iespējas, pamatojoties uz kopīgu interešu jautājumiem. Sadarbojoties ar ES delegācijām, kā arī attiecīgā gadījumā ar dalībvalstu vēstniecībām visā pasaulē, ES jāveido neformāls **ES kiberdiplomātijas tīkls**, lai popularizētu ES redzējumu par kibertelpu, apmainītos ar informāciju un regulāri veiktu koordināciju attiecībā uz kibertelpas attīstību[110].

Pamatojoties uz 2016. gada 8. jūlija[111] un 2018. gada 10. jūlija[112] kopīgajām deklarācijām, ES ir jāturpina virzīt **ES un NATO sadarbība**, jo īpaši attiecībā uz kiberaizsardzības sadarbspējas prasībām. Šajā sakarā ES būtu jācenšas tuvināt attiecīgo KDAP struktūru saikne ar NATO vienoto misiju tīklu, ļaujot panākt tīkla sadarbspēju ar NATO un partnervalstīm, kur tā ir nepieciešama. Turklāt būtu sīkāk jāizvērtē ES un NATO sadarbības iespējas izglītības, apmācības un mācību jomā, tostarp cenšoties panākt sinerģiju starp Eiropas Drošības un aizsardzības koledžu un NATO Kopējo kiberaizsardzības izcilības centru.

ES atbilstīgi savām vērtībām ļoti atbalsta un sekmē **daudzu ieinteresēto personu interneta pārvaldības modeli**. Nevienai struktūrai, valdībai vai starptautiskai organizācijai nebūtu jācenšas kontrolēt internetu. ES ir jāturpina iesaiste forumos[113], lai uzlabotu sadarbību un nodrošinātu, ka tiek aizsargātas pamattiesības un brīvības, jo īpaši tiesības uz cieņu, privātumu un vārda un informācijas brīvību. Lai virzītu uz priekšu daudzu ieinteresēto personu sadarbību kiberdrošības jautājumos, Komisija un Augstais pārstāvis atbilstīgi savai kompetencei plāno stiprināt **regulāru un strukturētu informācijas apmaiņu ar ieinteresētajām personām**, ieskaitot privāto sektoru, akadēmisko vidi un pilsonisko sabiedrību, uzsverot, ka kibertelpas savstarpējā savienojamība prasa, lai visas ieinteresētās personas apmainītos ar informāciju un uzņemtos īpašu atbildību nolūkā uzturēt globālu, atvērtu, stabilu un drošu kibertelpu. Šie centieni nodrošinās vērtīgu informāciju iespējamām pamatdarbībām ES līmenī.

3.3. Globālo spēju stiprināšana globālās noturības paaugstināšanai

Lai nodrošinātu, ka visas valstis var izmantot sociālos, ekonomiskos un politiskos ieguvumus no interneta un tehnoloģiju izmantošanas, ES turpina atbalstīt partnervalstis, lai uzlabotu to kibernoturību un spējas izmeklēt kibernoziegumus un celt apsūdzības par tiem, kā arī risināt kiberdraudus. Lai nodrošinātu kopējo saskaņotību, ES būtu jāizstrādā **ES ārējo kiberspēju veidošanas darba programma**, lai virzītu šos centienus atbilstīgi Ārējo kiberspēju veidošanas nostādnēm[114] un Ilgtspējīgas attīstības programmai 2030. gadam[115]. Darba programmā būtu jāizmanto dalībvalstu, attiecīgo ES iestāžu, struktūru un aģentūru, ieskaitot Eiropas Kiberspēju veidošanas tīklu[116], zinātība un iniciatīvas atbilstīgi to attiecīgajām pilnvarām. Ir jāizveido **ES kiberspēju veidošanas padome**, lai aptvertu attiecīgas ES iestāžu ieinteresētās personas un pārraudzītu progresu, kā arī identificētu tālākas sinerģijas un iespējamās nepilnības. Tā var arī atbalstīt ciešāku sadarbību ar dalībvalstīm un ar privātā un

[110] Attiecīgos gadījumos tā varētu arī izmantot neformālā ES digitālās diplomātijas tīkla, kurā ietilpst dalībvalstu ārlietu ministrijas, veiktās darbības.
[111] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[112] https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Piemēram, Piešķirto nosaukumu un numuru interneta korporācijā (*ICANN*) un Interneta pārvaldības forumā (*IGF*).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/lv/pdf.
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm.
[116] https://www.eucybernet.eu/.

publiskā sektora partneriem un citām attiecīgām starptautiskām struktūrām, lai nodrošinātu centienu koordinēšanu un izvairītos no to dublēšanās.

ES kiberspēju veidošanā arī turpmāk jāpievērš uzmanība Rietumbalkāniem un ES kaimiņreģioniem, kā arī partnervalstīm, kas piedzīvo strauju digitālo attīstību. Ar ES centieniem būtu jāatbalsta partnervalstu tiesību aktu un politikas izstrāde atbilstīgi attiecīgajai ES kiberdiplomātijas politikai un standartiem. Šajā sakarā ES spēju veidošanas centieniem digitalizācijas jomā būtu jāietver kiberdrošība kā standarta elements. Šim nolūkam ES būtu jāizstrādā par ES digitālo un kibernozares ārējo spēju veidošanu atbildīgajiem ES darbiniekiem paredzēta mācību programma. Atbilstīgi centieniem, ko paredz Eiropas Demokrātijas rīcības plāns, ES būtu arī jāpalīdz šīm valstīm apkarot pieaugošās grūtības, ko rada ļaunprātīgas kiberdarbības, kuras kaitē šo sabiedrību attīstībai un **demokrātisko sistēmu integritātei un drošībai**. Šajā ziņā sevišķi noderīga varētu būt ES dalībvalstu, kā arī attiecīgo ES aģentūru un trešo valstu mācīšanās no līdzbiedriem.

Visbeidzot, 2018. gada Civilās KDAP pakta[117] kontekstā civilās KDAP misijas var sniegt ieguldījumu arī ES plašākā atbildē cīņai ar kiberdrošības problēmām, jo īpaši stiprinot partnervalstu tiesiskumu, kā arī to tiesībaizsardzības un civilās pārvaldes spējas.

Stratēģiskās iniciatīvas

Eiropas Savienībai būtu:

- jādefinē mērķu kopums starptautisko standartu noteikšanas procesam un tie jāsekmē starptautiskajā līmenī;
- jāstiprina starptautiskā drošība un stabilitāte kibertelpā, jo īpaši izmantojot ES un tās dalībvalstu priekšlikumu ANO rīcības programmai, kā sekmēt valstu atbildīgu uzvedību kibertelpā (RP);
- jāsniedz praktiski norādījumi, kā kibertelpā piemērot cilvēktiesības un pamatbrīvības;
- labāk jāaizsargā bērni no seksuālas vardarbības un izmantošanas, kā arī jāparedz Bērnu tiesību stratēģija;
- jāstiprina un jāsekmē Budapeštas Konvencija par kibernoziegumiem, tostarp darbā pie Budapeštas Konvencijas otrā papildprotokola;
- jāpaplašina ES dialogs par kiberjautājumiem ar trešām valstīm, reģionālām un starptautiskām organizācijām, tostarp ar neformāla ES kiberdiplomātijas tīkla starpniecību;
- jāstiprina informācijas apmaiņa ar daudzu ieinteresēto personu kopienu, jo īpaši regulāra un strukturēta informācijas apmaiņa ar privāto sektoru, akadēmisko vidi un pilsonisko sabiedrību, un
- jāierosina ES ārējo kiberspēju veidošanas darba programma un ES kiberspēju veidošanas padome.

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/lv/pdf.

III. KIBERDROŠĪBA ES IESTĀDĒS, STRUKTŪRĀS UN AĢENTŪRĀS

Ņemot vērā to lielo politisko nozīmību, kritiski svarīgos uzdevumus — koordinēt ļoti sensitīvus jautājumus — un lomu liela apjoma valsts līdzekļu pārvaldībā, **ES iestādes, struktūras un aģentūras regulāri kļūst par mērķi kibernoziegumiem**, jo īpaši kiberspiegošanai. Tomēr šo struktūru kibernoturības līmenis un spēja atklāt un reaģēt uz ļaunprātīgām kiberdarbībām būtiski atšķiras gatavības ziņā. Tādēļ, izmantojot konsekventus un viendabīgus noteikumus, ir nepieciešams uzlabot kopējo kiberdrošības līmeni.

Informācijas drošības jomā ir panākts progress ceļā uz konsekventākiem **noteikumiem par ES klasificētās informācijas un sensitīvas neklasificētas informācijas aizsardzību.** Tomēr klasificētas informācijas sistēmu sadarbspēja joprojām ir ierobežota, kas liedz netraucēti nodot informāciju no vienas struktūras citai. Ir jāpanāk turpmāks progress, lai darbībām ar ES klasificētu informāciju un sensitīvu neklasificētu informāciju varētu izmantot starpiestāžu pieeju, kas varētu kalpot arī kā dalībvalstu sadarbspējas modelis. Būtu jānosaka arī pamatscenārijs, lai vienkāršotu procedūras ar dalībvalstīm. ES būtu arī tālāk jāattīsta spēja droši sazināties ar attiecīgajām partnervalstīm, iespēju robežās balstoties uz pastāvošo kārtību un procedūrām.

Kā izziņots Drošības savienības stratēģijā, Komisija tādēļ 2021. gadā, balstoties uz pastāvīgajām ES starpiestāžu apspriedēm par kiberdrošību, iesniegs priekšlikumus **kopējiem saistošiem noteikumiem par informācijas drošību un kopējiem saistošiem kiberdrošības noteikumiem visām ES iestādēm, struktūrām un aģentūrām**[118].

Pašreizējās un turpmākās tāldarba tendences arī prasīs veikt papildu ieguldījumus droša aprīkojuma, infrastruktūras un instrumentu nodrošināšanā, lai būtu iespējams attālināti strādāt ar sensitīvām un klasificētām lietām.

Turklāt arvien naidīgākā kiberdraudu aina un pieaugošā izsmalcinātāku kiberuzbrukumu izplatība, kas ietekmē ES iestādes, struktūras un aģentūras, nosaka nepieciešamību palielināt ieguldījumus augsta kiberdrošības līmeņa sasniegšanā. Visām ES iestādēm, struktūrām un aģentūrām tiek veidota kiberinformētības programma, lai uzlabotu strādājošo informētību un kiberhigiēnu, kā arī atbalstītu vienotu kiberdrošības kultūru.

Ir nepieciešams **stiprināt *CERT-EU* ar uzlabotu finansēšanas mehānismu**, lai uzlabotu tās spēju palīdzēt ES iestādēm, struktūrām un aģentūrām piemērot jaunos kiberdrošības noteikumus un uzlabot to kibernoturību. Ir jāstiprina arī *CERT-EU* pilnvaras, lai tai nodrošinātu nemainīgus līdzekļus šo mērķu sasniegšanai.

Stratēģiskās iniciatīvas

1. Regula par informācijas drošību ES iestādēs, struktūrās un aģentūrās
2. Regula par vienotiem ES iestāžu, struktūru un aģentūru kiberdrošības noteikumiem
3. Jauns juridiskais pamats *CERT-EU*, lai stiprinātu tās pilnvaras un finansējumu.

[118] Regulāras ES starpiestāžu apspriedes par kiberdrošību ir daļa no plašākas informācijas apmaiņas par digitālās pārveides radītajām iespējām un grūtībām ES iestādēm.

IV. SECINĀJUMI

Šīs stratēģijas saskaņota īstenošana sekmēs kiberdrošu ES digitālo desmitgadi un drošības savienības sasniegšanu, kā arī palīdzēs stiprināt ES pozīciju pasaulē.

ES būtu jāvirza būtisku sabiedrisku pakalpojumu un kritiskās infrastruktūras kiberdrošības pasaules līmeņa risinājumi, standarti un normas, kā arī jaunu tehnoloģiju izstrāde un izmantošana. Ikviena organizācija un persona, kas lieto internetu, ir daļa no risinājuma, kas ļaus nodrošināt kiberdrošu digitālo pārveidi.

Komisija un Augstais pārstāvis atbilstīgi savai attiecīgajai kompetencei uzraudzīs šīs stratēģijas ietvaros panākto progresu un izstrādās novērtēšanas kritērijus. Ieguldījumam šajā uzraudzībā būtu jāiekļauj *ENISA* ziņojumi un Komisijas regulārie ziņojumi par drošības savienību. Tās rezultāti palīdzēs sasniegt turpmākās digitālās desmitgades mērķus[119]. Komisija un Augstais pārstāvis atbilstīgi savai kompetencei turpinās sazināties ar dalībvalstīm, lai identificētu praktiskus pasākumus, ar kuriem pēc nepieciešamības savienot četras ES kiberdrošības kopienas — kritiskās infrastruktūras un iekšējā tirgus noturības, tieslietu un tiesībaizsardzības, kiberdiplomātijas un kiberaizsardzības. Turklāt Komisija un Augstais pārstāvis turpinās sadarboties ar kopienu, ko veido daudzas ieinteresētās personas, uzsverot, ka ikvienam interneta lietotājam ir nepieciešams sniegt ieguldījumu globālas, atvērtas, stabilas un drošas kibertelpas uzturēšanā, kurā ikviens var droši dzīvot savu digitālo dzīvi.

[119] Kā paziņots Komisijas 2021. gada darba programmā.

Papildinājums. Turpmākie 5G tīklu kiberdrošības pasākumi

Balstoties uz Komisijas ieteikuma par 5G tīklu kiberdrošību[120] pārskatīšanas rezultātiem, nākamajos ES līmenī koordinētā darba soļos būtu jāorientējas uz trim svarīgākajiem mērķiem un galvenajām īstermiņa un vidēja termiņa darbībām, kas ir izklāstītas tālāk dotajā tabulā un kas ir jāīsteno dalībvalstu iestādēm, Komisijai un *ENISA*.

Svarīgākā prioritāte nākamajā posmā ir **pabeigt instrumentu kopuma īstenošanu valstu līmenī un risināt 2020. gada jūlija progresa ziņojumā identificētās problēmas**. Šajā sakarā daži no rīkkopas stratēģiskajiem pasākumiem iegūtu, ja tiktu **uzlabots koordinācijas darbs vai informācijas apmaiņa** TID darbplūsmā, uz ko jau ir norādīts progresa ziņojumā un kas, iespējams, varētu novest pie **labākās prakses vai norādījumu** izstrādes. Kas attiecas uz tehniskajiem pasākumiem, papildu atbalstu varētu sniegt *ENISA*, balstoties uz jau paveikto darbu un padziļinātāk izmeklējot konkrētus jautājumus, kā arī **izstrādājot visaptverošu pārskatu par visām attiecīgajām 5G kiberdrošības prasību nostādnēm mobilo tīklu operatoriem**.

Otrkārt, dalībvalstis uzsvēra, cik svarīgi ir sekot notikumu attīstībai, **pastāvīgi uzraugot tehnoloģiju, 5G arhitektūras, draudu un 5G lietojumu un izmantojumu, kā arī ārējo faktoru attīstību**, lai spētu **identificēt un risināt jaunus vai aktualitāti iegūstošus riskus**. Turklāt ir sīkāk jāpēta vairāki sākotnējās riska analīzes aspekti, jo īpaši, lai nodrošinātu, ka tā aptver visu 5G ekosistēmu, ieskaitot visas attiecīgās tīkla infrastruktūras un 5G piegādes ķēdes daļas. Lai gan rīkkopa ir izstrādāta kā elastīgs un pielāgojams rīks, vidējā termiņā, ja nepieciešams, varētu veikt pasākumus tās papildināšanai vai grozīšanai, lai nodrošinātu, ka tā arī turpmāk ir visaptveroša un aktuāla.

Treškārt, ir jāturpina veikt **ES līmeņa darbības**, lai atbalstītu un papildinātu rīkkopas mērķus un tos pilnībā integrētu attiecīgajā Savienības un Komisijas politikā, jo īpaši kā turpmāko rīcību pēc darbībām, ko Komisija izziņoja savā 2020. gada 29. janvāra paziņojumā par rīkkopu[121] dažādās jomās (piem., attiecībā uz ES finansējumu drošiem 5G tīkliem, ieguldījumiem 5G un pēc 5G gaidāmajās tehnoloģijās, tirdzniecības aizsardzības instrumentiem un konkurenci, lai izvairītos no 5G piegādes tirgus izkropļojumiem utt.).

Attiecīgos gadījumos vadošajiem dalībniekiem 2021. gada sākumā ir jāvienojas par svarīgāko turpmāk izklāstīto darbību detalizētu kārtību un starpposma mērķrādītājiem.

1. pamatmērķis: nodrošināt saskanīgas valstu pieejas efektīvai riska mazināšanai visā ES		
Jomas	**Galvenās īstermiņa un vidēja termiņa darbības**	**Vadošie dalībnieki**
Rīkkopas īstenošana dalībvalstīs	Pabeigt rīkkopas secinājumos ieteikto pasākumu īstenošanu līdz 2021. gada otrajam ceturksnim, periodiski veicot novērtēšanu TID darbplūsmā.	Dalībvalstu iestādes
Ar piegādātājiem saistītu stratēģisko	Pastiprināt informācijas apmaiņu un apsvērt iespējamo labāko praksi, jo īpaši attiecībā uz:	Dalībvalstu iestādes,

[120] Komisijas ziņojums par ietekmi, kādu radījis Komisijas 2019. gada 26. marta Ieteikums 2019/534 par 5G tīklu kiberdrošību.

[121] Komisijas paziņojums COM (2020) 50 "Droša 5G ieviešana ES — ES rīkkopas īstenošana", 2020. gada 29. janvāris.

pasākumu informācijas un labākās prakses apmaiņa	- ierobežojumiem augsta riska piegādātājiem (SM03) un ar pārvaldīto pakalpojumu sniegšanu saistītajiem pasākumiem (SM04); - piegādes ķēžu drošību un noturību, jo sevišķi kā turpmāko rīcību pēc *BEREC* veiktās aptaujas par SM05–SM06.	Komisija
Spēju veidošana un norādījumi tehnisko pasākumu jomā	Veikt tehnisku padziļinātu izpēti un izstrādāt vienotus norādījumus un rīkus, tostarp: - visaptverošu un dinamisku 5G drošības kontroles un labākās prakses matricu; norādījumus atsevišķu rīkkopas tehnisko pasākumu īstenošanas atbalstam.	*ENISA*, dalībvalstu iestādes
2. pamatmērķis: atbalsts pastāvīgai zināšanu apmaiņai un spēju veidošanai		
Jomas	**Galvenās īstermiņa un vidēja termiņa darbības**	**Vadošie dalībnieki**
Pastāvīga zināšanu veidošana	Organizēt zināšanu veidošanas aktivitātes attiecībā uz tehnoloģijām un ar tām saistītajām problēmām (atvērto arhitektūru, 5G īpašībām, kā virtualizāciju, konteinerizāciju, sadalīšanu utt.), draudu ainas attīstību, incidentiem no reālās dzīves utt.	*ENISA*, dalībvalstu iestādes, citas ieinteresētās personas
Riska novērtējumi	Aktualizēt un apmainīties ar informāciju par jaunākajiem valstu riska novērtējumiem.	Dalībvalstu iestādes, Komisija, *ENISA*
Kopīgi ES finansēti projekti rīkkopas īstenošanas atbalstam	No ES finansējuma sniegt finansiālu atbalstu projektiem, kas atbalsta rīkkopas īstenošanu, jo īpaši saskaņā ar programmu "Digitālā Eiropa" (piem., valstu iestāžu spēju veidošanas projektus, izmēģināšanas stacijas vai citas paaugstinātas spējas utt.).	Dalībvalstu iestādes, Komisija
Ieinteresēto personu sadarbība	Sekmēt 5G kiberdrošībā iesaistīto valstu iestāžu (piem., TID sadarbības grupas, kiberdrošības iestāžu, telesakaru regulatoru) kopdarbību un sadarbību gan savstarpēji, gan ar privātām ieinteresētajām personām.	Dalībvalstu iestādes, Komisija, *ENISA*
3. pamatmērķis: sekmēt piegādes ķēžu noturību un citus ES stratēģiskās drošības mērķus		
Jomas	**Galvenās īstermiņa un vidēja termiņa darbības**	**Vadošie dalībnieki**
Standartizācija	Kā daļu no TID standartizācijas apakšgrupas darba nākamajiem posmiem definēt un īstenot konkrētu rīcības plānu, kā uzlabot ES pārstāvību standartu noteikšanas struktūrās, lai sasniegtu konkrētus mērķus drošības jomā, ieskaitot sadarbspējīgu saskarņu popularizēšanu nolūkā atvieglot piegādātāju dažādošanu.	Dalībvalstu iestādes
Piegādes ķēžu noturība	- Veikt 5G ekosistēmas un piegādes ķēdes padziļinātu analīzi, lai labāk identificētu un uzraudzītu svarīgākos aktīvus un iespējamās kritiski svarīgās atkarības. - Nodrošināt, ka 5G tirgus un piegādes ķēdes darbība atbilst Komisijas 29. janvāra paziņojumā definētajiem ES tirdzniecības un konkurences noteikumiem un mērķiem un ka notikumu attīstībai ieguldījumu jomā, kas varētu ietekmēt 5G pievienotās vērtības veidošanas ķēdi, piemēro ĀTI izvērtēšanu, ņemot vērā rīkkopas mērķus.	Dalībvalstu iestādes, Komisija

	- Uzraudzīt esošās un paredzamās tirgus tendences, izvērtēt riskus un iespējas atvērto radiopiekļuves tīklu jomā, jo īpaši, izmantojot neatkarīgu pētījumu.	
Sertificēšana	Sākt gatavot attiecīgu(-as) sertifikācijas kandidātshēmu(-as) svarīgākajiem 5G komponentiem un piegādātāju procesiem, lai palīdzētu novērst atsevišķus ar tehnisko ievainojamību saistītus riskus, kā definēts rīkkopas riska mazināšanas plānos.	Komisija, *ENISA*, valstu iestādes, citas ieinteresētās personas
ES spējas un droša tīklu ieviešana	- Veikt ieguldījumus pētniecībā un inovācijā, kā arī spējās, jo īpaši pieņemot viedo tīklu un pakalpojumu partnerību. - Ieviest attiecīgus drošības nosacījumus ES finansējuma programmām un finanšu instrumentiem (iekšējiem un ārējiem), kā izziņots Komisijas 29. janvāra paziņojumā.	Dalībvalstis, Komisija, 5G nozares ieinteresētās personas
Ārējie aspekti	Labvēlīgi reaģēt uz to trešo valstu lūgumiem, kuras vēlas saprast un, iespējams, izmantot ES izstrādāto rīkkopas pieeju.	Dalībvalstis, Komisija EĀDD, ES delegācijas