EIROPAS
KOMISIJA

Briselē, 13.12.2022.
COM(2022) 745 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

par piekto progresa ziņojumu par ES Drošības savienības stratēģijas īstenošanu

1. IEVADS

Komisija 2020. gada jūlijā pieņēma visaptverošu Drošības savienības stratēģiju[1]. Kopš tā laika apdraudējumu vide ir ļoti būtiski mainījusies. Covid-19 krīze uzsvēra dažas neaizsargātības jomas, jo īpaši saistībā ar tiešsaistē pārcelto darbību. Kiberdrošības uzbrukumu mērogs turpina pieaugt un izplatās arvien jauni uzbrukumu veidi[2]. Ir jūtama Krievijas agresijas kara pret Ukrainu ietekme uz ES iekšējo drošību, jo ir palielinājies cilvēku tirdzniecības risks, ķīmisku katastrofu un kodolnegadījumu draudi, kā arī šaujamieroču nelikumīga aprite. Tas ir arī veicinājis ārvalstu īstenotu informācijas manipulāciju un iejaukšanos. Nesenais *Nord Stream* cauruļvadu sabotāžas gadījums ir uzsvēris, ka tādas būtiskas nozares kā enerģētika, digitālā infrastruktūra, transports un kosmoss ir atkarīgas no noturīgas kritiskās infrastruktūras. Tas vēlreiz parādīja, ka gan fiziskā, gan digitālā drošība ir cieši saistītas un ir jāaizsargā paralēli.

Šā Drošības savienības progresa ziņojuma mērķis ir sniegt "vidusposma" pārskatu par stratēģijas īstenošanu, uzsverot, kas ir sasniegts un kas vēl ir jāpaveic līdz šīs Komisijas pilnvaru termiņa beigām. Kopš 2020. gada jūlija ES ir guvusi lielus panākumus virzībā uz darbību pabeigšanu galvenajās jomās, uz kurām attiecas visi četri stratēģijas pīlāri[3]. Šis ziņojums liecina, ka ir īstenots vairums stratēģijā paredzēto darbību[4]. Tomēr vēl ir daudz darāmā, lai panāktu Drošības savienības stratēģijas pilnīgu ietekmi uz iedzīvotājiem, konkrētāk, lai Eiropas Parlaments un Padome pieņemtu atlikušos tiesību aktu priekšlikumus un lai dalībvalstis īstenotu tiesību aktus, par kuriem panākta vienošanās. Drošības savienības mērķus vislabāk var sasniegt, cieši sadarbojoties ar saistītām ES iniciatīvām tādās jomās kā enerģētiskā drošība, Eiropas veselības savienība un Eiropas Demokrātijas rīcības plāns. Komisijas turpmākais ieguldījums ietver trīs priekšlikumus, kas pieņemti līdztekus šim ziņojumam, proti, par kultūras priekšmetu nelikumīgu tirdzniecību, par būtiskiem izlūkdatiem, ko sniedz iepriekšēja pasažieru informācija[5], kā arī par priekšlikumu risināt cilvēku tirdzniecības problēmu[6].

2. FIZISKĀS UN DIGITĀLĀS INFRASTRUKTŪRAS AIZSARDZĪBA PRET FIZISKIEM UZBRUKUMIEM, KIBERUZBRUKUMIEM UN HIBRĪDUZBRUKUMIEM

ES kritiskās infrastruktūras aizsardzība pret fiziskiem un digitāliem uzbrukumiem

Vēl pirms nesenajiem uzbrukumiem kritiskajai infrastruktūrai ES veidoja savu noturību, izmantojot divas savstarpēji saistītas iniciatīvas: pārskatīto direktīvu[7], ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā (**Tīklu un informācijas**

---

1 COM(2020) 605.

2 *ENISA Threat landscape 2022*.

3 1) nākotnes prasībām atbilstoša drošības vide, 2) vēršanās pret jauniem apdraudējumiem, 3) Eiropas iedzīvotāju aizsardzība pret terorismu un organizēto noziedzību, 4) spēcīga Eiropas drošības ekosistēma.

4 Pielikumā iekļautajā tabulā sniegts pārskats par leģislatīvajām un neleģislatīvajām darbībām kopš Drošības savienības stratēģijas īstenošanas sākuma.

5 Rīcības plāns kultūras priekšmetu nelikumīgas tirdzniecības apkarošanai (COM(2022) 800 un divi priekšlikumi par iepriekšējas pasažieru informācijas direktīvas pārskatīšanu (COM(2022) 729 un COM(2022) 731).

6 Priekšlikumu pārskatītai direktīvai par cilvēku tirdzniecības apkarošanu (COM(2022) 732) un 4. progresa ziņojumu par cilvēku tirdzniecību ir paredzēts pieņemt 2022. gada 19. decembrī.

7 Priekšlikums pārskatīt Direktīvu (ES) 2016/1148.

drošība — "TID2 direktīva")[8], un jauno direktīvu par kritisko vienību noturību (**Kritisko vienību noturība — "KVN direktīva"**)[9]. Kopā šis regulējums ir vērsts uz pašreizējiem un nākotnes tiešsaistes un bezsaistes riskiem, sākot ar kiberuzbrukumiem un beidzot ar dabas katastrofām. Par šīm direktīvām ir vienojušies likumdevēji, un tās stāsies spēkā tuvāko nedēļu laikā. Ar **TID2 direktīvu** palielinās vidējo un lielo vienību aptvērumu vairākās galvenajās nozarēs[10]. Ar to pastiprina drošības prasības, tai skaitā attiecībā uz reaģēšanu uz incidentiem un krīžu pārvaldību, piegādes ķēdes drošību, rīcību neaizsargātības gadījumā un atklāšanā, kiberdrošības testēšanu un efektīvu šifrēšanas izmantošanu. Ar to arī racionalizē pienākumu ziņot par incidentiem, ievieš stingrākus uzraudzības pasākumus un tiecas saskaņot sankciju režīmus visās dalībvalstīs[11]. **KVN direktīva** attiecas uz kritisko vienību fizisko noturību gan pret cilvēka radītiem, gan dabiskiem apdraudējumiem. Šī direktīva aptver 11 nozares un ir nozīmīgs solis virzībā uz kritisko vienību, kas sniedz pamatpakalpojumus, uzlabotu spēju izvairīties no incidentiem, aizsargāt pret tiem, reaģēt uz tiem, pretoties tiem, mazināt un absorbēt tos, pielāgoties tiem un pārvarēt tos.

Finanšu nozarē kā daļa no digitālo finanšu tiesību aktu kopuma ir pieņemts arī Digitālās darbības noturības akts (*Digital Operational Resilience Act — DORA*)[12]. Pēc ieviešanas *DORA* stiprinās ES finanšu nozares struktūru digitālās darbības noturību, racionalizējot un uzlabojot spēkā esošos noteikumus un vajadzības gadījumā ieviešot jaunas prasības.

Lai vēl vairāk uzlabotu **kritiskās infrastruktūras aizsardzību pret liela mēroga kiberuzbrukumiem**, Komisija, Augstais pārstāvis un TID sadarbības grupa[13] izstrādā **riska scenārijus**, galveno uzmanību pievēršot kiberdrošībai enerģētikas, telesakaru, transporta un kosmosa nozarēs. Turpinās arī darbs pie pasākumiem, kuru mērķis ir uzlabot kosmosa sistēmu un pakalpojumu kolektīvo aizsardzības līmeni un kibernoturību[14]. Pašlaik tiek veikti arī mērķorientēti kiberdrošības riska novērtējumi attiecībā uz sakaru infrastruktūru un tīkliem ES (arī attiecībā uz fiksēto un mobilo infrastruktūru, satelītiem, zemūdens kabeļiem un interneta maršrutēšanu)[15]. Lai uzlabotu katastrofu novēršanu, sagatavotību tām un reaģēšanu uz tām, Komisija ir arī uzsākusi scenāriju veidošanas iniciatīvu, kas aptver **dabas katastrofas, kuras saistītas ar tādiem drošības apdraudējumiem** kā kiberuzbrukumi vai terorisms.

Nord Stream gāzes cauruļvadu sabotāža un citi nesenie incidenti uzsvēra **ES kritiskās infrastruktūras** apdraudējumu un nepieciešamību steidzami rīkoties. Tāpēc tiek paredzēts KVN direktīvas un TID2 direktīvas satvars nolūkā paātrināt rīcību kritiskās infrastruktūras noturības stiprināšanai un uzlabot sagatavotību un reaģēšanu svarīgajās nozarēs. Tas ir

---

8 COM(2020) 823.

9 COM(2020) 829.

10 TID2 un KVN direktīva attiecas uz šādām nozarēm: enerģētika, transports, banku pakalpojumi, finanšu tirgus infrastruktūra, digitālā infrastruktūra, veselības aprūpe, dzeramais ūdens, notekūdeņi, valsts pārvalde, kosmoss un pārtikas ražošana, pārstrāde un izplatīšana.

11 Notiek diskusijas starp valstu ekspertiem TID sadarbības grupā, lai palīdzētu dalībvalstīm transponēt un īstenot TID2 direktīvu.

12 COM (2020) 595. Politiskā vienošanās panākta 2022. gada maijā.

13 Grupā ir dalībvalstu, Komisijas un Eiropas Savienības Kiberdrošības aģentūras (*ENISA*) pārstāvji nolūkā atbalstīt un veicināt stratēģisko sadarbību starp dalībvalstīm tīklu un informācijas sistēmu drošības jomā.

14 Padomes secinājumi par Eiropas Savienības pozīcijas kiberjautājumos izstrādi, 2022. gada 23. maijs.

15 Saskaņā ar Nevēras Aicinājumu pastiprināt ES kiberdrošības spējas , par kuru tika panākta vienošanās telesakaru ministru neoficiālajā sanāksmē 2022. gada 9. martā.

apkopots **Padomes ieteikumā**[16], kas ļaus paātrināt direktīvu efektīvu īstenošanu. Tas piedāvā vienotu pieeju **stresa testu** veikšanai attiecībā uz vienībām, kas ekspluatē kritisko infrastruktūru, sākot ar enerģētikas nozari, pamatojoties uz vienotiem kopīgiem principiem. Darbs pie stresa testiem sāksies nekavējoties, lai tos varētu pabeigt līdz 2023. gada beigām, un 2023. gada aprīlī tiks izvērtēts progress. Plāns, kas Komisijai jāsagatavo sadarbībā ar Padomi, pamatojoties uz attiecīgo Savienības aģentūru atbalstu un ieguldījumu, palīdzēs nodrošināt koordinētu reakciju ES līmenī uz būtiskiem kritiskās infrastruktūras traucējumiem.

Enerģētikas nozarē Komisija strādā pie tīkla kodeksa attiecībā uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem[17], tai skaitā pie noteikumiem par riska novērtējumu, kopīgām minimālajām prasībām, plānošanu, uzraudzību, ziņošanu un krīžu pārvaldību, kas būs pilnībā saskaņoti ar TID2 regulējumu. Atsevišķā pasākumā, reaģējot uz Krievijas agresiju pret Ukrainu, 2022. gada martā Ukrainas un Moldovas Republikas elektrotīkli tika sinhronizēti ar kontinentālās Eiropas tīklu, papildinot riska mazināšanas pasākumus, tai skaitā attiecībā uz kiberdrošību.

Transporta nozarē Komisija sadarbojas ar dalībvalstīm, Eiropas Savienības Aviācijas drošības aģentūru (*EASA*) un ES Izlūkošanas un situāciju centru (ES *INTCEN*) nolūkā regulāri novērtēt ES civilās aviācijas apdraudējuma un riska līmeni konflikta zonās. ES Konfliktu zonu trauksmes izziņošanas sistēma ir minēta kā labākā prakse starptautiskā līmenī[18]. Pasākumi ietver gaisa kravu riska novērtējuma darba plūsmas atsākšanu, pirmo riska novērtējumu ES līmenī nolūkā novērtēt apdraudējumu pasažieru kuģiem un visaptverošu aviācijas drošības riska kartēšanu nolūkā atjaunināt civilās aviācijas apdraudējumu novērtējumu.

Īpaša uzmanība tiek pievērsta arī **jūras kritiskajai infrastruktūrai**[19]. Pašlaik tiek izstrādāta un līdz 2023. gada beigām pilnībā darbosies vienota informācijas apmaiņas vide jūrniecības jomā, kas pēc brīvprātības principa savienos jūras uzraudzības iestādes, nodrošinot gandrīz reāllaika informācijas apmaiņu. Arī Eiropas Krasta apsardzes funkciju forums ir nostiprinājis savas spējas aizsargāties pret kiberuzbrukumiem.

Vairāki pamatprogrammas **"Apvārsnis Eiropa"** pētniecības projekti ir vērsti arī uz to, lai padarītu mūsu digitālo infrastruktūru drošāku un palielinātu spēju novērst un mazināt kiberuzbrukumus[20].

ES kiberdrošības uzlabošana

Komisija un Augstais pārstāvis 2020. gada 16. decembrī nāca klajā ar jaunu **ES kiberdrošības stratēģiju digitālajai desmitgadei**[21] nolūkā stiprināt Eiropas kolektīvo noturību pret kiberdraudiem un nodrošināt, ka iedzīvotāji un uzņēmumi var izmantot uzticamus un drošus pakalpojumus un digitālos rīkus. Stratēģija ir gandrīz pilnībā īstenota.

---

16 Pēc Komisijas priekšlikuma COM(2022) 551 2022. gada 8. decembrī tika pieņemts Padomes ieteikums.

17 To nosaka Elektroenerģijas regula (ES) 2019/943.

18 Starptautiskā Civilās aviācijas organizācija (Dok. 10084 "*Risk Assessment Manual for Civil aircraft Operations Over or Near Conflict Zones*", 2018. gads).

19 Tai skaitā īstenojot *PESCO* spēju projektus un pamatprogrammas "Apvārsnis 2020" projektus.

20 *EU-CIP — European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection* (Eiropas zināšanu centrs un politikas izmēģinājumu telpa kritiskās infrastruktūras aizsardzībai) un *ATLANTIS — The Atlantic Testing Platform for Maritime Robotics: New Frontiers for Inspection and Maintenance of Offshore Energy Infrastructures.*

21 JOIN(2020) 18.

Saskaņā ar TID2 direktīvu ir paredzēts izveidot **Eiropas Kiberkrīžu sadarbības organizāciju tīklu** (***EU-CyCLONe***)[22] nolūkā atbalstīt liela mēroga jeb plašapmēra kiberdrošības incidentu un krīžu koordinētu pārvaldību operatīvā līmenī. Tas nodrošinās regulāru attiecīgās informācijas apmaiņu starp dalībvalstīm un ES iestādēm, struktūrām, birojiem un aģentūrām. Komisija veido **kiberdrošības situācijas un analīzes centru** nolūkā palielināt savas iekšējās spējas. Komisija sadarbojas ar dalībvalstīm, cita starpā veicot turpmākus pasākumus saistībā ar tās ieteikumu par **Kopējo kibervienību**[23] nolūkā nodrošināt ES koordinētu reakciju uz liela mēroga kiberincidentiem. Komisija un Augstais pārstāvis 2022. gadā ir arī aktīvi iesaistījušies kiberdrošības mācībās, kas tika organizētas kopā ar dalībvalstīm[24].

Tīkliem un datorsistēmām nepieciešama pastāvīga uzraudzība un analīze, kas ļautu reāllaikā atklāt ielaušanos un anomālijas. Komisija ir ierosinājusi izveidot **drošības operāciju centru** (*SOC*) tīklu visā ES, kas ļautu uzraudzīt sakaru tīklus un identificēt aizdomīgus notikumus. Palielinot esošos *SOC*, izveidojot jaunus centrus un savienojot *SOC* vairākās dalībvalstīs, tiks palielinātas kolektīvās atklāšanas spējas. Tie varētu izmantot arī jaunāko mākslīgo intelektu (MI) un datu analīzi, aizsargājot civilo sakaru tīklus un paātrinot kiberuzbrukumu atklāšanu[25].

Lai pastiprinātu gatavību nozīmīgiem kiberincidentiem un reaģēšanu uz tiem, Komisija ir izveidojusi arī īstermiņa programmu dalībvalstu atbalstam, izmantojot *ENISA* saņemto papildu finansējumu, tai skaitā kritisko vienību ielaušanās testēšanu iespējamās neaizsargātības noteikšanas nolūkā. Tas var arī palīdzēt dalībvalstīm reaģēt uz incidentiem, ko *ENISA* nodrošina ar uzticamu privāto kiberdrošības pakalpojumu sniedzēju atbalstu, pēc būtiska incidenta, kas skar kritiskas vienības. Nākamais solis būs nodrošināt, lai dalībvalstis pilnībā izmantotu šīs iespējas.

Gan aparatūra, gan programmatūras arvien biežāk tiek pakļautas **kiberuzbrukumiem**. Kiberuzbrukumu skaits un sarežģītība pieaug, un to galvenais vektors ir programmatūras neaizsargātības izmantošana. Divas trešdaļas no visiem incidentiem, par kuriem ziņots saskaņā ar TID, ir saistīti ar programmatūras neaizsargātības izmantošanu. Pieaug arī ietekme uz iedzīvotājiem, infrastruktūru vai uzņēmumiem[26]. Divas trešdaļas no visiem incidentiem, par kuriem ziņots saskaņā ar TID, ir saistīti ar programmatūras neaizsargātības izmantošanu. Komisija 2022. gada septembrī ierosināja **Kibernoturības aktu**[27] nolūkā mazināt neaizsargātību ("ievainojamību") produktos ar digitāliem elementiem un nodrošināt ielāpu un riska mazināšanas pasākumu ātru pieejamību. Tajā ierosināts, ka produktus ar digitāliem elementiem (aparatūru un programmatūru) drīkstētu laist tirgū tikai tad, ja tie atbilst

---

[22] *EU-CyCLONe* veido dalībvalstu kiberkrīžu pārvaldības iestāžu pārstāvji
ar Komisijas līdzdalību gadījumos, kad potenciāls vai notiekošs liela mēroga kiberdrošības incidents būtiski ietekmē
vai var ietekmēt direktīvā paredzētos pakalpojumus un darbības.

[23] COM (2021) 4520.

[24] Kā piemēru var minēt Lietuvas un *ENISA* organizētās operatīvā līmeņa mācības (*Blueprint Operational Level Exercise — Blue OLEx*),
kā arī prezidentvalsts Francijas organizētās mācības "ES kiberkrīzes sasaiste ar solidaritāti" (*EU CyCLES*).

[25] Pirmais posms tika uzsākts ar 2022. gada novembrī publicēto uzaicinājumu iesniegt priekšlikumus "Drošības operāciju centru spēju veidošana"
un uzaicinājumu izteikt ieinteresētību kopā ar *ECCC* iesaistīties kopīgā rīku un infrastruktūru iepirkumā
ar kopējo finansējumu 110 miljonu EUR apmērā no programmas *DIGITAL*.

[26] *ENISA Threat landscape 2022.*

[27] COM(2022) 454.

konkrētām kiberdrošības pamatprasībām[28]. Ražotājiem un izstrādātājiem būtu pienākums piecus gadus nodrošināt savu produktu kiberdrošību un pārredzami informēt patērētājus par kiberdrošību. Tas būtiski veicinās piegādes ķēdes drošību[29].

Lai palielinātu svarīgu digitālās pasaules produktu un pakalpojumu uzticamību un drošību, izšķiroša nozīme ir **sertifikācijai**. Ar Kiberdrošības aktu[30] izveidots Eiropas kiberdrošības sertifikācijas satvars, saskaņā ar kuru Komisija var lūgt *ENISA* izstrādāt sertifikācijas shēmas. Ir izstrādāta uz kopīgiem kritērijiem balstīta Eiropas kiberdrošības sertifikācijas shēma, un tiek gatavotas shēmas mākoņpakalpojumiem un 5G drošībai.

Komisija turpina sadarboties ar dalībvalstīm, lai nodrošinātu, ka **5G tīkli** ir droši un noturīgi, un pārrauga ES 5G rīkkopas īstenošanu valstu un ES līmenī. Lai gan lielākā daļa dalībvalstu jau ir pastiprinājušas vai patlaban pastiprina drošības prasības 5G tīkliem, tagad ir steidzami nepieciešams, lai visas dalībvalstis pabeigtu rīkkopas pasākumu[31] īstenošanu, konkrētāk, lai dalībvalstis ieviestu ierobežojumus attiecībā uz augsta riska piegādātājiem, ņemot vērā to, ka laika zudums var palielināt Savienības tīklu neaizsargātību, kā arī pastiprinātu 5G tīklu kritisko un jutīgo daļu fizisko un nefizisko aizsardzību, tai skaitā izmantojot stingru piekļuves kontroli.

Lai palīdzētu ES un dalībvalstīm īstenot proaktīvu un stratēģisku pieeju kiberdrošības rūpniecības politikai, **Eiropas kiberdrošības kompetenču centrs** sadarbosies ar valstu koordinācijas centriem nolūkā atbalstīt inovācijas kiberdrošības jomā un stiprināt kiberdrošības tehnoloģiju kopienas spējas[32].

ENISA 2022. gada septembrī oficiāli ieviesa **Eiropas kiberdrošības prasmju sistēmu**, kas nosaka šajā jomā visnepieciešamākos darba profilus un nodrošina vienotu Eiropas pamatu prasmju atzīšanas veicināšanai un ar kiberdrošību saistītas apmācības izstrādei. Šī sistēma būs pamatelements Komisijas darba programmā 2023. gadam ierosinātajai **Kiberdrošības prasmju akadēmijai**, kas piedāvās visaptverošu pieeju, kā risināt pieaugošo pieprasījumu pēc kiberdrošības speciālistiem Eiropā.

Ņemot vērā to, ka **ES iestādes, struktūras, biroji un aģentūras (*EUIBA*)** apstrādā konfidenciālu neklasificētu un ES klasificētu informāciju, ir svarīgi, lai tā būtu labi aizsargāta pret kiberuzbrukumiem. Komisija 2022. gada martā ierosināja regulu par vienādi augsta līmeņa kiberdrošību visās šajās struktūrās[33], piemērojot TID2 direktīvas pamatā esošos principus ES institucionālajai videi. Tā ietver jaunu Iestāžu kiberdrošības padomi un pastiprinātu kiberdrošības centru (*CERT-EU*)[34] pienācīgai informācijas apmaiņai un sadarbībai ar dalībvalstu iestādēm, piemēram, izmantojot kiberdrošības incidentu reaģēšanas

---

28 Tikmēr Komisija 2021. gada oktobrī pieņēma deleģēto regulu saskaņā ar Radioiekārtu direktīvu, ar kuru bezvadu ierīču ražotājiem uzliek pienākumu uzlabot ierīču kiberdrošības līmeni, privātumu un aizsardzību pret krāpšanu.

29 Saskaņā ar Padomes secinājumiem par IKT piegādes ķēdes drošību, 2022. gada 17. oktobris.

30 Regula (ES) 2019/881, ar ko ievieš ES mēroga kiberdrošības sertifikācijas satvaru IKT produktiem, pakalpojumiem un procesiem.

31 Dalībvalstis ar Komisijas un *ENISA* atbalstu šā gada sākumā publicēja ziņojumu par kiberdrošību atvērtajiem radiopiekļuves tīkliem, kuri pēc to pilnveides nodrošinās alternatīvu veidu, kā izvērst 5G tīklu radiopiekļuves daļu, pamatojoties uz atvērtām saskarnēm.

32 Ir izveidota *ECCC* valde, un 2022. gada 20. oktobrī notiks tās 4. sanāksme.

33 COM(2022) 122.

34 *CERT-EU* ir arī veikusi ievērojamus ieguldījumus nolūkā vēl vairāk uzlabot savus esošos pakalpojumus *EUIBA* un papildināt tos ar jauniem pasākumiem, kas ļautu labāk novērst un atklāt kiberuzbrukumus un reaģēt uz tiem.

vienību (*CSIRT*) tīklu. Vienlaikus Komisija ir pieņēmusi priekšlikumu regulai par informācijas drošību *EUIBA*[35] nolūkā uzlabot noturību pret kiberdraudiem un hibrīddraudiem, izveidojot vienotu augsta līmeņa informācijas drošības standartu kopumu visām Savienības iestādēm, struktūrām, birojiem un aģentūrām. Ir svarīgi, lai Padome paātrinātu darbu pie šā priekšlikuma, ņemot vērā daudzkārtējos dalībvalstu aicinājumus Komisijai izstrādāt pasākumus, kas labāk aizsargātu ES lēmumu pieņemšanas procesu no jebkāda veida ļaunprātīgām darbībām. *CERT-EU* un *ENISA* ir arī izstrādājušas un izmēģinājušas jauna veida kiberdrošības mācības, kas pielāgotas ES aģentūrām, kā to ieteikusi Eiropas Revīzijas palāta.

Svarīgākie izpildes piemēri

Eiropas kiberdrošības mēnesis (*European Cybersecurity Month — ECSM)*: ieskaitot darbseminārus, sociālo mediju kampaņas un lekcijas, *ECSM* iniciatīva ir paplašinājusies no 184 pasākumiem 2014. gadā līdz 500 pasākumiem 2022. gada oktobrī. Tie palīdz uzlabot lietotāju reaģēšanu tiešsaistē, saskaroties ar kiberdrošības draudiem (par to 2021. gadā ziņoja 73 % aptaujāto dalībvalstu).

Augstākās izglītības datubāze kiberdrošības jomā (*Cybersecurity Higher Education Database — CyberHEAD*): *CyberHEAD* ir visbiežāk apmeklētā *ENISA* tīmekļa vietne pēdējo 2 gadu laikā — aptuveni 70 000 apmeklējumu gadā. Tā ļauj jaunajiem talantiem pieņemt uz informāciju balstītus lēmumus par daudzveidīgajām iespējām, ko piedāvā augstākā izglītība kiberdrošības jomā, un palīdz augstskolām piesaistīt augstas kvalitātes studentus, kuri ir motivēti nodrošināt Eiropas kiberdrošību.

Hibrīddraudu novēršana, cīņa pret ārvalstu iejaukšanos un ES kiberaizsardzības stiprināšana

ES stratēģiskajā kompasā drošībai un aizsardzībai ir izklāstīts vērienīgs rīcības plāns, kā palielināt ES rīcībspēju, stiprināt noturību un labāk investēt ES aizsardzības spējās.

Lai gan **hibrīddraudu** novēršana galvenokārt ir dalībvalstu kompetencē, ES papildina valstu rīcību, atbalstot koordināciju, uzlabojot situācijas apzināšanos, veicinot sadarbību ar līdzīgi domājošām valstīm un starptautiskām organizācijām un nodrošinot kopīgas reaģēšanas iespējas. Pēdējo desmit gadu laikā ES līmenī ir ieviesti vairāk nekā 200 pasākumi nolūkā uzlabot noturību un novērst hibrīddraudus. ES *INTCEN* Hibrīddraudu analīzes vienība piedalās ES lēmumu pieņemšanā un ir galvenā struktūra, kas nodrošina visaptverošu situācijas apzināšanos un stratēģisko prognozēšanu, apkopo visu avotu informāciju un veic izlūkdatu novērtējumus par hibrīddraudiem. Ir sākts darbs, lai izveidotu ES Hibrīddraudu novēršanas ātrās reaģēšanas vienības, par kurām paziņots stratēģiskajā kompasā, nolūkā atbalstīt dalībvalstis un kopējās drošības un aizsardzības politikas misijas un operācijas, kā arī partnervalstis hibrīddraudu novēršanā, kas ļautu īsā laikā piesaistīt attiecīgās valstu un ES speciālās zināšanas, tai skaitā vajadzības gadījumā arī militārās zināšanas. Tiek gatavota ES hibrīddraudu novēršanas rīkkopa, kas nodrošinās sistēmu koordinētai reakcijai uz hibrīdkara kampaņām, kuras ietekmē ES un dalībvalstis, integrējot ārējo un iekšējo dimensiju vienotā plūsmā un apvienojot valsts un ES mēroga apsvērumus. Ievērojams progress ir panākts arī noturības uzlabošanā un hibrīddraudu apkarošanā, nosakot esošās nozaru noturības pamatu[36]. Komisija ir arī turpinājusi analītiskus pētījumus par noturības veidošanu pret hibrīddraudiem[37] un pabeigusi hibrīddraudu apsvērumu integrēšanu politikas veidošanā.

35 COM(2022) 119.
36 SWD(2022) 21.
37 *"Hybrid threats: a comprehensive resilience ecosystem"*, JRC130097.

Covid-19 pandēmija un Krievijas karš pret Ukrainu parādīja, kā manipulācijas ar informācijas vidi var ietekmēt ES un partnerus visā pasaulē. Arvien nozīmīgāks hibrīduzbrukumu elements ir **ārvalstu īstenota informācijas manipulācija un iejaukšanās (*FIMI*)**, kuras mērķis ir graut uzticību ES un uz noteikumiem balstītajai starptautiskajai kārtībai. Lai cīnītos pret informācijas manipulāciju un dezinformāciju, Komisija, pamatojoties uz Eiropas Demokrātijas rīcības plānu, ir ieviesusi konkrētu pasākumu un struktūru kopumu, tai skaitā pārskatīto ES prakses kodeksu dezinformācijas jomā, Digitālo pakalpojumu aktu un priekšlikumu par politiskās reklāmas pārredzamību, par kuru patlaban notiek starpiestāžu sarunas. Rezultātā platformām tiktu noteikti jauni pienākumi un pirmo reizi tiktu ieviesta juridiski saistoša uzraudzības sistēma. Turklāt, kā paziņots Stratēģiskajā kompasā, EĀDD ciešā sadarbībā ar Komisiju un dalībvalstīm turpina izstrādāt **ES rīkkopu pret ārvalstu īstenotu informācijas manipulāciju un iejaukšanos (*FIMI* rīkkopa)** nolūkā veicināt koordinētu reakciju uz ārvalstu dalībnieku manipulatīvu rīcību[38]. EĀDD arī turpināja stiprināt sadarbību ar starptautiskajiem partneriem, piemēram, G7 ātrās reaģēšanas mehānismu (*Rapid Response Mechanism — RRM*) un NATO.

Komisija nosoda jebkādu ārvalstu iejaukšanos ES dalībvalstu suverēnajā teritorijā un pauž bažas par ziņojumiem par Ķīnas aizjūras policijas dienestu stacijām ES, kas, ja tā ir taisnība, būtu pilnīgi nepieņemami. Lai gan šo apgalvojumu izmeklēšana ir dalībvalstu iestāžu kompetencē, Komisija ar Eiropola atbalstu ir gatava veicināt informācijas apmaiņu starp dalībvalstīm. Komisija šo jautājumu izvirzīja Tieslietu un iekšlietu padomes sanāksmē, kas notika 2022. gada decembrī.

Komisija un Augstais pārstāvis 2022. gada novembrī nāca klajā ar jaunu ES **kiberaizsardzības** politiku[39], kurā izklāstīti līdzekļi, kā uzlabot sadarbību un ieguldījumus kiberaizsardzībā ar mērķi panākt labāku aizsardzību pret kiberuzbrukumiem. Mērķis ir aizsargāt ES intereses kibertelpā, palielinot sadarbību starp ES kiberaizsardzības dalībniekiem un izstrādājot mehānismus spēju izmantošanai ES līmenī, tai skaitā saistībā ar KDAP misijām un operācijām. Tas veicinās pilna spektra kiberaizsardzības spēju attīstību un stiprinās sadarbību starp ES militārajām un civilajām kiberdrošības kopienām, uzlabojot situācijas apzināšanos, krīzes koordināciju un apmācību, arī ar privāto sektoru. Tas arī palīdzēs mazināt stratēģisko atkarību kritisko kiberdrošības tehnoloģiju jomā, izstrādājot stratēģisku ceļvedi attiecībā uz kritiskajām kiberdrošības un kiberaizsardzības tehnoloģijām, un stiprināt Eiropas aizsardzības tehnisko un rūpniecisko pamatu.

Stratēģiskajā kompasā **kosmoss** ir atzīts par piekto karadarbības jomu (līdzās sauszemei, jūras, gaisa un kibertelpai), un pausts aicinājums Komisijai un Augstajam pārstāvim izstrādāt pirmo kosmosa stratēģiju drošībai un aizsardzībai. Stratēģijā tiks ierosināti pasākumi nolūkā uzlabot kosmosa sistēmu un pakalpojumu kolektīvās aizsardzības un noturības līmeni, kā arī atturēt no jebkādiem draudiem, tai skaitā kiberdraudiem, sensitīvām kosmosa sistēmām un pakalpojumiem ES un reaģēt uz tiem.

---

[38] Turpinās darbs pie stratēģiskā kompasa uzdevumiem nolūkā
izveidot *FIMI* datu telpu un nodrošināt KDAP misijas un operācijas ar spējām un resursiem, kas ļautu izmantot attiecīgos šīs rīkkopas instrumentus. EĀDD
turpina nodrošināt ES dalībvalstīm atklātā pirmkoda situācijas apzināšanos, izmantojot ES ātrās ziņošanas sistēmu,
palielina sabiedrības informētību, konkrētāk, izmantojot kampaņu *EUvsDisinfo*, un ir vēl vairāk uzlabojis sadarbību ar
ieinteresētajām personām, piemēram, NATO un G7 ātrās reaģēšanas mehānismu.

[39] JOIN(2022) 49.

3. TERORISMA UN RADIKALIZĀCIJAS APKAROŠANA

Lai atbalstītu dalībvalstis cīņā pret terorismu un radikalizāciju, ir pieņemtas gandrīz visas galvenās iniciatīvas, kas izklāstītas ES Drošības stratēģijā. Īpaša uzmanība tika pievērsta aizsardzībai pret apdraudējumiem tiešsaistē. Nākamais solis ir nodrošināt, lai šīs iniciatīvas pilnībā sasniegtu savu ietekmi.

Terorisma apkarošana

Kopš **ES Terorisma apkarošanas programmas**[40] pieņemšanas 2020. gada decembrī tā ir nodrošinājusi ES iespējas labāk paredzēt un novērst terorisma draudus, kā arī aizsargāt no tiem un reaģēt uz tiem. Arī konkrētas ģeogrāfiskas iniciatīvas ir palīdzējušas reaģēt uz mainīgo apdraudējumu situāciju. Ņemot vērā notikumus Afganistānā, ES terorisma apkarošanas koordinators sadarbībā ar Komisiju, Augsto pārstāvi, prezidentvalsti un galvenajām ES aģentūrām izstrādāja **rīcības plānu terorisma apkarošanai attiecībā uz Afganistānu**[41], ko dalībvalstis apstiprināja 2021. gada oktobrī. Nepārprotams sasniegums ir brīvprātīga procedūra pastiprinātām drošības pārbaudēm attiecībā uz personām, kas ierodas no Afganistānas.

Prioritāte ir novērst draudus, ko rada **ārvalstu kaujinieki teroristi, kuri atgriežas** Sīrijā un Irākā. Lai gan galvenā atbildība gulstas uz dalībvalstīm, sadarbība ES līmenī palīdz dalībvalstīm risināt kopīgas problēmas, piemēram, saukt pie atbildības tos, kas pastrādājuši teroristiskus noziegumus, novērst neatklātu ieceļošanu Šengenas zonā un no jauna integrēt un reabilitēt tos ārvalstu kaujiniekus teroristus, kuri atgriežas. Lai nodrošinātu kaujas lauka pierādījumu iekļaušanu ES datubāzēs un informācijas sistēmās, Komisija turpina cieši sadarboties ar dalībvalstīm un galvenajām partnervalstīm. Vienojoties ar dalībvalstīm, ES terorisma apkarošanas koordinators ciešā sadarbībā ar Augsto pārstāvi un Komisiju pēta jaunus veidus, kā uzlabot dzīves apstākļus cietumos un nometnēs Sīrijas ziemeļaustrumos, kas palīdzētu apkarot radikalizāciju.

Ir atjaunināti ar terorisma apkarošanu saistītie ES tiesību akti. Lai sodītu par tādām darbībām kā teroristu apmācība un ceļošana terorisma nolūkā, kā arī teroristu finansēšana, tagad visas dalībvalstis īsteno 2017. gadā pieņemto **direktīvu par terorisma apkarošanu**[42]. Vairākās dalībvalstīs joprojām ir jārisina jautājums par direktīvas nepareizu transponēšanu.

Cīņā pret terorismu ir svarīgi **atņemt teroristiem līdzekļus uzbrukuma veikšanai**. Gandrīz visas dalībvalstis savos tiesību aktos ir iekļāvušas atjauninātos tiesību aktus par šaujamieročiem[43]. 2021. gada februārī stājās spēkā jauni tiesību akti, kuru mērķis ir ierobežot tādu sprāgstvielu prekursoru pieejamību, kurus teroristi varētu izmantot bumbu ražošanai. Pamatojoties uz pieeju, ko izmanto, lai regulētu piekļuvi sprāgstvielu prekursoriem, Komisija pēta, kā ierobežot piekļuvi dažām bīstamām ķīmiskām vielām, ko varētu izmantot uzbrukumu veikšanai.

[40] COM(2020) 795.

[41] Afganistāna: Rīcības plāns terorisma apkarošanai, 2021. gada 29. septembris.

[42] COM(2021) 701. Dalībvalstīm minētā direktīva savā valsts tiesiskajā regulējumā bija jātransponē līdz 2018. gada 8. septembrim.

[43] COM(2015) 750.

Teroristu uzbrukumi vairākkārt ir notikuši **sabiedriskās vietās**. Komisija ir izdevusi rokasgrāmatu sabiedrisko vietu integrētās drošības veicināšanai[44]. Tai seko sīki izstrādāti tehniskie norādījumi[45], instrumenti sabiedrisko vietu neaizsargātības novērtēšanai[46] un visaptverošs atbalsts galvenajām ieinteresētajām personām[47], kā arī Ieteikums par brīvprātīgām tādu rentgena iekārtu veiktspējas prasībām, ko izmanto sabiedriskās vietās (ārpus aviācijas jomas)[48]. Iekšējās drošības fonds 2022. gadā ir finansējis arī 14,5 miljonus EUR vērtus projektus, lai uzlabotu sabiedrisko vietu, tai skaitā kulta vietu, aizsardzību. **Droni** ir ļoti inovatīvs rīks, ko var izmantot ne tikai likumīgiem, bet arī ļaunprātīgiem mērķiem, tai skaitā uzbrukumiem sabiedriskām vietām, privātpersonām un kritiskajai infrastruktūrai. Komisija 2022. gada novembrī pieņēma **Dronu stratēģiju 2.0**[49], kurai 2023. gadā sekos detalizētāka ES pieeja cīņai pret dronu ļaunprātīgu izmantošanu.

Cīņa pret radikalizāciju, kas noved pie vardarbīga ekstrēmisma un terorisma tiešsaistē un bezsaistē

Efektīvas pretterorisma politikas pamatā ir **radikalizācijas** novēršana un apkarošana. Komisija atbalsta dalībvalstis, izveidojot Radikalizācijas izpratnes tīklu (*RAN*), kas apvieno 6000 ekspertu, kuri aktīvi darbojas profilakses jomā. Galvenās jomas, kurās dalībvalstīm tiek sniegts atbalsts, ir cīņa pret vardarbīgām ekstrēmistu ideoloģijām un polarizāciju, kas noved pie radikalizācijas; radikalizācija tiešsaistē un jauno tehnoloģiju ļaunprātīga izmantošana; no ieslodzījuma atbrīvoto likumpārkāpēju reintegrācijas pārvaldība un sagatavošana. ES rīcības kodeksā cīņai pret nelikumīgiem naidīgiem izteikumiem tiešsaistē risināts jautājums par saiknēm starp vardarbīgām ekstrēmistu grupām un ideoloģijām un naida runas izpausmēm[50].

ES strādā arī pie tā, lai novērstu ārvalstu ietekmi un finansējumu, kas atbalsta radikālus/ekstrēmistiskus uzskatus dalībvalstīs. Savukārt Komisija joprojām modri seko līdzi tam, lai ES fondi neatbalstītu nevienu projektu, kas nav saderīgs ar Eiropas vērtībām vai ar ko tiek īstenota nelikumīga programma. Šajā sakarā, tiklīdz ir parakstīts dotāciju līgums, Komisijas pārvaldītie projekti kopš 2021. gada beigām tiek publicēti unikālā platformā, ko dēvē par finansējuma un iepirkuma iespēju platformu. Ir svarīgi, lai dalībvalstis izmantotu šo iespēju pašām pārbaudīt saņēmējus un sniegt Komisijai visu tām pieejamo papildu informāciju. Šajā kontekstā Komisijas ierosinātajā Finanšu regulas pārskatīšanā ir iekļauts jautājums par notiesāšanu par "naida kurināšanu" kā pamats izslēgšanai no ES finansējuma. Komisija aicina Eiropas Parlamentu un Padomi šo jautājumu efektīvi risināt galīgajā redakcijā. Turklāt Komisija veic iekšējus izpratnes veicināšanas pasākumus un izstrādā iekšējās darba metodes, lai nodrošinātu pastiprinātu kontroli projektu atlasē.

Vēl viens svarīgs aspekts ir radikalizācijas novēršana tiešsaistē. **Regula par vēršanos pret teroristiska satura izplatīšanu tiešsaistē**[51] stājās spēkā 2022. gada jūnijā. Kopš tā laika

---

44 SWD(2022) 398.

45 *"Guideline - Building Perimeter Protection"*, EUR 30346 EN.

46 http://counterterrorism.jrc.ec.europa.eu

47 Jo īpaši sk.: *"EU Digital Autumn School"*, JRC127168 Terorisma un ekstrēmisma datubāze: lietotāja rokasgrāmata, JRC130461.

48 Šajā tiesību aktā dalībvalstīm ieteikts ievērot ES veiktspējas prasības, iepērkot rentgena iekārtas, ko izmanto apdraudējuma atklāšanai sabiedriskās vietās (C(2022) 4179).

49 COM(2022) 652.

50 https://ec.europa.eu/commission/presscorner/detail/lv/IP_16_1937.

51 Eiropas Parlamenta un Padomes Regula (ES) 2021/784 (2021. gada 29. aprīlis) par vēršanos pret

valstu kompetentās iestādes var pieprasīt, lai teroristisks saturs tiktu izņemts vienas stundas laikā pēc oficiāla izņemšanas rīkojuma. Tiešsaistes pakalpojumu sniedzējiem, kuri saskaras ar teroristisku saturu, ir jāveic īpaši pasākumi, lai aizsargātu savas platformas pret ļaunprātīgu izmantošanu. Tas papildina **ES Interneta foruma** (*EUIF*) darbu, ko Komisija uzsāka, lai apvienotu dalībvalstis, interneta uzņēmumus un pilsonisko sabiedrību ar mērķi novērst vardarbīga ekstrēmistiska un teroristiska satura izplatīšanu tiešsaistē. Nesenais *EUIF* atbalsts tehnoloģiju uzņēmumiem un interneta infrastruktūras nodrošinātājiem to satura moderācijas centienos ietver teroristu pārvaldīto tīmekļa vietņu direktoriju un katru gadu atjauninātu zināšanu kopumu par vardarbīgiem labējā spārna ekstrēmistu grupējumiem, simboliem un manifestiem[52]. Kopš 2019. gada šajā forumā tiek apspriests arī jautājums par to, kā novērst seksuālu vardarbību pret bērniem tiešsaistē.

Svarīgākie izpildes piemēri

Kā sadarbība ar *Eurojust* palīdzēja notiesāt ārvalstu kaujinieku par terorismu: ar terorismu saistītas izmeklēšanas galvenajam mērķim 2021. gadā tika piespriests četru gadu cietumsods par dalību teroristu organizācijā pēc tam, kad Itālijas iestādes izmantoja Terorisma apkarošanas reģistru nolūkā identificēt saikni starp aizdomās turēto ārvalstu kaujinieku un citām terorisma lietām. *Eurojust* apvienoja valstu iestādes, kā rezultātā tika izpildīti Eiropas izmeklēšanas rīkojumi un savstarpējās tiesiskās palīdzības pieprasījumi.

Eiropola koordinācija pret tiešsaistē pieejamām bumbu izgatavošanas rokasgrāmatām: vienā no regulārām kopīgām iniciatīvām 2022. gada februārī, kuru atbalstīja Eiropols un kurā piedalījās 8 dalībvalstis un Apvienotā Karaliste, tika atrasti simtiem dokumentu tiešsaistē, tai skaitā norādījumi par to, kā izgatavot bumbas, izmantojot prekursorus, un kā tās izmantot teroristu uzbrukumos. Informācija tika nodota tiešsaistes pakalpojumu sniedzējiem.

4. CĪŅA PRET ORGANIZĒTO NOZIEDZĪBU

Organizētās noziedzības vidē Eiropā sadarbība starp noziedzniekiem nemitīgi mainās. Noziedzīgie tīkli var būt iesaistīti dažādās noziedzīgās darbībās, tai skaitā narkotiku tirdzniecībā, organizētos noziedzīgos nodarījumos pret īpašumu, migrantu kontrabandā un cilvēku tirdzniecībā[53]. Kibernoziedzību un ar dzimumu saistītu kibervardarbību vēl vairāk ir veicinājusi plašāka interneta un tiešsaistes pakalpojumu izmantošana. Aizvien plašāka šifrētu saziņas kanālu izmantošana, vienlaikus aizsargājot privātumu un pamattiesības, rada papildu problēmas tiesībaizsardzības iestādēm[54]. Tikmēr Krievijas agresijas kara pret Ukrainu radītie traucējumi ir radījuši jaunas iespējas, ko nekavējoties izmanto organizētās noziedzības grupējumi.

---

teroristiska satura izplatīšanu tiešsaistē, OV L 172, 17.5.2021., 79.–109. lpp.

[52] Citi mērķuzdevumi: atjaunināt ES Krīzes protokolu; rokasgrāmatas ar vadlīnijām par tāda apšaubāma satura un videospēļu ļaunprātīgu izmantošanu, kas veicina radikalizāciju; un pētījums par algoritmiskās amplifikācijas ietekmi uz lietotāju radikalizācijas veicināšanu.

[53] Eiropols (2021. gads), *"European Union serious and organised crime threat assessment, a corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime"*, Eiropas Savienības Publikāciju birojs, Luksemburga.

[54] Interneta organizētās noziedzības draudu novērtējums (*IOCTA*), 2021. gads.

Komisija 2021. gada aprīlī pieņēma **ES Organizētās noziedzības novēršanas stratēģiju 2021.–2025. gadam**[55]. Stratēģijā uzsvērts, cik svarīgi ir izjaukt organizētās noziedzības struktūras, pievēršoties tām grupām, kas rada lielāku risku Eiropas drošībai, un atsevišķām personām noziedzīgo organizāciju augstākajos ešelonos. Stratēģijas īstenošana jau ir sākusies, un vairākas galvenās darbības jau ir pieņemtas vai īstenotas. Komisija ir arī sniegusi finansiālu atbalstu dalībvalstīm nolūkā apkarot noziedzības draudus, ar kuriem saskaras ES[56].

Kibernoziedzība

Paātrinātā digitalizācija Covid-19 pandēmijas laikā veicināja kiberdraudu, piemēram, izspiedējprogrammatūru, izplatīšanos[57]. **Izspiedējprogrammatūras** rada būtiskus kiberdrošības riskus kritiskajai infrastruktūrai un sabiedrības drošībai. Eiropola Kibernoziedzības apkarošanas centrs (*EC3*) kopā ar Kopīgo kibernoziedzības rīcības uzdevumgrupu (*J-CAT*) nesen izstrādāja *International Ransomware Response Model* (Starptautiskā reaģētspēja attiecībā uz izspiedējprogrammatūrām) nolūkā īstenot visaptverošu tiesībaizsardzības iestāžu reakciju. ES piedalījās izspiedējprogrammatūru apkarošanas iniciatīvas 2022. gada samitā nolūkā stiprināt starptautisko sadarbību izspiedējprogrammatūru apkarošanas jomā. 36 valstis un ES vienojās turpināt darbu pie starptautiskās izspiedējprogrammatūru apkarošanas darba grupas izveides nolūkā koordinēt darbu noturības veicināšanai un traucējumu novēršanai un apkarot nelikumīgas finansēšanas darbības[58]. Komisija un Eiropols ir kopīgi izveidojuši atšifrēšanas platformu[59], kas samazina nepieciešamo laiku tiesu ekspertīzes piekļuvei digitālajiem pierādījumiem un palīdz cīnīties pret šifrētiem noziedzīgiem sakaru tīkliem, tādējādi radot ievērojamus triecienus organizētās noziedzības darbībām.

ES palīdzēja sekmīgi risināt sarunas saistībā ar **Budapeštas Konvencijas par kibernoziegumiem** otro papildprotokolu 2022. gada maijā. Tas ietver ļoti nepieciešamos instrumentus pārrobežu sadarbībai kibernoziegumu izmeklēšanas un kriminālvajāšanas jomā, kā arī detalizētus datu aizsardzības nosacījumus un aizsardzības pasākumus. Visām dalībvalstīm būtu nekavējoties jāparaksta otrais papildprotokols, un Eiropas Parlaments tiek aicināts dot savu piekrišanu, kas ļautu to ātri ratificēt. Komisija ES vārdā risina arī sarunas par jaunu Apvienoto Nāciju Organizācijas konvenciju par kibernoziegumiem.

Tikai 2021. gadā vien visā pasaulē ziņots par 85 miljoniem fotoattēlu un videomateriālu, kuros attēlota **seksuāla vardarbība pret bērniem**, taču ir vēl daudz citu gadījumu, par kuriem nav ziņots. Seksuāla vardarbība pret bērniem ir satraucoši plaši izplatīta. Bērni, pavadot vairāk laika tiešsaistē, ir kļuvuši mazāk aizsargāti pret iedraudzināšanu, kā rezultātā ir palielinājies pašizgatavotu seksuālas izmantošanas materiālu daudzums. Saskaņā ar 2020. gada jūlijā pieņemto ES stratēģiju efektīvākai cīņai pret bērnu seksuālu izmantošanu[60] un 2021. gada martā pieņemto ES stratēģiju par bērna tiesībām[61] Komisija 2022. gada maijā

---

55 COM(2021) 170.

56 Komisija 2022. gada jūlijā ar Iekšējās drošības fonda (IDF) starpniecību piešķīra 15,7 miljonus EUR dalībvalstīm,
nolūkā atbalstīt ilgtermiņa projektus un pasākumus Eiropas daudzdisciplīnu platformā pret noziedzības draudiem (*EMPACT*),
risinot desmit ES noziedzības prioritātes, ko Padome pieņēma 2022.–2025. gadam.

57 Interneta organizētās noziedzības draudu novērtējums (*IOCTA*).

58 *"International Counter Ransomware Initiative 2022, Washington DC"*, 2022. gada 1. novembris.

59 Eiropola atšifrēšanas platforma ir izvietota EK Kopīgā pētniecības centra telpās Isprā.

60 COM(2020) 607.

61 COM(2021) 142.

pieņēma priekšlikumu, kurā izklāstīti noteikumi nolūkā novērst un apkarot seksuālu vardarbību pret bērniem tiešsaistē[62], paredzot jaunus pienākumus tiešsaistes pakalpojumu sniedzējiem. Ja preventīvie pasākumi nespēj samazināt būtisku risku, pakalpojumu sniedzējiem var likt atklāt seksuālu vardarbību pret bērniem tiešsaistē, ziņot par to, izņemt un bloķēt šādu saturu. Ar šo priekšlikumu tiktu izveidots arī īpašs ES centrs, lai atvieglotu īstenošanu. Pagaidu tiesību akti, kas tika pieņemti 2021. gada augustā un ļauj tiešsaistes pakalpojumu sniedzējiem turpināt brīvprātīgi atklāt seksuāla vardarbību pret bērniem tiešsaistē un ziņot par to[63], zaudēs spēku 2024. gada vasarā. Tāpēc ir svarīgi, lai Eiropas Parlaments un Padome ātri panāktu vienošanos par ierosināto regulu. Nākamā gada sākumā šo iniciatīvu papildinās priekšlikums atjaunināt 2011. gada direktīvu par seksuālās vardarbības pret bērniem, bērnu seksuālās izmantošanas un bērnu pornogrāfijas apkarošanu[64].

Kibervardarbība pret sievietēm un meitenēm ir jauns **ar dzimumu saistītas kibervardarbības** aspekts. Tiek lēsts, ka 2020. gadā šāda veida vardarbību piedzīvoja katra otrā jauniete[65]. Savā priekšlikumā direktīvai par vardarbības pret sievietēm un vardarbības ģimenē apkarošanu[66], kas tika pieņemts 2022. gada martā, Komisija ierosināja mērķtiecīgus noteikumus par tādu vardarbību pret sievietēm tiešsaistē vai bezsaistē, kas saistīta ar dzimumu[67].

Organizētā noziedzība

Cilvēku tirdzniecība ir viena no galvenajām organizētās noziedzības aktivitātēm ES[68]. Lai gan tā jau ir noteikta kā prioritāte Drošības savienības stratēģijā, noziedznieki Covid-19 pandēmijas laikā atrada jaunas iespējas gūt ievērojamu peļņu un pastiprināt noziedzīgās darbības. Ātra koordinācija ES līmenī palīdz novērst cilvēku tirdzniecības draudus, kas pastiprinājās pēc Krievijas agresijas kara pret Ukrainu. ES koordinators cilvēku tirdzniecības apkarošanas jomā izstrādāja **kopīgu plānu cilvēku tirdzniecības apkarošanas jomā,**[69] kas ļaus apvienot Komisijas un dalībvalstu, ES aģentūru un Eiropas Ārējās darbības dienesta darbu nolūkā novērst cilvēku tirdzniecības riskus un atbalstīt potenciālos upurus. Šie centieni ir palīdzējuši nodrošināt, ka apstiprināto cilvēku tirdzniecības gadījumu skaits joprojām ir ierobežots, pat ja apdraudējums joprojām ir liels.

2021. gada aprīlī pieņemtā ES Stratēģiju cilvēku tirdzniecības apkarošanai 2021.–2025. gadā nodrošināja visaptverošu iekšējo un ārējo rīcības satvaru[70]. Komisija ir nākusi klajā ar priekšlikumu grozīt **direktīvu par cilvēku tirdzniecības apkarošanu**[71], lai novērstu

---

62 COM(2022) 209.

63 COM(2020) 568.

64 Direktīva 2011/93/ES (2011. gada 13. decembris) par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu, OV L 335, 17.12.2011.

65 *"European Parliamentary Research Service (EPRS), Combating gender-based violence*: *Cyberviolence, European added value assessment"*, 2021. gads.

66 COM(2022) 105.

67 Priekšlikums ietver krimināltiesību noteikšanu ES līmenī par intīmu materiālu kopīgošanu bez piekrišanas, kibervajāšanu, kiberuzmākšanos un kiberkūdīšanu uz naidu vai vardarbību. To papildinātu jauns regulējums sadarbībai starp interneta platformām nolūkā labāk aizsargāt sieviešu drošību tiešsaistē.

68 Smagās un organizētās noziedzības draudu novērtējums (*SOCTA*), 2021. gads.

69 *"An Anti-Trafficking Plan to protect people fleeing the war in Ukraine"* (europa.eu).

70 COM(2021) 171.

71 Ceturtajā progresa ziņojumā par cilvēku tirdzniecību, kas jāpieņem kopā ar šo priekšlikumu, ir sniegta padziļināta informācija par ES stratēģijas 2019.–2022. gadam īstenošanu, kā arī galvenie dati un

pašreizējā tiesiskā regulējuma trūkumus un atjauninātu direktīvu nolūkā atspoguļot tiešsaistes dimensiju, kā arī samazināt pieprasījumu. 2022. gada septembrī, *EMPACT* vienotās rīcības dienā, kas bija vērsta pret noziedzīgiem tīkliem, kuri izmanto tīmekļa vietnes un sociālo mediju platformas nolūkā vervēt upurus seksuālai izmantošanai, notika pirmais ES mēroga hakatons pret cilvēku tirdzniecību, ko atbalstīja Eiropols un *Eurojust,* piedaloties tiesībaizsardzības iestādēm no 20 valstīm. Tika identificēti 11 aizdomās turētie cilvēku tirgotāji un 45 iespējamie upuri[72].

Atšķirībā no cilvēku kontrabandas gadījumiem personas, kas maksā kontrabandistiem par nelegālu ieceļošanu ES, to dara brīvprātīgi. Tomēr kontrabandistu darbība ir noziedzīga, bieži vien apdraud dzīvības un var radīt papildu drošības riskus ES. **Migrantu kontrabandas** novēršana un apkarošana ir ES Drošības savienības stratēģijas, ES Organizētās noziedzības novēršanas stratēģijas un jaunā Migrācijas un patvēruma pakta[73] galvenais mērķis. Tam ir nepieciešama pastāvīga starptautiska sadarbība un koordinācija visos līmeņos. Turpinās ES rīcības plāna cīņai pret migrantu kontrabandu 2021.–2025. gadam[74] īstenošana, un ar ES iestāžu, struktūru un aģentūru un ES finansējuma atbalstu tiek veidotas operatīvās partnerības kontrabandas apkarošanai ar Maroku, Nigēru un Rietumbalkāniem.

Nelikumīgo narkotisko vielu tirgus, kura minimālā mazumtirdzniecības vērtība tiek lēsta 30 miljardu EUR apmērā gadā, joprojām ir lielākais noziedzīgais tirgus ES un galvenais ienākumu avots organizētās noziedzības grupējumiem, kā arī apdraud sociālo stabilitāti un veselību. ES rīcības un sadarbības rezultātā 2021. gadā no ielām tika izņemtas narkotiskās vielas 7 miljardu EUR vērtībā[75]. 2020. gada jūlija **ES Narkomānijas apkarošanas programmā un rīcības plānā 2021.–2025. gadam**[76] ir izklāstīti konkrēti pasākumi rīcības pastiprināšanai ES līmenī, tai skaitā Eiropas Narkotiku un narkomānijas uzraudzības centra pārveidošana par Eiropas Savienības Narkotiku aģentūru. Aģentūras pārskatītās pilnvaras, kas ierosinātas 2022. gada janvārī[77], stiprinātu tās uzraudzības un draudu novērtēšanas spējas un spēju reaģēt uz jauniem izaicinājumiem. Padome 2022. gada jūnijā pieņēma vispārēju pieeju, un darbs Eiropas Parlamentā turpinās. Komisija arī uzsāka sadarbību ES interneta forumā nolūkā risināt jautājumu par narkotiku kontrabandu tiešsaistē un ierosināja īpašu tematisku Šengenas izvērtējumu par kokaīna kontrabandu ES ostās. Tika palielināts atbalsts Narkotiku jūras ceļu izpētes un operatīvajam centram. ES turpina arī politiskos dialogus par narkotikām ar trešām valstīm, 2022. gada jūlijā uzsākot otro dialogu ar Ķīnu un 2022. gada jūnijā uzsākot jaunu dialogu ar Kolumbiju.

Saskaņā ar Eiropola datiem gandrīz 99 % noziedzīgi iegūto līdzekļu ES netiek **konfiscēti** un paliek likumpārkāpēju rīcībā[78]. Padomē tiek virzīti priekšlikumi stiprināt ES nelikumīgi iegūtu līdzekļu legalizēšanas un terorisma finansēšanas novēršanas sistēmu, ko Komisija ierosināja 2021. gada jūlijā[79]. Komisija 2022. gada maijā ierosināja pastiprināt un modernizēt

---

statistika.

72 *"20 countries spin a web to catch human traffickers during a hackathon"* | Eiropols (europa.eu)

73 COM(2020) 609.

74 COM(2021) 591.

75 *Eurojust* 2021. gada pārskats.

76 COM(2020) 606.

77 COM(2022) 18.

78 Eiropols, "*Does crime still pay? Criminal Asset Recovery in the EU – Survey of statistical information 2010-2014"*, 2016. gads.

79 COM(2021) 421, COM(2021) 420, COM(2021) 423, COM(2021) 422. 2022. gada jūnijā tika panākta politiska vienošanās par

ES noteikumus par aktīvu atgūšanu un konfiskāciju[80]. Priekšlikums ir apspriests Padomes darba grupās, un vairākās jomās ir panākts progress.

Eiropas Prokuratūra ir nostrādājusi pirmo pilno darba gadu, aizsargājot ES finanšu intereses. Tā saņēma 4006 ziņojumus par noziegumiem, sāka 929 izmeklēšanas un piešķīra iesaldēšanas rīkojumus par kopējo summu 259 miljonu EUR apmērā. Pirmajos septiņos darbības mēnešos izmeklējamās lietas, iespējams, radīja zaudējumus Savienības budžetam 5,4 miljardu EUR apmērā[81].

Komisija arī strādā pie tā, lai sagatavotu **ES rīkkopu viltošanas apkarošanai, kā** paziņots Rīcības plānā intelektuālā īpašuma jomā[82] un uzsvērts Organizētās noziedzības novēršanas stratēģijā.

Korupcija ne tikai grauj uzticību starp valsti un pilsoņiem, bet arī apdraud drošību. Tas ir galvenais organizētās noziedzības instruments un veicina visdažādākās noziedzīgās darbības. Tā ir viena no galvenajām ikgadējā tiesiskuma ziņojuma cikla tēmām[83]. Lai gan dažas ES dalībvalstis joprojām ir vienas no labākajām pasaulē korupcijas apkarošanas jomā, joprojām pastāv daudzas problēmas, jo īpaši attiecībā uz kriminālizmeklēšanu, kriminālvajāšanu un sankciju piemērošanu korupcijas gadījumos. Daudzās dalībvalstīs tiek īstenoti pasākumi korupcijas novēršanas un integritātes sistēmu stiprināšanai, taču korupcijas apkarošanai piešķirtie resursi bieži vien ir nepietiekami. Komisija strādā pie korupcijas apkarošanas tiesību aktu paketes 2023. gadam, ar ko atjauninās un racionalizēs tiesību aktus šajā jomā.

ES 2020.–2025. gada rīcības plāns attiecībā uz **šaujamieroču nelikumīgu tirdzniecību**[84] tika pieņemts kopā ar Drošības savienības stratēģiju 2020. gada jūlijā. Pēc tam 2022. gada oktobrī tika iesniegts priekšlikums pārskatīt noteikumus par šaujamieroču eksporta atļaujām, importa un tranzīta pasākumiem[85], pievēršot lielāku uzmanību digitalizācijai. Kopumā tam vajadzētu uzlabot civilām vajadzībām izmantojamo šaujamieroču izsekojamību. Turpinās arī darbs nolūkā sniegt labāku atbalstu Ukrainai un Moldovas Republikai, nodrošinot **kājnieku ieročus un vieglos ieročus** (VIKI) saistībā ar Krievijas agresiju pret Ukrainu.

Kultūras priekšmetu nelikumīga tirdzniecība ir ienesīgs bizness organizētās noziedzības grupējumiem un dažos gadījumos arī konfliktā iesaistītajām pusēm un teroristiem[86]. Tādējādi tas veicina organizēto noziedzību, kā arī negatīvi ietekmē kultūras mantojumu. Noziedznieki var ļaunprātīgi izmantot pat likumīgi iegādātus kultūras priekšmetus tādiem nolūkiem kā nelikumīgi iegūtu līdzekļu legalizēšana, sankciju apiešana, izvairīšanās no nodokļu

---

līdzekļu pārvedumu regulu un tika panākta arī daļēja vispārēja pieeja
attiecībā uz regulu, ar ko izveido Iestādi nelikumīgi iegūtu līdzekļu legalizēšanas un terorisma finansēšanas novēršanai
(izņemot noteikumus par resursiem un atrašanās vietu).

80 COM(2022) 245 final.

81 *EPPO* pirmais gada pārskats, 2022. gads.

82 COM(2020) 760.

83 Jaunākais ziņojuma izdevums tika pieņemts 2022. gada 13. jūlijā (COM(2022) 500).

84 COM(2020) 608 final.

85 COM(2022) 480.

86 Sk., piemēram, Apvienoto Nāciju Organizācijas Drošības padomes Rezolūcijas 2199 (2015), 2253 (2015), 2322 (2016), 2347 (2017), 2462 (2019) un 2617 (2021); G20 kultūras ministru 2021. gada 30 jūlija Romas deklarāciju.

maksāšanas vai terorisma finansēšana. Lai pastiprinātu **cīņu pret kultūras priekšmetu nelikumīgu tirdzniecību**, Komisija šodien pieņem rīcības plānu[87].

Saskaņā ar Interpola un Apvienoto Nāciju Organizācijas Vides programmas datiem **noziegumi pret vidi** ir ceturtā lielākā noziedzīgā darbība pasaulē pēc narkotiku tirdzniecības, cilvēku tirdzniecības un viltošanas. Pašlaik tiek apspriesti vērienīgi Komisijas priekšlikumi jaunai direktīvai par noziegumiem pret vidi[88], jaunai regulai par atkritumu sūtījumiem[89] un jaunai regulai par atmežošanu[90]. Pēc pieņemšanas tie stiprinās izpildes ķēdi un nodrošinās lielākas sankcijas un atbilstošus izmeklēšanas instrumentus. Tos papildina arī pārskatīts rīcības ES rīcības plāns savvaļas dzīvnieku un augu kontrabandas apkarošanai[91].

Svarīgākie izpildes piemēri

Encrochat: ar Eiropola un *Eurojust* atbalstu Beļģijas, Francijas un Nīderlandes tiesu un tiesībaizsardzības iestādes sadarbojās, lai bloķētu šifrētu sakaru izmantošanu lielos organizētās noziedzības grupējumos. Laikā, kad pakalpojums tika slēgts, tam bija 60 000 abonentu, no kuriem aptuveni 90 % bija kriminālnoziedznieki.

ES tiesu un policijas sadarbības rezultātā tika likvidēts liela mēroga organizētās noziedzības grupējums (“*Pollino* lieta”): kopēja izmeklēšanas grupa, kas 2016. gadā tika izveidota starp Itāliju, Vāciju un Nīderlandi, uzsāka rīcības dienu, kuru koordinēja *Eurojust* un atbalstīja Eiropols un kuras rezultātā 34 personas tika notiesātas un kopumā tika piespriests vairāk nekā 400 gadu cietumsods. Vēlāk vēl 12 personas tika notiesātas uz vairāk nekā 173 gadiem cietumā, un vairākās dalībvalstīs tiesvedība joprojām turpinās.

4. MŪSU ROBEŽU DROŠĪBAS GARANTĒŠANA UN ATBALSTS TIESĪBAIZSARDZĪBAS UN TIESU IESTĀŽU SADARBĪBAI

Papildus ekonomiskajiem un sociālajiem ieguvumiem labi funkcionējoša **Šengenas zona** ir būtiska ES drošībai. Tam nepieciešama efektīva ES ārējo robežu pārvaldība un ciešāka tiesībaizsardzības iestāžu sadarbība. Komisija 2021. gada jūnijā pieņēma stratēģiju “Stratēģija pilnībā funkcionējošai un noturīgai Šengenas zonai”[92], kurā izklāstīts, kā ar pasākumiem drošības, policijas un tiesu iestāžu sadarbības jomā var nodrošināt, ka ES arī bez iekšējās robežkontroles ir spēcīga pret drošības apdraudējumiem. Stratēģija tagad tiek īstenota ikgadējā Šengenas ciklā, kas ir jauns Šengenas zonas pārvaldības modelis, un progress ir atspoguļots pirmajā ziņojumā par Šengenas stāvokli, kas tika pieņemts 2022. gada maijā[93]. Būtisks solis ir grozītais Šengenas Robežu kodekss,[94] kurā ar Komisijas 2021. gada decembra priekšlikumu tika iekļauti jauni noteikumi nolūkā atbalstīt efektīvu sadarbību drošības jomā un pasākumus, kas jāveic, lai efektīvāk pārvaldītu ārējās robežas krīzes situācijās. Tā kā no 2022. gada jūnija ir paredzēts īstenot Padomes vispārējo pieeju, ir svarīgi, lai Eiropas Parlaments un Padome nekavējoties pabeigtu sarunas. Komisija arī uzsvēra ieguvumus, iekļaujot Bulgāriju, Rumāniju un Horvātiju visos Šengenas aspektos, tādējādi stiprinot

87 COM(2022) 800.
88 COM(2021) 851.
89 COM(2021) 709.
90 COM(2021) 706.
91 COM(2022) 581.
92 COM(2021) 277.
93 COM(2022) 301.
94 COM(2021) 891.

drošību un savstarpēju uzticēšanos Šengenas zonā[95]. Padome 2022. gada decembrī pieņēma lēmumu par Šengenas *acquis* pilnīgu piemērošanu Horvātijā[96].

Zonā bez iekšējās robežkontroles policijas ierēdņiem vienā dalībvalstī būtu jāspēj piekļūt tai pašai informācijai, kas ir pieejama kolēģiem citā dalībvalstī. Normai jābūt pilnīgai un efektīvai sadarbībai. Tāpēc ir svarīgi pastiprināt tiesībaizsardzības un tiesu iestāžu rīcībā esošos **informācijas apmaiņas un pārrobežu sadarbības** rīkus visā ES. Policijas sadarbības pakete, kas pieņemta 2021. gada decembrī,[97] ļāva būtiski uzlabot pieejamos rīkus. **Ar direktīvu par informācijas apmaiņu** tagad ir panākta politiska vienošanos starp Eiropas Parlamentu un Padomi, un 2022. gada jūnijā Padome pieņēma Padomes ieteikumu, ar ko pastiprina operatīvo pārrobežu policijas sadarbību. Turpinās sarunas par regulu, ar ko pārskatīs Prīmes sistēmu[98], kas ļaus nodrošināt datu efektīvāku automatizētu apmaiņu starp tiesībaizsardzības iestādēm konkrētās jomās, piemēram, DNS, daktiloskopisko un transportlīdzekļu reģistrācijas datu jomā, kā arī pievienot policijas reģistru un sejas attēlu datus. Ātra vienošanās par **Prīmes II regulu** ļautu visu jauno informācijas apmaiņas rīku klāstu ieviest praksē dalībvalstu tiesībaizsardzības iestādēs.

Lai efektīvāk apkarotu pārrobežu noziedzību, dalībvalstu tiesībaizsardzības un tiesu sistēmām ir jāstrādā ciešā sadarbībā ar tādu ES aģentūru kā Eiropols un *Eurojust* atbalstu. **Eiropola** jaunās pilnvaras stājās spēkā 2022. gada jūnijā, ļaujot Eiropolam palielināt savas speciālās zināšanas un operatīvās spējas, lai labāk atbalstītu dalībvalstis cīņā pret smagu un organizētu noziedzību un terorismu. Pilnvaras arī nostiprina Eiropola datu aizsardzības sistēmu un Eiropas Datu aizsardzības uzraudzītāja īstenoto pārraudzību. Noziegumu izmeklēšanā un kriminālvajāšanā dažādu dalībvalstu izmeklēšanas iestādēm un tiesām ir savstarpēji jāsadarbojas un jāsniedz atbalsts, kā arī droši un ātri jāapmainās ar informāciju un pierādījumiem. 2021. gada decembrī pieņemtā **digitālā tieslietu sistēmu pakete**[99] ietvēra praktiskus pasākumus nolūkā uzlabot digitālo informācijas apmaiņu par pārrobežu terorisma lietām, izveidot sadarbības platformu, kas ļautu atbalstīt kopējo izmeklēšanas grupu darbību un veicināt pārrobežu tiesu iestāžu sadarbības digitalizāciju un tiesu iestāžu pieejamību civillietās, komerclietās un krimināllietās. Ja Eiropas Parlaments un Padome ātri pieņemtu šo tiesību aktu paketi, tiktu būtiski veicināta informācijas apmaiņa starp tiesu iestādēm.

Elektroniskie pierādījumi ir gandrīz katras izmeklēšanas sastāvdaļa. 2022. gada novembrī panāktā provizoriskā politiskā vienošanās par **e-pierādījumiem**[100] nodrošinās drošu apmaiņu ar dalībvalstu tiesu iestādēm kritiski svarīgiem pierādījumiem, veicinot efektīvāku noziedzības apkarošanu.

ES ārējo robežu aizsardzība ir kopīga atbildība. Kopš 2021. gada janvāra ir veiksmīgi izvietotas pirmās Eiropas Robežu un krasta apsardzes pastāvīgā korpusa vienības, un šobrīd pastāvīgajā korpusā ir aptuveni 4800 *Frontex* un valstu virsnieku.

Šogad ir palielinājies nelegālo ieceļotāju skaits lielākajā daļā migrācijas maršrutu, apliecinot to, cik svarīgi ir sistemātiski veikt visu to migrantu identitātes un drošības pārbaudes, kuri

[95] COM(2022) 636.

[96] No 2023. gada 1. janvāra tiks atceltas personu pārbaudes pie iekšējām sauszemes un jūras robežām starp Horvātiju un pārējām Šengenas zonas valstīm. No 2023. gada 26. marta tiks atceltas pārbaudes pie iekšējām gaisa robežām.

[97] COM(2021) 782, COM(2021) 780.

[98] COM(2021) 784.

[99] COM(2021) 756, COM(2021) 757, COM(2021) 759.

[100] COM(2018) 225, COM(2018) 226.

ierodas pie ES ārējām robežām, kā arī veikt kopīgiem standartiem atbilstīgas veselības pārbaudes. Drošība ir svarīgs temats jaunajā Migrācijas un patvēruma paktā. Migrantu ātra novirzīšana uz attiecīgajām procedūrām saskaņā ar **priekšlikumu par skrīningu** palīdzētu nodrošināt, ka drošības pārbaudes tiek veiktas, pilnībā ievērojot visus ar pamattiesībām saistītos pienākumus. Joprojām tiek gaidīta Eiropas Parlamenta nostāja attiecībā uz šo priekšlikumu.

Baltkrievijas režīma īstenotā **migrantu instrumentalizācija** politiskos nolūkos 2021. gada otrajā pusē radīja vēl nepieredzētas juridiskas, operatīvas un cilvēciskas problēmas, tai skaitā drošības jomā. Šengenas Robežu kodeksa priekšlikumā risināts arī jautājums par migrantu instrumentalizāciju, ko īsteno trešās valstis politiskos nolūkos. Dalībvalstis, kas saskaras ar šādu situāciju, piemēram, varētu ierobežot robežšķērsošanas vietu skaitu un pastiprināt robežu uzraudzību.

Lai labāk atbalstītu valstu iestāžu darbu drošības, kā arī robežu un migrācijas pārvaldības jomā, tiek izstrādāta jauna ES **informācijas sistēmu** arhitektūra. Tās centrā ir atjaunotā Šengenas Informācijas sistēma, kurai būtu jāsāk darboties 2023. gada martā. Citi galvenie rīki ir ieceļošanas/izceļošanas sistēma (plānots, ka tā sāks darboties 2023. gada maijā), Eiropas ceļošanas informācijas un atļauju sistēma *ETIAS* (tai jāsāk darboties līdz 2023. gada beigām) un Vīzu informācijas sistēmas (VIS) atjauninājums. Tie ļaus veikt vairāk pārbaužu un novērst drošības informācijas nepilnības, nodrošinot labāku informācijas apmaiņu starp dalībvalstīm. Šajā darbā būtiska nozīme ir sistēmu savstarpējai izmantojamībai: ir svarīgi, lai *eu-LISA* un dalībvalstis nekavējoties veiktu nepieciešamos pasākumus, kas ļautu šo vērienīgo projektu pilnībā īstenot līdz 2024. gada beigām.

Lai samazinātu riskus ES un tās iedzīvotājiem, **ienākošo preču kontrolei** ir jābūt efektīvai, vienlaikus nodrošinot likumīgu ES uzņēmumu konkurētspēju. Šo preču drošības kontrole ir uzlabota, izmantojot modernizētu ES importa kontroles sistēmu[101], lai atbalstītu efektīvu, uz risku balstītu muitas kontroli un pasākumus gaisa kravu drošības aizsardzībai pret terorisma draudiem. Muitas kontroles iekārtu atbalsta instrumenta (*CCEI*) programma[102] finansē arī relevantu, mūsdienīgu un uzticamu muitas kontroles iekārtu pārredzamu iegādi, uzturēšanu un atjaunināšanu.

Iepriekšējas pasažieru informācijas (IPI) spēju veicināt drošību kavē novecojuši un nevienmērīgi piemēroti noteikumi. Ar jaunajiem Komisijas priekšlikumiem tiktu atcelta pašreizējā IPI direktīva nolūkā precizēt un uzlabot IPI izmantošanu gan robežu pārvaldībā, gan tiesībaizsardzībā[103]. Tas paplašinātu IPI izmantošanu, attiecinot to uz atsevišķiem ES iekšējiem lidojumiem, tādējādi paplašinot dalībvalstu tiesībaizsardzības iestādēm pieejamo rīkkopu Šengenas zonā. Turpinās apspriedes par ES politikas ārējo dimensiju attiecībā uz **pasažieru datu reģistru** (PDR), ņemot vērā to, ka arvien vairāk trešo valstu attīsta spēju apstrādāt šo informāciju tiesībaizsardzības un robežu drošības vajadzībām. Lai efektīvi atklātu noziedzniekus un teroristus, Komisija gatavo arī tiesību akta priekšlikumu par sistēmu savstarpējai piekļuvei ar drošību saistītai informācijai, kas paredzēta ES un trešo partnervalstu priekšposteņa darbiniekiem.

---

[101] Importa kontroles sistēma 2 (*ICS2*) sāks darboties trīs versijās (2021. gada martā, 2022. gada martā un 2023. gada martā). Katra versija skars dažādus uzņēmējus un transporta modeļus.

[102] Regula (ES) 2021/1077 (2021. gada 24. jūnijs), ar ko izveido finansiālā atbalsta instrumentu muitas kontroles iekārtām,
kurš ir daļa no Integrētās robežu pārvaldības fonda.

[103] COM (2022) 729 un 731.

Ceļošanas dokumentu viltošana veicina noziedznieku un teroristu nelikumīgu pārvietošanos, un tai ir būtiska nozīme cilvēku un narkotiku tirdzniecībā. Tas ir jārisina vienlaikus ar nepieciešamību atvieglot likumīgu ceļošanu, tāpēc kopš 2021. gada augusta dalībvalstis izsniedz personas apliecības ar saskaņotiem drošības standartiem, tai skaitā mikroshēmu ar biometriskiem identifikatoriem, ko var pārbaudīt visas ES robežkontroles iestādes[104]. Komisija gatavo turpmāku iniciatīvu attiecībā uz ceļošanas dokumentu digitalizāciju un ceļošanas atvieglošanu[105], kas uzlabos drošību un paātrinās ceļošanas un robežšķērsošanas procesus, izmantojot ceļošanas un persondatu elektronisku, uzlabotu paziņošanu un biometriskās pārbaudes pie robežām.

Tiesībaizsardzība un jaunās tehnoloģijas

Tādas tehnoloģijas kā **mākslīgais intelekts** vai šifrēšana var sniegt pievienoto vērtību tiesībaizsardzības un tiesu iestādēm, bet var arī traucēt to darbu. Paziņojumā par mākslīgo intelektu (MI) un Mākslīgā intelekta aktā[106] Komisija uzsvēra, ka mākslīgais intelekts var būtiski sekmēt Drošības savienības stratēģijas mērķu sasniegšanu, vēršoties pret pašreizējiem draudiem un paredzot nākotnes riskus un iespējas[107]. Saskaņā ar ES pētniecības un inovācijas programmu "Apvārsnis Eiropa" laikposmam no 2021. līdz 2027. gadam ir pieejams finansējums **civilās drošības pētniecības** darbībām un inovācijai, tai skaitā attiecībā uz MI vai biometriju. Tikai 2021. un 2022. gadam vien jau ir ieplānoti 413,8 miljoni EUR[108].

Svarīgākais izpildes piemērs

Šengenas Informācijas sistēmas (*SIS*) izmantošana: 2021. gadā dalībvalstis *SIS* veica gandrīz 7 miljardus meklējumu. Dalībvalstu iestādes vidēji dienā sistēmā veica gandrīz 20 miljonus meklējumu, kas ļāva atrast vidēji 600 informācijas atbilsmes attiecībā uz ārvalstu brīdinājumiem dienā, kas palīdzēja atrisināt līdzvērtīgu skaitu lietu. Piemēram, pēc brutālas dubultslepkavības Rumānijā 2021. gadā vainīgais tika atrasts Itālijā tikai dažas dienas vēlāk, pateicoties *SIS* brīdinājumam par aizturēšanu, kas informēja Itālijas izmeklētājus, kuriem izdevās arestēt vīrieti Romā.

5. IEKŠĒJĀS UN ĀRĒJĀS DROŠĪBAS SAIKNE: DROŠĪBA ES KAIMIŅVALSTĪS UN PARTNERVALSTĪS

Notikumi ārpus ES robežām un drošība Eiropā ir cieši saistīti. Lai uzlabotu ES iekšējo drošību, ir nepieciešams atbalstīt un palīdzēt mūsu kaimiņvalstīm un partneriem uzlabot to

[104] Pamatojoties uz Eiropas Parlamenta un Padomes Regulu (ES) 2019/1157 (2019. gada 20. jūnijs) par Savienības pilsoņu personas apliecību un Savienības pilsoņiem un viņu ģimenes locekļiem, kuri izmanto tiesības brīvi pārvietoties, izsniegto uzturēšanās dokumentu drošības uzlabošanu (OV L 188, 12.7.2019., 67. lpp.).

[105] EUR-lex 52022PC0658.

[106] COM(2021) 206.

[107] COM(2021) 205.

[108] Pamatprogrammass "Apvārsnis Eiropa" ietvaros turklāt tiek ieguldīti ievērojami līdzekļi inovatīvajās tehnoloģijās, kas paredzētas tiesībaizsardzības iestādēm cīņā pret radikalizāciju, kā arī projektos narkotiku un sprāgstvielu atklāšanas, kultūras priekšmetu kontrabandas, migrantu kontrabandas, sabiedrisko vietu drošības un identitātes zādzību jomā.

iekšējo drošību un sadarboties ar mūsu sabiedrotajiem un starptautiskajām organizācijām, piemēram, NATO vai ANO.

Eiropas Ārējās darbības dienests (EĀDD) un Komisijas dienesti cieši sadarbojas ar galvenajām partnervalstīm un starptautiskajām organizācijām, izmantojot regulārus **terorisma apkarošanas** (TA) dialogus. Pašlaik notiek vairāk nekā 30 TA dialogi ar trešām valstīm un starptautiskām organizācijām[109]. Vienlaikus ir pastiprināts terorisma apkarošanas un drošības ekspertu tīkls ES delegācijās galvenajās trešās valstīs.

Lai labāk novērstu iekšējās drošības apdraudējumus, kas izriet no Krievijas agresijas kara pret Ukrainu, Komisijas dienesti un EĀDD kopā ar ES terorisma apkarošanas koordinatoru vienojās ar **Ukrainu** izveidot pastāvīgu strukturētu sadarbību drošības jomā. Šīs sadarbības mērķis ir uzlabot operatīvo sadarbību, tai skaitā ar Eiropolu un *Frontex*, un stiprināt informācijas apmaiņu par iekšējās drošības apdraudējumiem. ES aģentūras sniedza tūlītēju atbalstu, reaģējot uz problēmām pēc iebrukuma. Šobrīd reģionā ir izvietoti 277 *Frontex* darbinieki, 15 Eiropola darbinieki un 60 Eiropas Savienības Patvēruma aģentūras darbinieki.

Dalībvalstu tiesībaizsardzības iestādes un to partneri sadarbojas **Eiropas daudzdisciplīnu platformas pret noziedzības draudiem (*EMPACT*)** ietvaros, organizējot operatīvus pasākumus un vienotās rīcības dienas pret jauniem vai mainīgiem noziedzīgiem draudiem, kas saistīti ar Krievijas agresiju pret Ukrainu.

ES un Ukrainas **kiberdrošības dialogs** ir pastiprināts ar saskaņotu politisku, finansiālu un materiālu atbalstu no ES puses nolūkā palīdzēt Ukrainai stiprināt tās kibernoturību. Kopējais finansējums 29 miljonu EUR apmērā Ukrainas kibernoturības un digitālās noturības palielināšanai ir atbalstījis kiberdrošības aprīkojumu, programmatūru un noturīgu digitālo pārveidi.

Moldovas Republikai tās ģeogrāfiskās atrašanās vietas dēļ ir būtiska nozīme, risinot Krievijas iebrukuma Ukrainā kriminālās sekas un ietekmi uz drošību. Komisija sadarbībā ar EĀDD 2022. gada jūlijā izveidoja ES atbalsta centru iekšējās drošības un robežu pārvaldības jomā ar Moldovas Republiku. Tā galvenais uzdevums ir veicināt sadarbību un operatīvu rīcību nolūkā novērst kopīgus drošības apdraudējumus sešās prioritārajās jomās, ko kopīgi noteikušas ES un Moldovas Republika: šaujamieroču tirdzniecība, migrantu kontrabanda, cilvēku tirdzniecība, terorisma un vardarbīga ekstrēmisma novēršana un apkarošana, kibernoziedzība un narkotiku tirdzniecība. Moldovas Republika 2022. gada martā parakstīja statusa nolīgumu ar *Frontex,* pamatojoties uz tās pastiprinātajām pilnvarām.

Pēdējos trīs gados turpināja pastiprināties tiesībaizsardzības sadarbība starp ES un **Rietumbalkānu valstīm**, izmantojot arī ES aģentūras. Saskaņā ar Padomes 2021. gada marta secinājumiem tiesībaizsardzības sadarbība ar trešām valstīm tika iekļauta visos Eiropas daudzdisciplīnu platformas pret noziedzības draudiem (*EMPACT*) operatīvajos rīcības plānos, tādējādi veicinot Rietumbalkānu līdzdalību *EMPACT* pasākumos. Ievērojams finansējums saskaņā ar Pirmspievienošanās instrumentu joprojām tiek nodrošināts tiesībaizsardzības reformai un darbības rezultātiem, un ES aģentūras arī nodrošina spēju veidošanu drošības jomas dalībniekiem. Ir panākts labs progress, īstenojot 2018. gadā parakstīto kopīgo rīcības

[109] 2022. gadā notika TA dialogi ar ANO, Izraēlu, Indiju; gaidāmi dialogi ar Turciju, Kataru un Apvienotajiem Arābu Emirātiem (AAE). 2023. gadā galvenie gaidāmie dialogi ir ar Maroku, Tunisiju, Ēģipti, Keniju, ASV un Saūda Arābijas Karalisti, iespējams, arī ar Alžīriju.

plānu terorisma apkarošanai, un attiecībā uz Ziemeļmaķedoniju un Albāniju, ņemot vērā to, ka lielākā daļa pasākumu ir pabeigti, 2022. gada decembrī tika parakstīta attiecīgo divpusējo nolīgumu pārskatīta atjaunināta versija nolūkā turpināt uzlabot mūsu sadarbību terorisma apkarošanas un vardarbīga ekstrēmisma novēršanas un apkarošanas jomā.

Padome 2022. gada 18. novembrī pilnvaroja sākt sarunas par ***Frontex* statusa nolīgumiem** starp ES un Albāniju, Serbiju, Melnkalni un Bosniju un Hercegovinu[110]. Šie nolīgumi ļautu *Frontex* izvietot robežu pārvaldības vienības robežkontroles uzdevumu veikšanai attiecīgo valsts iestāžu vadībā. Tas būs īpaši noderīgi cīņā pret migrantu kontrabandu. Ziemeļmaķedonija 2022. gada oktobrī parakstīja statusa nolīgumu ar *Frontex,* pamatojoties uz tās pastiprinātajām pilnvarām.

ES un ASV īsteno arī ilgstošu partnerību un sadarbību drošības jautājumos, kuras mērķis ir sistemātiskāka un savlaicīgāka informācijas apmaiņa par tādiem jautājumiem kā terorisms, radikalizācija un organizētā noziedzība. ES un ASV regulāri rīko kopīgas sanāksmes tieslietu un iekšlietu jomā nolūkā padziļināt sadarbību kopīgu interešu jautājumos, veicināt globālo drošību un informēt viena otru par likumdošanas progresu TI lietās. Eiropas tiesu un tiesībaizsardzības iestādes cieši sadarbojas ar ASV kolēģiem operatīvajos un likumdošanas jautājumos. ASV tiesībaizsardzības iestādes aktīvi piedalās vairākos *EMPACT* pasākumos un tīklos, un ASV un Eiropols ir noslēguši operatīvās sadarbības nolīgumu. Spēcīgs efektīvas sadarbības piemērs ir operatīvā darba grupa *Greenlight/Trojan Shield,* kas ir viena no līdz šim lielākajām un sarežģītākajām tiesībaizsardzības operācijām cīņā pret šifrētām noziedzīgām darbībām. Teroristu finansēšanas izsekošanas programma starp ES un ASV nodrošina daudzus konkrētus pavedienus terorisma izmeklēšanā[111]. Sadarbības pamatā ir arī skaidra drošības pasākumu un kontroles uzraudzība.

Regulāri ES un ASV kiberdrošības dialogi stiprina sadarbību un koordināciju gan kiberdiplomātijas, gan kibernoturības, tai skaitā kiberdrošības standartizācijas, jomā. Tirdzniecības un tehnoloģiju padome (*TTC*) ir ļāvusi padziļināt sadarbību, sagatavojot kopīgu paziņojumu par kiberdrošību un pasākumus iespējamai sadarbībai pētniecības un izstrādes jomā ārpus 5G un 6Geksporta kontroles un ieguldījumu pārbaudes jomā, kā arī attiecībā uz sankcijām pret Krieviju un Baltkrieviju. *TTC* arī veicinās ES un ASV sadarbību ārvalstu īstenotas informācijas manipulācijas un iejaukšanās jomā.

Nozīmīgas drošības problēmas Āfrikā tieši ietekmē Āfrikas iedzīvotājus, kā arī ES drošību. Daudzi projekti tiek īstenoti, lai palīdzētu partnervalstīm veidot spējas risināt šīs problēmas, piemēram, finansējot starptautisko terorisma apkarošanas akadēmiju (*AILCT*) Rietumāfrikā vai izmantojot reģionālo iniciatīvu nolūkā apkarot nelikumīgi iegūtu līdzekļu legalizēšanu un terorisma finansēšanu Lielā raga reģionā.

Latīņamerikas un Karību jūras reģiona valstis (*LAC*) ir nozīmīgas ES partnervalstis, un 2022. gada maijā tika uzsākta jauna Eiropas reģionālās komandas iniciatīva drošības un tiesiskuma jomā nolūkā izveidot ES un *LAC* partnerību tiesiskuma stiprināšanai un cīņai pret organizēto noziedzību.

[110] Padomes Lēmums (ES) 2022/2271: Albānija; Padomes Lēmums (ES) 2022/2272: Bosnija un Hercegovina; Padomes Lēmums (ES) 2022/2273: Melnkalne; Padomes Lēmums (ES) 2022/2274: Serbija.

[111] Sk. sesto kopīgo pārskatu par *TFTP* nolīguma īstenošanu, COM(2022) 585.

ES **Ārvalstu tiešo ieguldījumu izvērtēšanas** regula stājās spēkā 2020. gada oktobrī[112], un tā nodrošina regulējumu nolūkā uzlabot aizsardzību pret ārvalstu tiešajiem ieguldījumiem, kas apdraud drošību vai sabiedrisko kārtību vairāk nekā vienā dalībvalstī. Pirmajā pilnajā darbības gadā Komisijai tika paziņots par vairāk nekā 400 lietām. Ar 2021. gada septembrī pieņemto Divējāda lietojuma preču regulu[113] tika modernizēta un nostiprināta ES **divējāda lietojuma preču eksporta kontroles** sistēma un ieviesti jauni noteikumi, kas ļauj ES, saskaņojot ar dalībvalstīm, pieņemt autonomas pārbaudes sarakstā neiekļautu preču un tehnoloģiju eksportam.

Globalizētā pasaulē, kurā smagi noziegumi un terorisms iegūst aizvien pārvalstiskākas dimensijas, tiesībaizsardzības un tiesu iestādēm vajadzētu būt pilnīgi sagatavotām sadarboties ar ārējiem partneriem, lai garantētu savu pilsoņu drošību. Tādēļ **Eiropolam un *Eurojust*** ir jāpaver iespējas sadarbībai un informācijas apmaiņai starp trešo valstu tiesu iestādēm. Pēc 2022. gada jūnijā parakstītā nolīguma starp Eiropolu un Jaunzēlandi par persondatu apmaiņu smagu noziegumu un terorisma apkarošanas nolūkā[114] notiek sarunas ar vairākām citām valstīm, taču vairumā gadījumu progress joprojām ir lēns. Attiecībā uz *Eurojust* sarunas ir krietni pavirzījušās uz priekšu ar Armēniju, kur ir panākta vienošanās par tekstu, un ir uzsāktas sarunas ar Kolumbiju, Alžīriju un Libānu.

Ceturtajā vadītāju dialogā par terorisma apkarošanu, kas notika 2022. gada aprīlī, **ES un ANO** veica konkrētus pasākumus esošās partnerības stiprināšanai cīņā pret pastāvīgiem, bet jauniem apdraudējumiem starptautiskajam mieram un drošībai. Stratēģiskā partnerība tika vēl vairāk nostiprināta, izveidojot jaunu "ES un ANO Globālo terorisma draudu mehānismu", kas ir ES finansēta iniciatīva to valstu atbalstam, kuras saskaras ar terorismu un vardarbīgu ekstrēmismu, kā arī sniedzot palīdzību, apmācot un sniedzot konsultācijas. Citi kopīgu interešu jautājumi ietver jaunus draudus, kas saistīti ar jaunajām tehnoloģijām, tai skaitā to, kā tās ietekmē jauniešus kā konkrētu mērķgrupu, kas radikalizējas vardarbībai, un terorismu, kā pamatā ir ksenofobija, rasisms un citi neiecietības veidi vai kas tiek īstenots reliģijas vai pārliecības vārdā.

Ir pastiprināta arī **ES un NATO** sadarbība, nodrošinot taustāmus rezultātus visās sadarbības jomās[115]. ES un NATO ir pastiprinājušas savu darbu un sadarbību pēc Krievijas agresijas kara, īstenojot vienotu politisko nostāju un koordināciju nolūkā palīdzēt Ukrainai aizsargāties un aizsargāt savus iedzīvotājus. ES un NATO stratēģiskā partnerība ir spēcīgāka un nozīmīgāka nekā jebkad agrāk šajā eiroatlantiskajai drošībai kritiskajā brīdī. Attiecībā uz noturību 2022. gada janvārī tika uzsākts īpašs strukturēts dialogs, kas tagad tiek padziļināts, lai atbalstītu kritiskās infrastruktūras aizsardzību, un šajā kontekstā tiks izveidota ES un NATO darba grupa. Militārās mobilitātes jomā ir veikti turpmāki uzlabojumi attiecībā uz transporta un regulatīvajiem aspektiem, tai skaitā bīstamo kravu pārvadājumiem. Viena no galvenajām sadarbības jomām ar NATO joprojām ir arī hibrīddraudu novēršana. Notiek informācijas apmaiņa par terorisma apkarošanu, kā arī stratēģiskās komunikācijas, ārvalstu īstenotas informācijas manipulācijas un iejaukšanās un kiberjautājumu jomā. Mācības ietvēra ES integrēto risinājumu 2022. gada novembrī paralēlo un koordinēto mācību (*PACE*)

[112] (ES) 2019/452.

[113] (ES) 2021/821, pārstrādāta redakcija.

[114] Eiropas Datu aizsardzības uzraudzītājs (EDAU) atzinīgi novērtēja nolīgumu kā paraugu turpmākiem nolīgumiem par persondatu apmaiņu tiesībaizsardzības nolūkos.

[115] Sk. Septīto progresa ziņojumu par ES un NATO Padomes 2016. gada 6. decembrī un 2017. gada 5. decembrī apstiprināto priekšlikumu kopuma īstenošanu, 2022. gada 20. jūnijs.

koncepcijas ietvaros, iesaistot NATO personālu mijiedarbības uzlabošanai starp attiecīgajiem krīzes reaģēšanas mehānismiem.

Kopš 2022. gada septembra ES ir **Globālā terorisma apkarošanas foruma** līdzpriekšsēdētāja. Prioritātes ietver terorisma draudu novēršanu Āfrikā un dzimuma un izglītības aspektu integrēšanu terorisma apkarošanas politikā.

Turpinās sarunas par sadarbības nolīgumu starp Savienību un **Interpolu** nolūkā 2023. gada pirmajā pusē panākt vienošanos tehniskā līmenī. Galvenais mērķis ir vēl vairāk pastiprināt informācijas apmaiņu starp Interpolu un ES aģentūrām un struktūrām, tādējādi nodrošinot labāku atbalstu dalībvalstīm un palielinot iedzīvotāju drošību ne tikai ES, bet arī visā pasaulē.

Svarīgākais izpildes piemērs

Operācija *"Desert Light"*: Eiropas narkotiku karteļa likvidēšana sešās valstīs: 2022. gada novembrī visā Eiropā un Apvienotajos Arābu Emirātos (AAE) tika veikti koordinēti reidi, ka bija vērsti gan pret vadības un kontroles centru, gan narkotiku tirdzniecības loģistikas infrastruktūru Eiropā. Augstvērtīgi mērķi bija izveidojuši "superkarteli", kas kontrolēja aptuveni vienu trešdaļu kokaīna tirdzniecības Eiropā. Pēc izmeklēšanas Spānijā, Francijā, Beļģijā, Nīderlandē un AAE ar Eiropola atbalstu tika arestēti 49 aizdomās turētie. Izmeklēšanas gaitā tiesībaizsardzības iestādes konfiscēja 30 tonnas narkotiku.

6. SECINĀJUMS

Pēdējo divarpus gadu laikā Komisija ciešā sadarbībā ar Eiropas Ārējās darbības dienestu ir veiksmīgi īstenojusi gandrīz visus Drošības savienības stratēģijā noteiktos pasākumus. Ir jāpieņem un galvenokārt jāīsteno plašs priekšlikumu klāsts. Eiropas Parlamenta, Padomes un atsevišķu dalībvalstu lēmumi un rīcība būs ļoti svarīga, lai nodrošinātu, ka ES saviem iedzīvotājiem nodrošina stabilu drošības ekosistēmu.

Tajā pašā laikā drošības vide ap mums turpinās mainīties. Kopš Drošības savienības stratēģijas pieņemšanas ES ir saskārusies ar Covid-19 pandēmiju un Krievijas agresijas pret Ukrainu ietekmi. Ir strauji izplatījušies apdraudējumi tiešsaistē, un ir nepieciešama ātra pielāgošanās un tālredzība. ES ir jāturpina sevi sagatavot, lai tiktu galā ar jebkādiem jauniem apdraudējumiem, kas skar tās iedzīvotāju drošību. Pastāvīga modrība, apņēmība rīkoties un kolektīva reakcija būs ES kolektīvo panākumu atslēga.