Eiropas Savienības
Padome

Briselē, 2023. gada 18. oktobrī
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2023. gada 18. oktobris
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretāre *Thérèse BLANCHET*
K-jas dok. Nr.:	COM(2023) 665 final
Temats:	KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI par Sesto progresa ziņojumu par ES Drošības savienības stratēģijas īstenošanu

Pielikumā ir pievienots dokuments COM(2023) 665 *final*.

Pielikumā: COM(2023) 665 *final*

EIROPAS
KOMISIJA

Briselē, 18.10.2023.
COM(2023) 665 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

par Sesto progresa ziņojumu par ES Drošības savienības stratēģijas īstenošanu

I. Ievads

Pirms trim gadiem Komisija pieņēma Drošības savienības stratēģiju 2020.–2025. gadam[1], nosakot Savienības galvenās prioritātes drošības jomā. Kopš tā laika esam guvuši lielus panākumus visu četru stratēģijas pīlāru īstenošanā, pieņemot būtiskus tiesību aktus visās jomās, sākot ar kritisko vienību aizsardzību un beidzot ar kibernoturības stiprināšanu. Taču tikmēr drošības apdraudējuma aina Eiropā un mūsu kaimiņvalstīs turpina mainīties. Nesenie teroristu uzbrukumi skolā Francijā un Briseles ielās jo skaudri atgādināja par nepieciešamību steidzami veikt turpmākus pielāgojumus mūsu drošības arhitektūrā un stiprināt to. Aizvien bīstamāki kļūst kiberuzbrukumi, jo tos veic arī ļaunprātīgas personas, kas atbalsta kādu no konfliktos iesaistītajām pusēm. Turpina vērsties plašumā hibrīddraudi, arī dezinformācija. Eiropols ir secinājis, ka pret mērķiem Eiropas Savienībā vērsto kiberuzbrukumu ievērojamā pieauguma cēlonis ir Krievijas agresijas karš pret Ukrainu, jo vērienīgos uzbrukumus politisku motīvu dēļ koordinē hakeru grupas, kas atbalsta Krieviju[2]. Šādu uzbrukumu rezultātā ir tikusi bloķēta piekļuve internetam un radīti pārrāvumi pamatpakalpojumu nodrošināšanā, piemēram, energotīklu darbībā[3].

Drošības savienības stratēģiju izstrādāja, lai ES varētu sekmīgāk tikt galā ar jauniem apdraudējumiem. Notikumu gaita kara un pandēmijas izraisīto krīžu pārvarēšanā apliecināja, cik nozīmīga ir stratēģijā noteiktā pieeja, proti, pamanīt sakarības starp atsevišķiem notikumiem ES drošības ekosistēmā un rūpēties par drošību kopumā, nenošķirot kibertelpu no fiziskās drošības, tajā skaitā organizētās noziedzības un terorisma, kā arī radikalizācijas apkarošanā.

Tomēr mums ir jāsaglabā modrība un nepārtraukti jāturpina pilnveidot centieni garantēt iedzīvotāju drošību. Stratēģija nosaka prioritārās jomas, kurās Savienība spēj sniegt pievienoto vērtību, atbalstot dalībvalstu darbības visu Eiropas iedzīvotāju drošības veicināšanā. Kopš stratēģijas pieņemšanas ir sākusies visu tajā paredzēto pasākumu īstenošana, un tā ir papildināta ar jauniem pasākumiem, reaģējot uz aktuāliem drošības apdraudējumiem.

Īstenojot Drošības savienības stratēģiju, Komisija ir iesniegusi pavisam 36 likumdošanas iniciatīvas. Pēc minēto priekšlikumu apspriešanas iestādēs vairāk nekā puse no tiem jau ir pārtapusi par pārdomātiem tiesību aktiem, kā aprakstīts pielikumā iekļautajā tabulā. Taču vairāku būtisku Komisijas ierosinātu iniciatīvu apspriešana Eiropas Parlamentā un Padomē vēl turpinās. Tā kā pašreizējā Parlamenta sasaukuma pilnvaru termiņš beigsies līdz ar Eiropas parlamenta vēlēšanām 2024. gada jūnijā, ir jārīkojas ātri, lai pabeigtu iesāktos darbus un pilnā mērā nodrošinātu iedzīvotājiem ieguvumus, ko sniegs drošības savienība. Tāpēc šajā sestajā progresa ziņojumā par drošības savienību ir aplūkoti galvenokārt tie Komisijas pieņemtie leģislatīvie un neleģislatīvie dokumenti, kuri ir būtiski drošības savienībai, bet kuru sagatavošanā vēl ir jāiegulda daudz darba, lai tos pabeigtu un varētu sākt faktiski īstenot.

---

1 COM(2020) 605.

2 Izkliedētās pakalpojumatteices (*DDoS*) uzbrukumi — sk. Eiropola īpašo ziņojumu "*Cyber-attacks: the apex of crime-as-a-service*", 2023. gada 13. septembris.

3 Ļaunprogrammatūras ar dzēšanas funkciju tika plaši izmantotas konfliktā Ukrainā, lai iznīcinātu datus un kaitētu sistēmu darbībai, piemēram, tūkstošiem abonentu ES tika traucēta piekļuve internetam un liels Vācijas energouzņēmums zaudēja piekļuvi 5800 vējturbīnu attālinātai uzraudzībai. "*The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*", Eiropas Parlamenta pētījums, 2023. gada septembris, PE 702.594.

Jau saskaņotie ES tiesību akti sniegs jūtamus ieguvumus vienīgi pēc to ieviešanas praksē. Tāpēc jāpievērš uzmanība to pilnīgai un pareizai transponēšanai, īstenošanai un piemērošanai dalībvalstīs. Komisija 2023. gadā turpināja nodrošināt ES Drošības savienības stratēģijas izpildi, izmantojot savas institucionālās pilnvaras sākt pārkāpuma procedūras katrreiz, kad dalībvalstis nav transponējušas ES tiesību aktus vai ir transponējušas tos nepareizi.

Šajā ziņojumā ir apkopotas arī jomas, kurās dalībvalstu un/vai ES darbības ir būtiskas stratēģijas izpildei. ES aģentūrām ir izšķiroša nozīme drošības savienības iniciatīvu īstenošanā, un pēdējo gadu laikā to pienākumi ir paplašinājušies. Ziņojumā ir izklāstīti daži no jaunajiem uzdevumiem, kas tām ir uzticēti, lai uzlabotu atbalstu dalībvalstīm drošības savienības svarīgāko iniciatīvu īstenošanā.

Turklāt ģeopolitiskā situācija skaidri apliecina, ka ārējā drošība ir nozīmīga mūsu iekšējai drošībai. Uzlabots ES iekšējais satvars drošības jomā ir nesaraujami saistīts ar ciešāku partnerību un sadarbību ar trešām valstīm. ES ir jāturpina aktīvi meklēt veidus, kā tās iesaiste starptautiskajās norisēs varētu sekmēt iedzīvotāju drošību Eiropas Savienībā.

II. Nākotnes prasībām atbilstoša drošības vide

Kiberdrošība un kritiskās infrastruktūras noturība

Saistībā ar Drošības savienību Savienība ir apņēmusies gādāt par to, lai visi Eiropas iedzīvotāji un uzņēmumi būtu labi aizsargāti gan tiešsaistē, gan bezsaistē, un veicināt atvērtu, drošu un stabilu kibertelpu. Kiberdrošības incidentu pieaugošais apmērs, biežums un ietekme būtiski apdraud tīklu un informācijas sistēmu darbību un iekšējo tirgu. Krievijas agresijas karš pret Ukrainu ir vēl vairāk palielinājis šo apdraudējumu, un saspīlēto ģeopolitisko situāciju saasina uzbrukumi, ko īsteno dažādi noziedzīgi subjekti un haktīvisti, kuri atbalsta valsts nostāju. *Nord Stream* cauruļvadu sabotāža pagājušā gada rudenī parādīja, cik ļoti tādas būtiskas nozares kā enerģētika, digitālā infrastruktūra, transports un kosmoss ir atkarīgi no noturīgas kritiskās infrastruktūras. Jaunākais incidents saistībā ar zemūdens gāzes cauruļvada un datu pārraides kabeļa bojājumiem Igaunijā un Somijā apliecina nepieciešamību pēc augsta līmeņa gatavības šādām situācijām. Lai gan bojājumu cēlonis nav noskaidrots un izmeklēšana turpinās, informācijas apmaiņa starp dalībvalstīm un Komisiju dažādos līmeņos vieš paļāvību. Minētie pārrāvumi neradīja tiešu ietekmi ne uz interneta pieejamību, ne uz gāzes piegādes drošību ne Eiropas, ne vietējā līmenī. Tas liecina par gūto progresu un pastiprinātiem centieniem gatavības uzlabošanai pēdējos mēnešos.

Tāpēc skaidrs un pārdomāts tiesiskais regulējums ir būtisks šādas kritiskās infrastruktūras aizsardzībai un noturībai. Šajā sakarā izšķirošs panākums bija divu direktīvu vienlaicīga pieņemšana — gan pārskatītā Direktīva par pasākumiem nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā ("TID 2 direktīva")[4], gan Direktīva par kritisko vienību noturību ("KVN direktīva")[5] stājās spēkā 2023. gada 16. janvārī. Tagad dalībvalstis tiek aicinātas ātri un pilnībā transponēt šos būtiskos tiesību aktus ne vēlāk kā līdz 2024. gada

[4] Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva).

[5] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2557 (2022. gada 14. decembris) par kritisko vienību noturību un Padomes Direktīvas 2008/114/EK atcelšanu.

17. oktobrim, lai ieviestu stingru Savienības satvaru kritiskās infrastruktūras aizsardzībai pret fiziskiem apdraudējumiem un kiberdraudiem.

Komisija 2023. gada jūlijā Komisijas Deleģētajā regulā[6] noteica pamatpakalpojumus 11 nozarēs, uz kurām attiecas KVN direktīva. Nākamajā posmā dalībvalstīm ir jāveic šo pakalpojumu riska novērtējums. Pēc Padomes 2022. gada 8. decembra ieteikuma[7] pieņemšanas darbs kritiskās infrastruktūras stresa testu veikšanā, sākot ar enerģētikas nozari, un sadarbības stiprināšanā ar NATO un galvenajām partnervalstīm noritēja aktīvāk. Šā darba rezultātā ES un NATO darba grupa kritiskās infrastruktūras noturības jautājumos 2023. gada jūnijā sagatavoja ziņojumu, kurā aprakstīja kritiskās infrastruktūras aktuālos drošības apdraudējumus četrās galvenajās nozarēs (enerģētika, transports, digitālā infrastruktūra un kosmoss) un izteica ieteikumus noturības stiprināšanai. Minētos ieteikumus, tajā skaitā par koordinācijas, informācijas apmaiņas un mācību uzlabošanu, ES un NATO personāls īsteno saskaņā ar strukturēto dialogu par noturību.

Vienlaikus Komisija 2023. gada 6. septembrī pieņēma priekšlikumu[8] Padomes ieteikumam par Plānu, lai uzlabotu koordinētu Savienības līmeņa reaģēšanu uz mēģinājumiem radīt traucējumus kritiskajā infrastruktūrā ar būtisku pārrobežu nozīmi. Plāna apspriešanai 2023. gada 4. oktobrī organizēja mācības, kuru gaitā pārrunāja scenāriju, lai pārbaudītu, kā to varēs īstenot praksē, un sniedza jaunāko informāciju par sarunām Padomē par attiecīgo priekšlikumu.

Ņemot vērā Padomes izteiktos aicinājumus[9], Komisija, augstais pārstāvis un TID sadarbības grupa veic riska izvērtējumu un izstrādā riska scenārijus no kiberdrošības viedokļa. Šajā darbā sākotnēji vislielāko uzmanību pievērš telesakaru un elektroenerģētikas nozarei. Pateicoties visu attiecīgo aģentūru un tīklu (kā civilo, tā militāro) iesaistei, pirmo reizi top visaptverošs un iekļaujošs Savienības mēroga novērtējums. Tas papildinās koordinētos drošības riska novērtējumus, ko veic kritiskajām piegādes ķēdēm saskaņā ar TID 2 direktīvu, un riska novērtējumus un stresa testus, ko veic kritiskajai infrastruktūrai enerģētikas, digitālās infrastruktūras komunikāciju, transporta un kosmosa nozarēs. Koordinācijas un saskaņotības labad minētās darbības būtu jāveic, ņemot vērā jau paveikto, lai veicinātu standarta pieejas izveidi, un tām būtu jāsniedz norādes turpmāku mācību sagatavošanai. Tagad šo darbību panākumi būs atkarīgi no dalībvalstu aktīvas iesaistes.

Ekonomika un sabiedrība kļūst aizvien atkarīgākas no pakalpojumiem un datiem, kas ir saistīti ar kosmosu, jo īpaši drošības un aizsardzības jomā. Kosmoss ir nozare, kurā sāncensība kļūst aizvien sīvāka, un tā nozīme drošības jomā vēl vairāk palielinājās pēc Krievijas iebrukuma Ukrainā. Lai stiprinātu mūsu stratēģisko pozīciju un patstāvību kosmosā, 2023. gada martā pieņēma ES kosmosa drošības un aizsardzības stratēģiju. Viens no nozīmīgākajiem pasākumiem, kuri izriet no minētās stratēģijas, ir ES Kosmosa akts, ko Komisija ierosinās 2024. gadā kosmosa darbību drošības, ilgtspējas un noturības/drošības reglamentēšanai Eiropas Savienībā.

Ja aplūkojam ārējo dimensiju, globālās ekonomikas un piegādes ķēžu noturības pamatā[10] ir droša infrastruktūra, tāpēc ES stratēģijā "*Global Gateway*" liela uzmanība ir pievērsta

---

6 COM(2023) 4878.

7 Padomes ieteikums (2022. gada 8. decembris) par Savienības mēroga koordinētu pieeju kritiskās infrastruktūras noturības stiprināšanai.

8 COM(2023) 526.

9 Padomes secinājumi (2022. gada 23. maijs) par Eiropas Savienības kiberdrošības statusa uzlabošanu un Nevēras aicinājums (2022. gada 9. marts) pastiprināt ES kiberdrošības spējas.

10 JOIN(2021) 30.

drošības jautājumiem. Tā kā ES un partnervalstu infrastruktūra ir savstarpēji savienota, tikpat nozīmīga ir arī turpmāka starptautiska sadarbība ar mērķi stiprināt globālo kibernoturību un atbalstīt brīvu, atklātu, drošu un aizsargātu kibertelpu.

Kibernoturības akts

Rūpējoties par Eiropas kiberdrošību, ir svarīgi nodrošināt, ka patērētāji un uzņēmumi var paļauties uz drošiem digitāliem produktiem. Lai to panāktu, Komisija 2022. gada 15. septembrī pieņēma priekšlikumu par Kibernoturības aktu[11]. Ar minēto aktu ieviesīs obligātas horizontālās kiberdrošības prasības attiecībā uz produktiem ar digitāliem elementiem, kuras būs spēkā piecus gadus vai visā produkta aprites ciklā (atkarībā no tā, kurš termiņš ir īsāks) Tas radīs apstākļus drošu, digitālus elementus saturošu produktu projektēšanai un izstrādei, nodrošinot, ka tirgū laiž aparatūras un programmatūras produktus, kuros ir iespējami maz ievainojamību. Tas būs būtisks sasniegums Eiropas kiberdrošības standartu uzlabošanā visās jomās, un varētu kļūt par starptautisku atskaites punktu, nodrošinot Savienības kiberdrošības nozarei nepārprotamas priekšrocības pasaules tirgos. Eiropas Parlaments un Padome pieņēma savas nostājas 2023. gada jūlijā, un sarunām būtu ātri jātuvojas noslēgumam.

Kiberdrošības sertifikācija ir arī nozīmīga, lai uzlabotu uzticēšanos IKT produktiem un pakalpojumiem, jo tā ļaus patērētājiem, uzņēmumiem un iestādēm veikt apzinātu izvēli, izvēloties piemērotu kiberdrošības līmeni. Darbs kiberdrošības sertifikācijas ieviešanā norit sekmīgi, un ES kiberdrošības sertifikācijas shēmu, kuras pamatā ir vienoti kritēriji, izskata komiteju procedūrā. ES mākoņdrošības sertifikācijas kandidātshēmu (*EUCS*) pašlaik gatavo Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) un apspriež Eiropas kiberdrošības sertifikācijas grupa. Aktīvi sadarbojoties ar dažādu nozaru ekspertiem, patērētājiem un pakalpojumu sniedzējiem, būtu jāatrod piemērota juridiskā un tehniskā pieeja, kas sniegtu nepieciešamās drošības garantijas, kuras atbilstu Savienības tiesību aktiem, starptautiskajām saistībām un PTO saistībām. Turklāt *ENISA* gatavo arī ES 5G kandidātshēmu un ES digitālās identitātes maku (*EUIDW*). Lai uzlabotu IKT produktu, IKT pakalpojumu un IKT procesu drošību, ir būtiski saskaņot centienus visās dalībvalstīs.

Regulas par informācijas drošību un kiberdrošību ES iestādēs, struktūrās un aģentūrās

Abas regulas kiberdrošības un informācijas drošības reglamentēšanai Savienības iestādēs ierosināja vienlaikus 2022. gada martā, bet priekšlikumu izskatīšanas temps atšķiras. Pagājušā gada jūnijā par Kiberdrošības regulu panāca politisku vienošanos, kas ļauj stiprināt visu ES iestāžu, struktūru, biroju un aģentūru kiberdrošības statusu un atspoguļo nozīmi, kādu ES piešķir attiecīgā priekšlikuma ātrai īstenošanai. Šajā situācijā īpašas bažas rada neparedzēti lēnais progress, izskatot paralēlo priekšlikumu par informācijas drošību, kas ir būtisks, lai varētu pabeigt ES iestādēm, struktūrām un aģentūrām paredzēta pārdomāta tiesiskā regulējuma izstrādi. Abus priekšlikumus būtu jāpieņem līdz Eiropas Parlamenta vēlēšanām, lai nodrošinātu ES pārvaldes uzticamību un noturību pašreizējā ģeopolitiskajā kontekstā. Informācijas drošības noteikumu un standartu kopums, kas obligāti jāievēro visām ES iestādēm, struktūrām un aģentūrām, sniegtu visām iesaistītajām personām noteiktību un nodrošinātu vienotu aizsardzību pret jaunajiem apdraudējumiem to informācijai — gan ES klasificētai, gan neklasificētai informācijai. Abi kopā šie jaunie noteikumi radītu stabilu pamatu drošai informācijas apmaiņai starp ES iestādēm, struktūrām un aģentūrām un ar dalībvalstīm, jo informācijas plūsmas aizsargātu standartizēta prakse un pasākumi. Līdz ar to tie sniedz risinājumu, ko Padome jau vairākkārt aicināja rast ES iestāžu, struktūru un aģentūru

[11] COM(2022) 454.

noturības stiprināšanai un Savienības lēmumu pieņemšanas procesa labākai aizsardzībai pret ļaunprātīgu iejaukšanos.

Kiberdrošības solidaritātes akts

Pamatojoties uz jau ieviesto stingro stratēģisko, politisko un tiesisko regulējumu, Kiberdrošības solidaritātes akta priekšlikums[12], ko Komisija pieņēma 2023. gada 18. aprīlī, vēl vairāk uzlabos kiberdraudu atklāšanu un noturību pret tiem, kā arī gatavību kiberdraudiem visos ES kiberdrošības ekosistēmas līmeņos. Minēto mērķu sasniegšanai īstenos trīs galvenās darbības:

(1) ***Eiropas kibervairoga*** izveide, lai veidotu un uzlabotu kopīgas atklāšanas un situācijas apzināšanās spējas. Kibervairogs sastāvēs no valstu drošības operāciju centriem ("valsts DOC") un pārrobežu drošības operāciju centriem ("pārrobežu DOC").
(2) ***Kiberavārijas mehānisma*** izveide, lai palīdzētu dalībvalstīm sagatavoties ievērojamiem un plašiem kiberincidentiem, uz tiem reaģēt un pēc tiem tūdaļ atkopties. Atbalsts reaģēšanai uz incidentiem ietvers ES kiberdrošības rezervi, kas būs pieejama arī ES iestādēm, struktūrām, birojiem un aģentūrām, kā arī programmas "Digitālā Eiropa" asociētām trešām valstīm, ja to paredz ar tām noslēgtais asociācijas nolīgums par dalību programmā "Digitālā Eiropa".
(3) ***Eiropas kiberincidentu izskatīšanas mehānisma*** izveide ievērojamu vai plašu incidentu izskatīšanai un novērtēšanai. Notikumu pārskatīšanu pēc incidenta koordinēs un pārskata ziņojumu sagatavos *ENISA*.

Ir sākusies priekšlikuma apspriešana Padomē un Eiropas Parlamentā. Sarunu pabeigšana pirms pašreizējā Eiropas Parlamenta sasaukuma pilnvaru termiņa beigām ievērojami sekmēs centienus aizsargāt iedzīvotājus un uzņēmumus visā Savienībā.

Kiberdrošības prasmju akadēmija

Kiberdraudiem pieaugot, ES ir steidzami vajadzīgi speciālisti ar prasmēm un iemaņām novērst, atklāt un apturēt kiberuzbrukumus un aizsargāt ES no tiem. Saskaņā ar pašreizējām aplēsēm ES ir vajadzīgi 883 000 kiberdrošības speciālisti, taču 2022. gadā neaizpildītas bija 260 000 līdz 500 000 vakances. Visas sabiedrības grupas būtu jāmudina palīdzēt novērst šo speciālistu trūkumu, taču jāuzsver, ka 2022. gadā tikai 20 % absolventu ar specializāciju kiberdrošībā un 19 % informācijas un komunikācijas tehnoloģiju speciālistu bija sievietes. 2023. gads ir Eiropas Prasmju gads, un kiberdrošības talantu deficīta pārvarēšanai Komisija 2023. gada 18. aprīlī pieņēma iniciatīvu par Kiberdrošības prasmju akadēmijas izveidi[13], ko augstu vērtēja dalībvalstis[14]. Kiberdrošības prasmju akadēmija apvienos esošās iniciatīvas par kiberdrošības prasmēm un uzlabos koordināciju. Komisija mudina dalībvalstis, reģionālās un vietējās iestādes, kā arī Eiropas publiskās struktūras pieņemt īpašas stratēģijas vai iniciatīvas par kiberdrošības prasmēm vai iekļaut kiberdrošības prasmes attiecīgajās stratēģijās vai iniciatīvās, kas aptver plašāku jautājumu loku (piemēram, kiberdrošība, digitālās prasmes, nodarbinātība u. c.). Lai mazinātu kiberdrošības prasmju nepietiekamību un attiecīgi darbaspēka trūkumu Eiropā, ir būtiski iesaistīt arī ieinteresētās personas no privātā sektora.

Droni

[12] COM(2023) 209.
[13] COM(2023) 207.
[14] Padomes secinājumi (2023. gada 22. maijs) par ES kiberaizsardzības politiku.

Aizvien lielāku apdraudējumu sabiedriskām vietām un kritiskajai infrastruktūrai rada arī droni. Gan Savienībā, gan ārpus tās aizvien biežāk notiek incidenti, kas ir saistīti ar dronu izmantošanu, un pretdronu risinājumi ir nozīmīgs rīks, ko izmanto tiesībaizsardzības iestādes un citas publiskās iestādes Eiropā, kā arī kritiskās infrastruktūras privātie operatori. Savukārt dronu likumīga izmantošana ievērojami sekmē virzību uz divējādo zaļo un digitālo pārkārtošanos[15]. Atbilstoši paziņojumam 2022. gada novembrī pieņemtajā "Dronu stratēģijā 2.0" Komisija šodien pieņem paziņojumu par to, kā novērst dronu radītos potenciālos apdraudējumus, ko papildina divas rokasgrāmatas, kurās ir sniegti praktiski norādījumi par galvenajiem tehniskajiem aspektiem[16]. Minētās iniciatīvas mērķis ir piedāvāt visaptverošu un saskaņotu politikas satvaru, veidojot vienotu izpratni par noteikumiem, kas ir ieviesti, lai novērstu dronu radītos iespējamos apdraudējumus un vajadzības gadījumā pielāgotos tehnoloģiju straujajai attīstībai. Dalībvalstis un attiecīgos privātos operatorus aicina cieši sadarboties ar Komisiju, lai nodrošinātu iniciatīvas pilnīgu īstenošanu.

Jūras un aviācijas drošība

Jūras drošību joprojām apdraud nelikumīgas darbības, piemēram, pirātisms un bruņota laupīšana jūrā, migrantu kontrabanda un cilvēku, ieroču un narkotiku tirdzniecība, kā arī terorisms, un saasinās arī jauni apdraudējumi, tajā skaitā hibrīduzbrukumi un kiberuzbrukumi. Komisija un augstais pārstāvis 2023. gada 10. martā pieņēma kopīgu paziņojumu par ES Jūras drošības stratēģijas atjaunināšanu[17], un tagad minēto stratēģiju jāīsteno saskaņā ar atjaunoto rīcības plānu.

Aviācijas drošības jomā Komisija 2023. gada 2. februārī pieņēma dienestu darba dokumentu "Virzība uz uzlabotu un noturīgāku aviācijas drošības politiku"[18], kurš ietver vērienīgu programmu, kuras mērķi ir 1) modernizēt aviācijas drošības regulatīvo struktūru, 2) veicināt inovatīvāku risinājumu izstrādi un ieviešanu un 3) atjaunināt aviācijas drošības pamatlīmeni, lai augstākās prioritātes apdraudējumu novēršanā Savienības lidostas varētu pilnībā izmantot priekšrocības, ko sniedz jaunas un progresīvas tehnoloģijas. Četrpadsmit pamatdarbības ir jāīsteno divu gadu laikā.

Komisija aicina Eiropas Parlamentu un Padomi steidzami, vēlākais līdz pašreizējā Eiropas Parlamenta sasaukuma pilnvaru termiņa beigām, pabeigt sarunas par šādiem dokumentiem:

- Kibernoturības akta priekšlikums;
- Kibersolidaritātes akta priekšlikums;
- priekšlikums regulai par informācijas drošību ES iestādēs, struktūrās un aģentūrās.

Komisija aicina dalībvalstis:

- transponēt Kritisko vienību noturības direktīvu prioritārā kārtā, kā arī veikt kritiskās infrastruktūras stresa testus enerģētikas nozarē;
- pieņemt Padomes ieteikumu par Plānu koordinētai reaģēšanai uz traucējumiem kritiskajā infrastruktūrā ar būtisku pārrobežu nozīmi;
- pilnībā un steidzamības kārtā transponēt TID 2 direktīvu, lai ievērojami uzlabotu būtisko vienību un svarīgo vienību kiberdrošību;
- aktīvi iesaistīties kiberdrošības riska novērtējumos un riska scenāriju izstrādē

[15] COM(2022) 652.
[16] COM(2023) 659.
[17] JOIN(2023) 8.
[18] SWD(2023) 37.

attiecībā uz kritisko infrastruktūru un piegādes ķēdēm;
- veikt turpmākus pasākumus saistībā ar Kiberdrošības prasmju akadēmiju, aktīvi piedaloties ES līmeņa darbībās un pieņemot īpašas valsts stratēģijas vai iniciatīvas par kiberdrošības prasmēm, šajā sakarā iesaistot galvenās ieinteresētās personas, arī reģionālās un vietējās iestādes;
- sadarboties ar attiecīgajiem privātajiem operatoriem un Komisiju, lai nodrošinātu, ka tiek īstenotas visas darbības, kas ir uzskaitītas paziņojumā par dronu radīto potenciālo apdraudējumu novēršanu;
- īstenot ES Jūras drošības stratēģijas rīcības plānu un regulāri ziņot par paveikto;
- īstenot 14 norādītās pamatdarbības aviācijas drošības uzlabošanai.

III. Vēršanās pret jauniem apdraudējumiem

Jauni ģeopolitiskie saspīlējumi skaudri liecina par to, ka ES drošības apdraudējumu kļūst arvien vairāk, turklāt tie iegūst jaunas izpausmes, ko daudzos gadījumos var raksturot kā hibrīddraudus. Drošības jomā ir jāreaģē arī uz pārmaiņām sabiedrībā un tehnoloģijās. Covid-19 pandēmija pavēra plašākas iespējas kibernoziedzniekiem, un jo īpaši pieauga apdraudējumi saistībā ar tiešsaistē izvietotiem materiāliem, kas atspoguļo seksuālu vardarbību pret bērniem. Noziedznieki un ļaunprātīgas personas vienmēr ir gatavas izmantot tehnoloģiju attīstību. Tā kā šādiem apdraudējumiem bieži vien ir raksturīgs dažādu elementu un aspektu kopums, ES rīcībai ir jābūt stingrai un konsekventai.

Regula par seksuālas vardarbības pret bērniem tiešsaistē apkarošanu

Eiropola veiktais interneta organizētās noziedzības draudu novērtējums atklāja, ka bērnu seksuāla izmantošana un seksuāla vardarbība pret bērniem 2022. gadā vēl vairāk palielinājās gan biežuma, gan nodarījuma smaguma ziņā, likumpārkāpējiem turpinot izmantot tehniskās iespējas, kas ļauj tiem slēpt savas darbības un identitātes[19]. Pašreizējā sistēma, kura balstās uz to, ka uzņēmumi brīvprātīgi atklāj pārkāpumus un ziņo par tiem, nenodrošina pietiekamu bērnu aizsardzību. Pagaidu regula ļauj uzņēmumiem brīvprātīgi atklāt pārkāpumus un ziņot par tiem, ja šāda rīcība ir likumīga saskaņā ar Vispārīgo datu aizsardzības regulu (VDAR). Regula zaudēs spēku 2024. gada augustā. Komisija 2022. gada maijā ierosināja regulu[20], lai novērstu tiešsaistes pakalpojumu ļaunprātīgu izmantošanu ar nolūku veikt seksuāla vardarbību pret bērnu. Ierosinātajā regulējumā ļoti liela uzmanība ir pievērsta šādu pārkāpumu novēršanai. Uzņēmumiem būs pienākums novērtēt risku, ka to sistēmas var tikt izmantotas seksuālai vardarbībai pret bērnu, un veikt preventīvus pasākumus. Galējas nepieciešamības gadījumā un vienīgi tad, ja risks ir būtisks, valsts tiesas vai neatkarīgas pārvaldes iestādes varēs izdot pakalpojumu sniedzējiem mērķorientētus atklāšanas rīkojumus. Pakalpojumu sniedzēju centienus veicinās jauns neatkarīgs ES centrs, kas darbosies kā speciālo zināšanu centrs, kurš sniegs uzticamu informāciju par konstatētajiem materiāliem, saņems un analizēs pakalpojumu sniedzēju ziņojumus par seksuālu vardarbību pret bērniem, kā arī sniegs atbalstu cietušajiem. Ir būtiski pieņemt un ieviest jaunos noteikumus iespējami ātrāk, lai pasargātu bērnus no turpmākas vardarbības, nepieļautu materiālu atkārtotu ievietošanu tiešsaistē un sauktu likumpārkāpējus pie atbildības. Padomē un Parlamentā notiek

[19] Eiropols (2023), Interneta organizētās noziedzības draudu novērtējums (*IOCTA*) 2023. gadā.
[20] COM(2022) 209.

sarunas, un ir iecerēts panākt vienošanos par dokumentu līdz pašreizējā Parlamenta sasaukuma pilnvaru termiņa beigām.

Direktīva par vardarbības pret sievietēm un vardarbības ģimenē apkarošanu

Kibervardarbība pret sievietēm, arī saistībā ar vardarbību ģimenē, ir kļuvusi par jaunu šādas vardarbības veidu, kas ar interneta un IT rīku starpniecību izplatās pāri atsevišķu dalībvalstu robežām. Komisija 2022. gada martā ierosināja direktīvu par vardarbības pret sievietēm un vardarbības ģimenē apkarošanu, kura ietver konkrētus noteikumus par kibervardarbību un pasākumus nepilnību novēršanai aizsardzības, tiesu pieejamības un prevencijas jomās. Ja minēto direktīvu pieņems un sāks īstenot ātri, dalībvalstis iegūs vēl vienu instrumentu šāda veida noziedzīgu nodarījumu apkarošanai. Likumdevējiestādes sāka sarunas 2023. jūlijā ar mērķi pabeigt tās līdz pašreizējā Eiropas Parlamenta sasaukuma pilnvaru termiņa beigām.

5G kiberdrošība

5G tīklu drošība ir viena no galvenajām Komisijas prioritātēm un arī Drošības savienības stratēģijas būtiska sastāvdaļa. 5G tīkli ir būtiska infrastruktūra, kas kalpo par pamatu dažādu, iekšējā tirgus darbībai un nozīmīgām sabiedriskām un ekonomiskām funkcijām būtisku pakalpojumu sniegšanai. TID sadarbības grupā pārstāvētās dalībvalstu iestādes ar Komisijas un *ENISA* atbalstu 2023. gada 15. jūnijā publicēja otro progresa ziņojumu par ES 5G kiberdrošības rīkkopas īstenošanu. Ziņojumā ir norādīts, ka 24 dalībvalstis ir pieņēmušas vai gatavo leģislatīvus pasākumus, kas piešķir valsts iestādēm pilnvaras veikt piegādātāju novērtējumu un noteikt ierobežojumus, un 10 dalībvalstis ir ieviesušas šādus ierobežojumus. Tomēr ir jāveic turpmāki pasākumi, lai Savienībā kopumā novērstu ievainojamības, kas var nopietni negatīvi ietekmēt atsevišķu lietotāju un uzņēmumu drošību visā Savienībā, kā arī Savienības kritiskās infrastruktūras drošību. Visām dalībvalstīm bez kavēšanās ir jāīsteno minētā rīkkopa. Tajā pašā dienā Komisija pieņēma paziņojumu par rīkkopas īstenošanu dalībvalstīs, kā arī par Komisijas korporatīvo komunikāciju un Savienības nodrošināto finansējumu. Paziņojumā Komisija pauda lielas bažas par riskiem, ko ES drošībai rada mobilo sakaru tīkla iekārtu piegādātāji *Huawei* un *ZTE*. Šajā sakarā Komisija veic pasākumus, lai novērstu situāciju, ka korporatīvā komunikācija notiek mobilajos tīklos, kuru iekārtas piegādājuši *Huawei* un *ZTE*. Nebūs atļauts iepirkt jaunus savienojamības pakalpojumus, kuru nodrošināšanai izmanto minēto piegādātāju iekārtas, un Komisija sadarbosies ar dalībvalstīm un telesakaru operatoriem, lai panāktu minēto piegādātāju pakāpenisku izslēgšanu no pastāvošajiem Komisijas vietņu savienojamības pakalpojumiem. Komisija arī apsver, kā šo lēmumu atspoguļot attiecīgajās ES finansēšanas programmās un instrumentos, pilnībā ievērojot Savienības tiesību aktus.

Piekļuve datiem efektīvai tiesībaizsardzībai

Pašreizējā digitālajā laikmetā gandrīz ikvienam noziedzīgam nodarījumam ir kāds digitāls aspekts. Noziedzīgos nolūkos izmanto arī tehnoloģijas un rīkus, tajā skaitā arī tādus, kas ir nepieciešami, lai apmierinātu mūsu sabiedrības vajadzības pēc kiberdrošības, datu aizsardzības un privātuma. Tas aizvien vairāk apgrūtina tādu turpmāku efektīvu tiesībaizsardzību visā ES, kas garantē sabiedrības drošību un novērš, atklāj un izmeklē noziedzīgus nodarījumus un veic kriminālvajāšanu par tiem. Neskatoties uz nozīmīgām pūlēm Savienības un valstu līmenī, tajā skaitā izmantojot gan tiesību aktus, gan spēju veidošanas un inovācijas iniciatīvas, joprojām pastāv juridiski un tehniski sarežģījumi. Komisija, iesaistot Padomes prezidentūru, ir izveidojusi augsta līmeņa grupu par piekļuvi datiem efektīvai tiesībaizsardzībai, lai nodrošinātu platformu sadarbībai ar plašu loku ieinteresēto personu un ekspertu ar mērķi risināt problēmas, ar kurām sakaras tiesībaizsardzības praktiķi (piemēram, šifrēšana, datu saglabāšana, 5G un standartizācija). Komisija sagaida, ka augsta līmeņa grupa

līdz 2024. gada jūnijam noformulēs līdzsvarotus, lietderīgus un īstenojamus ieteikumus, kuri atspoguļos šo problēmu sarežģītību, tajā skaitā no kiberdrošības un datu aizsardzības viedokļa. Tāpēc dalībvalstis un iesaistītie eksperti tiek mudināti aktīvi piedalīties šajā procesā un izstrādāt lietderīgus, likumīgus un vispārpieņemamus risinājumus.

Hibrīddraudi

Ģeopolitiskajā situācijā, ko raksturo aizvien sarežģītāki un specializētāki hibrīddraudi, ES Stratēģiskais kompass drošībai un aizsardzībai[21] ("Stratēģiskais kompass") sniedza kopīgu novērtējumu par apdraudējumiem un problēmām, ar ko saskaras ES, kā arī stratēģisko rīcības plānu. To, ka kibertelpa ietilpst ārlietu un drošības politikas jomā, uzskatāmi apliecina valstu un nevalstisko dalībnieku veiktu ļaunprātīgu kiberdarbību pieaugums, tajā skaitā arī saistībā ar karu pret Ukrainu. Iespējamo ļaunprātīgas rīcības un dezinformācijas risku dēļ jābūt īpaši modriem vēlēšanu laikā, tajā skaitā arī laikposmā līdz Eiropas Parlamenta vēlēšanām 2024. gadā.

Tā kā plašākas ietekmes iespējamības risks ir augsts, ES turpināja izstrādāt pasākumus kiberdrošības spēju veidošanai un stiprināt partnerību ar trešām valstīm, tajā skaitā organizējot īpašus dialogus par kiberdrošību, lai aktīvi veicinātu ES kopējās noturības uzlabošanu. Nolūkā stiprināt Savienības spēju efektīvi risināt hibrīddraudus izstrādāja, pārskatīja un uzlaboja virkni rīku, kā tas ir aprakstīts 2023. gada 14. septembrī publicētajā septītajā progresa ziņojumā par hibrīddraudu apkarošanu[22]. To vidū ir šādi rīki:

- ES hibrīddraudu novēršanas rīkkopa, lai nodrošinātu satvaru koordinētai un pārdomātai reaģēšanai uz hibrīddraudiem un hibrīdkampaņām;
- notiek darbs ar mērķi izveidot ES hibrīddraudu novēršanas ātrās reaģēšanas vienības, kas spētu ātri sniegt dalībvalstīm, partnervalstīm un kopējās drošības un aizsardzības politikas (KDAP) misijām un operācijām konkrētajai situācijai pielāgotu atbalstu;
- pārskatītais ES protokols hibrīddraudu apkarošanai ("*EU Playbook*")[23], kurā ir aprakstīti Savienības procesi un struktūras, kas ir atbildīgas par hibrīddraudu un hibrīdkampaņu apkarošanu;
- satvars vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām[24] ("kiberdiplomātijas rīkkopa"), kas ļauj izstrādāt ilgstošas, īpaši pielāgotas, saskaņotas un koordinētas stratēģijas, lai vērstos pret personām, kuras rada pastāvīgus kiberdraudus;
- rīkkopa pret ārvalstu īstenotu informācijas manipulāciju un iejaukšanos ("*FIMI*"), lai stiprinātu esošos Savienības rīkus *FIMI* novēršanai un atturēšanai, un reaģēšanai uz *FIMI*;
- ES kiberaizsardzības politika[25], lai uzlabotu ES kiberaizsardzības spējas un situācijas apzināšanos un koordinētu visu pieejamo aizsardzības pasākumu klāstu nolūkā stiprināt noturību, reaģēt uz kiberuzbrukumiem un nodrošināt solidaritāti un savstarpēju palīdzību.

Tāpēc mudinām dalībvalstis turpināt un pastiprināt sadarbību šajā jomā, nodrošinot minēto rīkkopu faktisku īstenošanu, tajā skaitā rīkojot regulāras mācības, un vienojoties par hibrīddraudu novēršanas ātrās reaģēšanas vienības koncepciju, kas sniegs norādes par turpmākajiem pasākumiem šādu vienību izveidošanai.

---

[21] Padomes dokuments 7371/22.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23 (2023. gada 8. jūnijs).
[25] JOIN(2022) 49.

MI saistībā ar tiesībaizsardzību

Mākslīgais intelekts ("MI") ir strauji kļuvis par pavisam ikdienišķu parādību. MI izmantošanas ietekme uz kibernoziedzību un kiberdrošību vēl nav pilnībā noskaidrota, taču nav šaubu, ka tas radīs jaunas problēmas. MI var būt noderīgs, ja to izmanto drošā un kontrolētā veidā, taču ļaunprātīgu personu rokās tas var būt bīstams, jo var, piemēram, palīdzēt noziedzniekiem slēpt savu identitāti, pastrādājot tādus noziedzīgus nodarījumus kā terorisms un seksuāla vardarbība pret bērnu. Tāpēc ir būtiski, lai iestādes sekotu jaunākajām norisēm šajā jomā un varētu novērst ļaunprātīgu izmantošanu un reaģēt uz nepareizu izmantošanu[26]. Šos jautājumus risina sarunās par Mākslīgā intelekta akta priekšlikumu, kurās tagad ir sācies izšķirošais posms, kad likumdevējiestādes apspriež tehniskus un politiskus aspektus, kuri noteiks mijiedarbību ar šo tehnoloģiju turpmākajos gados. Būs būtiski atrast līdzsvarotus risinājumus, jo īpaši attiecībā uz augsta riska lietojumiem, tajā skaitā tiesībaizsardzības jomā.

Komisija aicina Eiropas Parlamentu un Padomi steidzami, vēlākais līdz pašreizējā Eiropas Parlamenta sasaukuma pilnvaru termiņā beigām, pabeigt iestāžu sarunas par šādiem dokumentiem:

- priekšlikums regulai par seksuālas vardarbības pret bērniem tiešsaistē apkarošanu;
- priekšlikums direktīvai par vardarbības pret sievietēm un vardarbības ģimenē apkarošanu;
- priekšlikums regulai, kas nosaka saskaņotas normas mākslīgā intelekta jomā ("MI akts").

Komisija aicina dalībvalstis:

- bez kavēšanās panākt ES rīkkopas 5G drošībai pilnīgu īstenošanu;
- atbalstīt darbu, ko veic augsta līmeņa grupa par piekļuvi datiem efektīvai tiesībaizsardzībai, nolūkā formulēt skaidrus, lietderīgus un īstenojamus ieteikumus, kā samērīgā veidā risināt esošās un gaidāmās problēmas;
- sadarbībā ar augsto pārstāvi veikt pasākumus, lai nodrošinātu ES hibrīddraudu novēršanas rīkkopas, pārskatītās kiberdiplomātijas rīkkopas un *FIMI* rīkkopas faktisku īstenošanu, tajā skaitā organizējot regulāras mācības un ņemot vērā notikumu attīstību pasaulē;
- panākt vienošanos par hibrīddraudu novēršanas ātrās reaģēšanas vienību koncepciju.

IV. Eiropas iedzīvotāju aizsardzība pret terorismu un organizēto noziedzību

Joprojām pastāv risks, ka pasaules vai vietēja mēroga notikumi izraisīs jaunus terorisma uzliesmojumus. Starp nopietnākajiem draudiem ES drošībai ir arī organizētā noziedzība un narkotiku tirdzniecība. Nolūkā pastiprināt Savienības kopīgos centienus apkarot šos apdraudējumus norit kopīgs darbs, lai īstenotu ES Organizētās noziedzības novēršanas

[26] Sk., piemēram, 2023. gada 17. aprīlī publicēto Eiropola ziņojumu "*ChatGPT — the impact of Large Language Models on Law Enforcement*".

stratēģiju[27], ES Stratēģiju cilvēku tirdzniecības apkarošanai[28], ES Narkomānijas apkarošanas programmu un rīcības plānu[29] un ES Terorisma apkarošanas programmu[30]. Tomēr, lai reaģētu uz situācijas satraucošo pasliktināšanos attiecībā uz organizēto noziedzību un narkotiku tirdzniecību, dalībvalstīm un ES jārīkojas vēl aktīvāk, lai stiprinātu sadarbību noziedzīgu tīklu darbības apkarošanā un uzlabotu noziegumā cietušo aizsardzību. Šajā nolūkā vienlaikus ar šo ziņojumu publicē ES ceļvedi narkotiku tirdzniecības un organizētās noziedzības apkarošanai[31].

Terorisma apkarošanas jomā ES stiprina arī savu ārējo rīkkopu[32], pilnībā izmantojot iespējas, ko sniedz augsta līmeņa dialogi par terorisma apkarošanu un terorisma apkarošanas/drošības ekspertu tīkls ES delegācijās, kā arī piedaloties daudzpusējos forumos, tajā skaitā Globālā terorisma apkarošanas foruma (*GCTF*) līdzpriekšsēdētāja amatā.

Narkotisko vielu nelikumīga tirdzniecība

ES Narkotiku aģentūras jaunajām pilnvarām stājoties spēkā 2024. gada jūlijā, uzlabosies ES spējas risināt sarežģītu drošības un veselības problēmu, kas skar miljoniem cilvēku ES un pasaulē. Komisija arī pārskata[33] regulas par narkotisko vielu prekursoriem[34], lai risinātu galvenās problēmas, ko tā norādīja 2020. gada novērtējumā[35], kurā uzsvēra nepieciešamību pievērsties problēmām, ko rada jaunradīti prekursori[36], lai mazinātu nelikumīgu narkotisko vielu piedāvājumu.

Tomēr, ņemot vērā nelikumīgu narkotisko vielu pieejamības vēl nepieredzēto pieaugumu, nelikumīgu narkotisko vielu tirdzniecība ir jāapkaro aktīvāk, sadarbojoties ar starptautiskajiem partneriem. Lai likvidētu noziedzīgos tīklus un uzlabotu noziegumā cietušo aizsardzību, dalībvalstīm un ES ir jāveic papildu pasākumi. Komisija šodien nāk klajā ar ES ceļvedi narkotiku tirdzniecības un organizētās noziedzības apkarošanai. Tas paredz 17 darbības četrās prioritārajās jomās, t. i., loģistikas centru noturības stiprināšana, izveidojot Eiropas Ostu apvienību, noziedzīgo tīklu likvidēšana, preventīvo pasākumu aktīvāka īstenošana un sadarbības stiprināšana ar starptautiskajiem partneriem. Minētās darbības jāīsteno 2024. un 2025. gadā.

Šaujamieroči

Šaujamieroču nelikumīga tirdzniecība veicina organizēto noziedzību ES un tās kaimiņvalstīs. Saskaņā ar aplēsēm Eiropas Savienībā civiliedzīvotāju rīcībā ir 35 miljoni nelikumīgu šaujamieroču, un apmēram 630 000 šaujamieroču ir reģistrēti Šengenas Informācijas sistēmā kā nozagti vai pazaudēti. Paku piegādei kļūstot ātrākai un attīstoties jaunām tehnoloģijām, piemēram, 3D drukāšanai, šaujamieroču nelikumīga tirdzniecība atrod jaunus veidus, kā

[27] COM(2021) 170.
[28] COM(2021) 171.
[29] COM(2020) 606.
[30] COM(2020) 795.
[31] COM(2023) 641.
[32] Atbilstoši aicinājumiem, ko izteica Stratēģiskajā kompasā un 2022. gada jūnijā pieņemtajos Padomes secinājumos par to, kā pievērsties teroristu un vardarbīgu ekstrēmistu radītā pastāvīgi mainīgā apdraudējuma ārējai dimensijai, kuros uzsvēra ārējo dimensiju.
[33] Narkotisko vielu prekursori — ES tiesību akti (pārskatīti noteikumi) (europa.eu).
[34] Regula (EK) Nr. 273/2004 par narkotisko vielu prekursoriem un Padomes Regula (EK) Nr. 111/2005, ar ko paredz noteikumus par uzraudzību attiecībā uz narkotisko vielu prekursoru tirdzniecību starp Kopienu un trešām valstīm.
[35] COM(2020) 768.
[36] 23. darbība rīcības plānā narkomānijas apkarošanai, COM(2020) 606.

izvairīties no kontroles pasākumiem. Šaujamieroču izplatīšanas risku ir palielinājis arī Krievijas agresijas karš pret Ukrainu. Komisija 2022. gada oktobrī pieņēma priekšlikumu, kas paredz atjaunināt esošos tiesību aktus, kuri attiecas uz civilām vajadzībām paredzētu šaujamieroču importu, eksportu un tranzītu, lai novērstu nepilnības esošajos noteikumos, kuru dēļ Eiropas Savienībā varētu nelikumīgi ievest vai novirzīt uz to lielāku skaitu šaujamieroču[37]. Vidējā termiņā šie jaunie noteikumi palīdzēs samazināt risku, ka varētu tikt apieti embargo attiecībā uz civilām vajadzībām paredzētu šaujamieroču eksportu, un palielināt kontroli attiecībā uz šāda veida šaujamieroču importu no trešām valstīm. Abām likumdevējiestādēm vēl ir jāpieņem nostāja par šo dokumentu, lai panāktu vienošanos par to līdz pašreizējā Parlamenta sasaukuma pilnvaru termiņa beigām.

Cilvēku tirdzniecība

Cilvēku tirdzniecība kā organizētās noziedzības paveids ir īpaši smags noziegums un ļoti nopietns cilvēktiesību pārkāpums. ES robežās cietušos pārvieto galvenokārt seksuālās ekspluatācijas un darbaspēka ekspluatācijas nolūkos, bet ir arī gadījumi, kad tos spiež ubagot un izdarīt noziegumus vai izmanto citā veidā. Komisija 2022. gada decembrī ierosināja grozīt Cilvēku tirdzniecības apkarošanas direktīvu[38], atjauninot noteikumus, lai novērstu nepilnības esošajā tiesiskajā regulējumā. Konkrētāk, pārskatītā direktīva, ja to pieņems, papildinās esošās direktīvas darbības jomu, iekļaujot tajā arī piespiedu laulības un nelikumīgu adopciju, kā arī ieviesīs nepārprotamu atsauci uz cilvēku tirdzniecības tiešsaistes dimensiju. Tā paredzēs arī obligātu sankciju režīmu, ko piemēro vainīgajiem, un formāli izveidos valsts mehānismus cietušo nosūtīšanai uz atbalsta dienestiem, lai uzlabotu cietušo agrīnu identificēšanu un pārrobežu nosūtīšanu palīdzības un atbalsta saņemšanai. Tādu pakalpojumu izmantošana, ko piespiedu kārtā sniedz cilvēku tirdzniecības upuri, tiks atzīta par noziedzīgu nodarījumu, un ikgadējo datu vākšanu par cilvēku tirdzniecību noteiks par obligātu, un šādi iegūtos datus publicēs *Eurostat*. Padome pieņēma vispārēju pieeju 2023. gada jūnijā, bet Eiropas Parlamentam sava nostāja vēl ir jāpieņem. Būs jārīkojas ātri, lai panāktu vienošanos līdz pašreizējā Parlamenta sasaukuma pilnvaru termiņa beigām.

Noziegumi pret vidi

Noziegumi pret vidi ir kļuvuši par globālu apdraudējumu, un saskaņā ar aplēsēm šādu noziegumu skaits katru gadu palielinās par 5–7 %. Organizēto noziedzību piesaista gan iespēja gūt lielu peļņu, gan nepilnības dalībvalstu tiesību aktos, gan zemais risks, ka pārkāpums tiks atklāts. Eiropols ir konstatējis pazīmes, kas liecina, ka šādu pārkāpumu rezultātā gūtos ieņēmumus izmanto terorisma finansēšanai. Komisija 2021. gada decembrī pieņēma priekšlikumu, kas paredz aizstāt 2008. gada Direktīvu par vides kriminmāltiesisko aizsardzību. Priekšlikuma galvenais nolūks ir precizēt un atjaunināt definīcijas, kas apraksta noziegumu pret vidi kategorijas, un noteikt iedarbīgus, atturošus un samērīgus sankciju veidus un apmērus, ko piemēro fiziskām un juridiskām personām. Starp jaunajiem nodarījumiem, ko paredzēts atzīt par noziedzīgiem, ir nelikumīga atmežošana, darbības, kas pārkāpj ES tiesību aktus par ķimikālijām, nelikumīga virszemes ūdeņu vai gruntsūdeņu ieguve un nelikumīga kuģu pārstrāde. Priekšlikuma mērķis ir būtiski uzlabot tiesībaizsardzības ķēdi un pārrobežu sadarbību starp dalībvalstu iestādēm un ES aģentūrām un struktūrām. Gan Eiropas Parlaments, gan Padome ir pieņēmuši savas nostājas par priekšlikumu un risina sarunas, ko vajadzētu izdoties pabeigt līdz gada beigām. Pārskatītais rīcības plāns[39] savvaļas dzīvnieku

[37] COM(2022) 480.
[38] COM(2022) 732.
[39] COM(2022) 581.

un augu kontrabandas apkarošanai ir jāīsteno, lai vēl vairāk uzlabotu pārkāpumu novēršanu un noteikumu izpildes nodrošināšanu.

Aktīvu atgūšana un konfiskācija

Cīņā ar organizēto noziedzību ir būtiski atņemt noziedzniekiem nelikumīgi iegūtos ieņēmumus. Tāpēc papildus priekšlikumam, kas piešķir tiesībaizsardzības iestādēm piekļuvi informācijai par bankas kontiem visā ES[40] (politisku vienošanos par to panāca 2023. gada jūnijā), Komisija 2022. gada maijā ierosināja priekšlikumu par aktīvu atgūšanu un konfiskāciju[41], lai uzlabotu aktīvu izsekošanu, identificēšanu, iesaldēšanu, konfiskāciju un pārvaldības spējas. Priekšlikuma svarīgākie noteikumi attiecas uz finanšu izmeklēšanai izvirzītajām prasībām, papildu pilnvaru un rīku piešķiršanu aktīvu atguves dienestiem, kā arī uz iedarbīgākiem iesaldēšanas un konfiskācijas pasākumiem, ko piemēro plašākam lokam noziedzīgu nodarījumu. Tajā skaitā šādus pasākumus piemēros par Savienības ierobežojošo pasākumu pārkāpumiem, kurus turpmāk uzskatīs par noziedzīgiem nodarījumiem. Komisija 2022. gada decembrī pieņēma atsevišķu priekšlikumu par noziedzīgu nodarījumu un sodu definēšanu attiecībā uz Savienības ierobežojošo pasākumu pārkāpumiem. Savienības ierobežojošo pasākumu faktiska īstenošana un izpilde joprojām ir viena no Komisijas galvenajām prioritātēm, un to veicina arī darba grupa "*Freeze and Seize*", ko Komisija izveidoja, reaģējot uz Krievijas agresijas karu pret Ukrainu. Gan Eiropas Parlaments, gan Padome ir pieņēmuši savas nostājas par abiem priekšlikumiem, lai vienošanos varētu panākt līdz šā gada beigām.

Nelikumīgi iegūtu līdzekļu legalizācijas novēršanas tiesību aktu kopums

Nelikumīgi iegūtu līdzekļu legalizācija ir saistīta praktiski ar visām noziedzīgām darbībām Eiropas Savienībā, kuru gaitā līdzekļus iegūst nelikumīgi[42], un tāpēc tās novēršana ir nozīmīgs rīks noziedzības apkarošanai Eiropas Savienībā. Komisija 2021. gada jūlijā nāca klajā ar vērienīgiem priekšlikumiem par to, kā stiprināt ES pasākumus nelikumīgi iegūtu līdzekļu legalizācijas un teroristu finansēšanas novēršanai[43], ierosinot četrus tiesību aktus, lai sekmīgāk novērstu un atklātu noziedznieku mēģinājumus legalizēt nelikumīgi iegūtus līdzekļus vai finansēt teroristu darbības, izmantojot finanšu sistēmu. Vienu no četrām ierosinātajām iniciatīvām — par kriptoaktīvu pārvedumu izsekošanu — likumdevējiestādes pieņēma 2023. gada maijā[44]. Attiecīgo regulu sāks piemērot 2024. gada 30. decembrī, un līdz tam visiem kriptoaktīvu pakalpojumu sniedzējiem būs jāiegūst un jāglabā informācija par kriptoaktīvu pārvedumu iniciatoru un kriptoaktīvu saņēmēju. Pārējo trīs priekšlikumu mērķis ir i) izveidot jaunu ES iestādi nelikumīgi iegūtu līdzekļu legalizēšanas novēršanai, lai nodrošinātu konsekventu un kvalitatīvu uzraudzību visā iekšējā tirgū, tajā skaitā uzraugot arī riskantākos pārrobežu subjektus, un atbalstītu un koordinētu finanšu ziņu vākšanas vienību darbu, ii) noteikt saskaņotus noteikumus, ko jāievēro privātajam sektoram, tajā skaitā ieviest vienotu ierobežojumu visā Eiropas Savienībā, paredzot, ka norēķināties par pakalpojumiem vai precēm skaidrā naudā drīkst vienīgi tad, ja pirkuma summa nepārsniedz 10 000 EUR, un iii) stiprināt kompetento iestāžu pilnvaras un sadarbības instrumentus. Paredzams, ka šis tiesību aktu kopums būtiski uzlabos ES spējas apkarot nelikumīgi iegūtu līdzekļu legalizāciju

[40] COM(2021) 429.

[41] COM(2022) 245.

[42] Eiropols, "*Enterprising criminals — Europe's fight against the global networks of financial and economic crime*", 2020.

[43] COM(2021) 420.

[44] Regula (ES) 2023/1113 (2023. gada 31. maijs) par līdzekļu un konkrētu kriptoaktīvu pārvedumiem pievienoto informāciju un ar ko groza Direktīvu (ES) 2015/849.

un aizsargāt ES iedzīvotājus no terorisma un organizētās noziedzības. Likumdevējiestādes patlaban risina sarunas par trim vēl nepieņemtajiem priekšlikumiem, un ir iecerēts panākt vienošanos par attiecīgo dokumentu līdz pašreizējā Parlamenta sasaukuma pilnvaru termiņa beigām.

Komisija aicina Eiropas Parlamentu un Padomi steidzami, vēlākais līdz pašreizējā Eiropas Parlamenta sasaukuma pilnvaru termiņa beigām, pabeigt iestāžu sarunas par šādiem dokumentiem:

- priekšlikums direktīvai par aktīvu atgūšanu un konfiskāciju;
- priekšlikums direktīvai par noziedzīgu nodarījumu un sodu definēšanu attiecībā uz Savienības ierobežojošo pasākumu pārkāpumiem;
- Cilvēku tirdzniecības apkarošanas direktīvas priekšlikums;
- priekšlikums direktīvai par vides krimināltiesiskās aizsardzības uzlabošanu;
- nelikumīgi iegūtu līdzekļu legalizācijas novēršanas tiesību aktu kopuma priekšlikums;
- priekšlikums atjaunināt esošos tiesību aktus par civilām vajadzībām paredzētu šaujamieroču importu, eksportu un tranzītu;

Komisija aicina dalībvalstis, ES aģentūras un struktūras:

- sadarboties, lai 2023. un 2024. gadā īstenotu 17 darbības, ko paredz ES ceļvedis narkotiku tirdzniecības un organizētās noziedzības apkarošanai.

V. Spēcīga Eiropas drošības ekosistēma

Pēdējos gados drošības apdraudējumiem aizvien biežāk piemīt pārrobežu raksturs, tāpēc ir jāveicina turpmāka sinerģija un ciešāka sadarbība visos līmeņos. Kopš Drošības savienības stratēģijas pieņemšanas ir īstenotas nozīmīgas iniciatīvas pārrobežu sadarbības maksimālai uzlabošanai, racionalizējot un modernizējot pieejamos instrumentus un procedūras gan uz ārējām robežām, gan Šengenas zonā, kā arī stiprinot informācijas apmaiņu starp tiesībaizsardzības un tiesu iestādēm, lai sekmīgāk apkarotu organizēto noziedzību. Šajos apstākļos datu apmaiņas sadarbspējas satvara faktiska īstenošana ir svarīga, lai uzlabotu drošību un Eiropa varētu rezultatīvi reaģēt uz pārrobežu apdraudējumiem, vienlaikus garantējot brīvu pārvietošanos tās iekšienē.

Uzlabota informācijas apmaiņa Šengenas zonā — iepriekšēja pasažieru informācija (IPI), pasažieru datu reģistri (PDR) un "Prīme II"

Divi priekšlikumi par IPI, ko Komisija pieņēma 2022. gada decembrī[45] , uzlabos Savienības iekšējo drošību, nodrošinot dalībvalstu tiesībaizsardzības iestādes ar papildu rīkiem smagu noziegumu un terorisma apkarošanai. Konkrētāk, iepriekšējas pasažieru informācijas vākšana par ES iekšējiem lidojumiem un tās izmantošana kopā ar aviopasažieru datu reģistriem ļaus dalībvalstu tiesībaizsardzības iestādēm būtiski uzlabot izmeklēšanas efektivitāti, padarot to darbības mērķorientētākas. Ir svarīgi, lai ierosinātos noteikumus pieņemtu iespējami ātrāk. Tas ne tikai sekmēs organizētās noziedzības un terorisma apkarošanu, bet arī ievērojami

[45] COM(2022) 729, COM(2022) 73.

samazinās nepieciešamību sistemātiski pārbaudīt visus ceļotājus, ja uz laiku tiks atjaunota iekšējā robežkontrole, tādējādi atvieglojot gaisa satiksmi un veicinot pārvietošanās brīvību. Eiropas Komisija 2023. gada 6. septembrī ieteica Padomei pilnvarot Komisiju sākt sarunas ar Šveici, Islandi un Norvēģiju par nolīgumu slēgšanu par PDR datu pārsūtīšanu. Minēto trīs ieteikumu pieņemšana sekmēs konsekventu un iedarbīgu ES ārējo politiku PDR jomā.

Prīmes sistēmu datu apmaiņai policija izmanto ikdienas darbā, lai apkarotu organizēto noziedzību, narkotiku tirdzniecību, terorismu, seksuālu izmantošanu un cilvēku tirdzniecību. Priekšlikums par datu automatizētu apmaiņu policijas sadarbībai ("Prīme II")[46] pārskata esošo Prīmes sistēmu, lai novērstu informācijas nepilnīgumu un uzlabotu noziedzīgu nodarījumu novēršanu, atklāšanu un izmeklēšanu Eiropas Savienībā. Pašreizējā sasaukuma laikā iesniegtie priekšlikumi par policijas sadarbību ietver ne vien pārskatītos noteikumus par datu automatizētu apmaiņu policijas sadarbībai, bet arī jau pieņemto Padomes ieteikumu pārrobežu operatīvās sadarbības stiprināšanai un Direktīvu par informācijas apmaiņu starp dalībvalstu tiesībaizsardzības iestādēm. Šo saistīto instrumentu ātra pieņemšana un īstenošana uzlabos, atvieglos un paātrinās datu apmaiņu starp tiesībaizsardzības iestādēm un palīdzēs atklāt noziedzniekus.

Pilnībā sadarbspējīga robežu pārvaldības sistēma drošai, stabilai, digitālai un vienotai Šengenas zonai

Lai Šengenas zona bez iekšējām robežām darbotos sekmīgi, būtisks nosacījums ir dalībvalstu savstarpēja uzticēšanās. Tā savukārt ir atkarīga no efektīvas kontroles, ko īsteno kā pie Savienības ārējām robežām, tā arī dalībvalstu teritorijās alternatīvu pasākumu veidā. Komisijas ierosinātajos grozījumos Šengenas Robežu kodeksā[47] ir izklāstīts, kā dalībvalstis var labāk izmantot iekšējās robežkontroles alternatīvas, kas spēj piedāvāt augstāka līmeņa drošību. Lai nodrošinātu augstu un samērīgu drošības līmeni Šengenas zonā, ir svarīgi pieņemt un pilnībā īstenot grozījumus Šengenas Robežu kodeksā. Lai labāk atbalstītu valsts iestāžu darbu drošības, kā arī robežu pārvaldības jomā, turpinās jaunas ES informācijas sistēmu arhitektūras izstrāde. Tajā ietilpst atjaunotā Šengenas Informācijas sistēma, Eiropas ceļošanas informācijas un atļauju sistēma, ieceļošanas/izceļošanas sistēma, Vīzu informācijas sistēmas atjauninājums un sadarbspējas satvars pilnībai drošai sistēmu savienošanai. Tiklīdz tā būs pilnībā pabeigta, šī jaunā arhitektūra nodrošinās valsts iestādes ar plašāku un uzticamu drošības informāciju. Visi sadarbspējas satvara komponenti ir būtiski, kas nozīmē, ka aizkavēšanās vienā no aspektiem vai vienā dalībvalstī aizkavēs sistēmas ieviešanu kopumā. Ieceļošanas/izceļošanas sistēmas tehniskajā izstrādē ir pieļaujama vienīgi minimāla aizkavēšanās, lai ieceļošanas/izceļošanas sistēma sāktu darboties iespējami ātrāk un varētu ieviest visus svarīgākos sadarbspējas satvara elementus.

Priekšlikums par skrīninga ieviešanu[48] uzlabos drošību Šengenas zonā, nosakot vienotus noteikumus par to trešo valstu valstspiederīgo identifikāciju, kuri neizpilda Šengenas Robežu kodeksā minētos ieceļošanas nosacījumus, un pakļaus viņus veselības un drošības pārbaudēm pie ārējām robežām. Šo mērķu sasniegšanu veicinās ierosinātā *Eurodac* sistēma, attiecīgos gadījumos pēc skrīninga norādot, ka konkrētā persona varētu radīt draudus iekšējai drošībai. Tas savukārt atvieglos ierosinātās Patvēruma un migrācijas pārvaldības regulas īstenošanu.

[46] COM(2021) 784.
[47] COM(2021) 891.
[48] COM(2020) 612.

Komisija mudina likumdevējiestādes ātri pabeigt sarunas par minētajiem dokumentiem, kamēr vēl nav beidzies pašreizējā Parlamenta sasaukuma periods.

Korupcijas apkarošana

Korupcija ļoti kaitē demokrātijai, ekonomikai un drošībai, jo tā veicina organizēto noziedzību un naidīgu ārvalstu iejaukšanos. Veiksmīga korupcijas novēršana un apkarošana ir būtiska, lai aizsargātu ES vērtības un ES politikas efektivitāti, kā arī lai stiprinātu tiesiskumu un uzticēšanos pārvaldes īstenotājiem un valsts iestādēm. Kā Komisijas priekšsēdētāja fon der Leiena jau paziņoja runā par stāvokli Savienībā 2022. gadā, Komisija 2023. gada 3. maijā pieņēma korupcijas apkarošanas pasākumu kopumu[49]. Komisijas priekšlikumā direktīvai par korupcijas apkarošanu ir iekļauti stingrāki noteikumi par krimināltbildības noteikšanu par korupcijas nodarījumiem un paredzēta sodu saskaņošana visā ES. Priekšlikums arī ļaus sekmīgāk īstenot izmeklēšanu un kriminālvajāšanu un īpaši uzsver to, cik svarīgi ir novērst korupciju un veidot godprātības kultūru, kurā nav vietas korupcijai. Ir sākusies priekšlikuma apspriešana Eiropas Parlamentā un Padomē. Turklāt dalībvalstis tiek aicinātas īstenot ieteikumus, kuri izriet no korupcijas apkarošanas pīlāra 2023. gada ziņojumā par tiesiskumu, ko pieņēma 2023. gada 5. jūlijā. Augstā pārstāvja priekšlikums, ko atbalsta Komisija, ierosina izveidot arī īpašu kopējās ārpolitikas un drošības politikas (KĀDP) sankciju režīmu, ko piemēros, lai vērstos pret būtiskiem korupcijas nodarījumiem visā pasaulē.

Cietušo tiesību stiprināšana

Komisija 2023. gada 12. jūlijā ierosināja grozījumus Cietušo tiesību direktīvā, lai uzlabotu cietušo piekļuvi informācijai, atbalstam un aizsardzībai un atvieglotu tiem dalību kriminālprocesā un kompensācijas saņemšanu. Viens no direktīvas pārskatīšanas vispārējiem mērķiem ir veicināt augsta līmeņa drošību, radot drošāku vidi, kas iedrošinātu cietušos ziņot par noziegumiem, mazinot to bailes no represijām.

Komisija aicina Eiropas Parlamentu un Padomi steidzami, vēlākais līdz pašreizējā Eiropas Parlamenta sasaukuma pilnvaru termiņa beigām, pabeigt iestāžu sarunas par šādiem dokumentiem:

- regulas "Prīme II" priekšlikums;
- priekšlikumi par iepriekšēju pasažieru informāciju (IPI);
- priekšlikumi par korupcijas apkarošanu un jo īpaši par īpaša kopējās ārpolitikas un drošības politikas (KĀDP) sankciju režīma izveidi;
- priekšlikums par grozījumiem Regulā par Šengenas Robežu kodeksu;
- Cietušo tiesību direktīvas priekšlikums;
- priekšlikums par skrīninga ieviešanu.

Komisija aicina dalībvalstis:

- nodrošināt ieceļošanas/izceļošanas sistēmas iespējami ātrāku stāšanos spēkā, lai pabeigtu ES informācijas apmaiņas arhitektūras ieviešanu.

VI. Īstenošana

Visas Eiropas drošības garantēšana ir kopīga atbildība, proti, ikvienam ir jāpilda savs uzdevums — Komisijai un likumdevējiestādēm ir jāpieņem jauni, stingri, visaptveroši un

[49] COM(2023) 234.

praktiski īstenojami noteikumi, dalībvalstīm šie noteikumi ir laikus jātransponē, jāīsteno un jāpiemēro, savukārt dažādām iestādēm, organizācijām un ieinteresētajām personām ir jāveic operatīvais darbs uz vietas. Svarīgs ir arī darbs, ko veic ES aģentūras tieslietu, iekšlietu un kiberdrošības jomā, un tas ir kļuvis vēl nozīmīgāks, jo nesen šo aģentūru pienākumus paplašināja.

ES finansējuma saņēmēju pārbaudīšanas uzlabošana

Īstenojot ES budžetu, Komisijas pienākums ir nodrošināt, ka ES finansējuma saņēmēji ievēro ES vērtības. Esošie mehānismi un kontroles sistēmas, kas nosaka, kurš drīkst saņemt ES finansējumu, jau ir stingras, un notiek sarunas par Finanšu regulas pārstrādāšanu ar mērķi piešķirt Komisijai spēcīgākus tiesiskos līdzekļus, lai nepieciešamības gadījumā tā varētu rīkoties. Turklāt Komisija pašlaik apsver iespējas, kā vēl vairāk uzlabot esošo un potenciālo ES finansējuma saņēmēju pārbaudīšanu, pilnveidojot norādījumus par pienākumiem ievērot ES vērtības un rīcību, kādai būtu jāseko, ja ES vērtības ir pārkāptas. Tas precizēs gan finansējuma saņēmēju, gan ES līmeņa kontroles veicēju pienākumus, un var kļūt par ierosmi valsts līmeņa rīcībai. Ja finansēšanas nosacījumi ir pārkāpti, Komisija nevilcinās un nevilcināsies pārtraukt sadarbību ar attiecīgajam projektam piešķirtā finansējuma saņēmējiem un nepieciešamības gadījumā atgūt līdzekļus. Ir svarīgi, lai dalībvalstis proaktīvi sniegtu Komisijai informāciju, jā tās konstatē iespējamus riskus attiecībā uz organizācijām, kuras pretendē uz ES finansējumu.

Pārkāpumi

Drošības jomā Komisija ir īstenojusi daudzas pārkāpuma procedūras. Piemēram, 2023. gadā ierosināja lielu skaitu pārkāpuma lietu (pret 16 dalībvalstīm) par to, ka nav izpildīti pienākumi, ko nosaka 2021. gada Regula par vēršanos pret teroristiska satura izplatīšanu tiešsaistē[50], un 2022. un 2023. gadā 20 dalībvalstis saņēma papildu oficiāla paziņojuma vēstules par to, ka nav pareizi īstenota 2011. gada Direktīva par seksuālas vardarbības pret bērniem apkarošanu[51]. Joprojām izskata ievērojamu skaitu pārkāpuma lietu par valsts tiesību aktu neatbilstību 2017. gada Direktīvai par terorisma apkarošanu[52], kā arī par to, ka nav transponēti noteikumi, kuri atvieglo finanšu un citas informācijas izmantošanu noteiktu noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai vai kriminālvajāšanai par tiem[53]. Starp citām jomām, kurās izskata pārkāpuma procedūras, ir tiesību akti par šaujamieročiem, noteikumi par psihoaktīvajām vielām, ko izmanto narkotiskajās vielās, krāpšanas un viltošanas apkarošana attiecībā uz bezskaidras naudas maksāšanas līdzekļiem, nelikumīgi iegūtu līdzekļu legalizācijas apkarošana, sodāmības reģistru informācijas apmaiņa starp dalībvalstīm un Cietušo tiesību direktīva. Dalībvalstīm, kuras īsteno saskaņotās iniciatīvas un darbības, ir pieejams atbalsts (tehnisks un finansiāls), un Komisija kā vienmēr ir gatava sadarboties ar dalībvalstīm, lai uzlabotu īstenošanu.

Uzraudzība, izmantojot Šengenas izvērtējumus, un jaunā pārvaldības sistēma

Šengenas izvērtēšanas un uzraudzības mehānisms turpināja sekmēt Šengenas noteikumu faktisku īstenošanu, kuras mērķis ir uzlabot drošību zonā, kurā neveic iekšējo robežkontroli.

---

[50] Regula (ES) 2021/784 par vēršanos pret teroristiska satura izplatīšanu tiešsaistē.

[51] Direktīva (ES) 2011/93 par seksuālas vardarbības pret bērniem apkarošanu.

[52] Eiropas Parlamenta un Padomes Direktīva (ES) 2017/541 (2017. gada 15. marts) par terorisma apkarošanu un ar ko aizstāj Padomes Pamatlēmumu 2002/475/TI un groza Padomes Lēmumu 2005/671/TI.

[53] Eiropas Parlamenta un Padomes Direktīva (ES) 2019/1153 (2019. gada 20. jūnijs), ar ko paredz noteikumus, lai atvieglotu finanšu un citas informācijas izmantošanu noteiktu noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai vai kriminālvajāšanai par tiem, un ar ko atceļ Padomes Lēmumu 2000/642/TI.

Pirmie izvērtējumi, ko saskaņā ar pastiprināto Šengenas izvērtēšanas un uzraudzības mehānismu veica 2023. gadā, ļāva savlaicīgi konstatēt un novērst stratēģisku neaizsargātību, kam būtu pārrobežu ietekme uz drošību Eiropas Savienībā. Turklāt 2023. gadā Komisija sāka tematisko Šengenas izvērtējumu par praksi tajās dalībvalstīs, kuras saskaras ar līdzīgām problēmām cīņā pret narkotisko vielu nelikumīgu tirdzniecību uz ES, pievēršot jo īpašu uzmanību liela apjoma narkotisko vielu nelikumīgai tirdzniecībai. Minētie izvērtējumi deva iespēju aplūkot Šengenas drošības elementus padziļināti un no plašāka skatpunkta. Pamatojoties uz periodiskiem, tematiskiem un neizziņotiem Šengenas izvērtējumiem, Padome 2023. gada jūnijā noteica 2023.–2024. gada Šengenas cikla prioritātes. Tajā ir norādītas prioritārās jomas, kurās ir vajadzīga papildus iniciatīva, lai padarītu Šengenas zonu drošāku un spēcīgāku. Šo prioritāšu rezultatīva un ātra īstenošana vienlaikus ar ciešāku politikas koordinēšanu Šengenas padomē vēl vairāk pastiprinās cīņu pret organizēto noziedzību un maksimāli uzlabos pārrobežu operatīvo sadarbību.

ES aģentūru un struktūru uzdevumi

Drošības savienības iniciatīvu īstenošanā būtiska nozīme ir partnerībai, jo dažādām valstu un ES iestādēm un struktūrām ir jāsadarbojas, lai sasniegtu konkrētus rezultātus. Piemēram, *EMPACT* (Eiropas daudzdisciplīnu platforma pret noziedzības draudiem) ļauj dalībvalstīm īstenot strukturētu daudzdisciplīnu sadarbību, ko atbalsta visas ES iestādes, struktūras un aģentūras (piemēram, Eiropols, *Frontex*, *Eurojust*, *CEPOL*, *OLAF*, *eu-LISA*). *EMPACT* īstenotās operācijas, tajā skaitā izmantojot īpašas operatīvās darba grupas (*OTF*), koordinē dalībvalstu un operatīvo partneru darbības noziedzīgo tīklu un smagu noziegumu apkarošanai. Pateicoties *EMPACT*, tikai 2022. gadā vien tika veiktas 9922 aizturēšanas, konfiscēti aktīvi un nauda vairāk nekā 180 miljonu EUR vērtībā, ierosinātas 9263 izmeklēšanas, apzināti 4019 cietušie, izņemtas vairāk nekā 62 tonnas narkotisko vielu, apzināts 51 īpaši vērtīgs mērķis (*HVT*) un aizturēti 12 *HVT*, īstenotas operācijas saistībā ar agresijas karu pret Ukrainu, jo īpaši vēršoties pret cilvēku tirdzniecību un ar šaujamieročiem saistītiem apdraudējumiem.

Frontex, Eiropas Jūras drošības aģentūra (*EMSA*) un Eiropas Zivsaimniecības kontroles aģentūra (*EFCA*) turpina stiprināt sadarbību krasta apsardzes funkciju pildīšanā, lai atbalstītu valsts iestādes jūras drošības uzlabošanā. Minētās aģentūras ievērojami veicinās ES Jūras drošības stratēģijas īstenošanu.

Vairākās drošības savienības iniciatīvās attiecīgajām aģentūrām ir uzticēti jauni pienākumi un uzdevumi, kuru izpildei dažos gadījumos būs jāveic izmaiņas cilvēkresursos.

*Eiropas Savienības Kiberdrošības aģentūra (*ENISA*)*

Attiecībā uz incidentiem un reaģēšanu uz tiem Komisija ir veikusi īstermiņa pasākumu nolūkā atbalstīt dalībvalstis, piešķirot **Eiropas Savienības Kiberdrošības aģentūrai (*ENISA*)** līdzekļus no programmas "Digitālā Eiropa", lai paaugstinātu gatavību smagiem kiberincidentiem un spējas reaģēt uz tiem. Šis pasākums ir 2023. gada aprīlī pieņemtā Kiberdrošības solidaritātes akta priekšlikuma pamatā, un, kad likumdevējiestādes būs minēto aktu pieņēmušas, *ENISA* varētu uzticēt papildu uzdevumus, piemēram, Savienības topošās kiberdrošības rezerves darbības nodrošināšanu un pārvaldību vai incidenta pārskata ziņojumu sagatavošanu par liela mēroga kiberdrošības incidentiem. Kibernoturības akta priekšlikums paredz uzdot *ENISA* saņemt ražotāju paziņojumus par ievainojamībām produktos ar digitāliem elementiem un par incidentiem, kuri ietekmē minēto produktu drošību, un *ENISA* būs šādi paziņojumi jāpārsūta attiecīgajām datordrošības incidentu reaģēšanas vienībām (*CSIRT*) vai attiecīgajiem dalībvalstu vienotajiem kontaktpunktiem. *ENISA* arī būs reizi divos

gados jāsagatavo tehniskais ziņojums par jaunākajām tendencēm attiecībā uz kiberdrošības riskiem produktos ar digitāliem elementiem un jāiesniedz tas TID sadarbības grupai.

*Eiropas Kiberdrošības kompetenču centrs (*ECCC*)*

Eiropas Kiberdrošības kompetenču centrs (*ECCC*) kopā ar Nacionālo koordinācijas centru (NKC) tīklu ir Savienības jaunā struktūra inovāciju un rūpniecības politikas atbalstam kiberdrošības jomā. Šī ekosistēma stiprinās kiberdrošības tehnoloģiju kopienas spējas, nodrošinās pētniecības izcilību un stiprinās Savienības ražošanas nozares konkurētspēju šajā jomā. *ECCC* un NKC pieņems lēmumus par ilgtermiņa stratēģiskajām investīcijām un apvienos Savienības un dalībvalstu resursus un netieši arī nozares resursus, lai uzlabotu un stiprinātu tehnoloģiskās un industriālās kiberdrošības spējas. Līdz ar to *ECCC* ir būtiska nozīme programmā "Digitālā Eiropa" un programmā "Apvārsnis Eiropa" izvirzīto vērienīgo kiberdrošības mērķu sasniegšanā.

ECCC ir pieņēmis darbā vairāk nekā pusi no personāla un drīz nolīgs izpilddirektoru. Starp jau sāktajiem darbiem ir programmas "Digitālā Eiropa" kiberdrošības daļa un jauna stratēģiskā programma[54] tehnoloģiju attīstībai un ieviešanai, kurā ir noteiktas prioritārās darbības, lai atbalstītu MVU stratēģisku kiberdrošības tehnoloģiju, pakalpojumu un procesu izstrādē un izmantošanā, atbalstītu un palielinātu profesionālu darbaspēku un stiprinātu pētniecības, izstrādes un inovācijas lietpratību plašākajā Eiropas kiberdrošības ekosistēmā.

Eiropas Savienības Aģentūra tiesībaizsardzības sadarbībai (Eiropols)

Pateicoties nesen iegūtajām jaunajām pilnvarām, **Eiropols** spēs labāk atbalstīt dalībvalstis organizētās noziedzības apkarošanā. Galvenā prioritāte ir cīņa pret nelikumīgu narkotisko vielu tirdzniecību, jo palielinās gan tās nozīmīgums, gan negatīvā ietekme uz ES iedzīvotāju drošību. Pēc pilnvarojuma saņemšanas no Eiropas Savienības Padomes 2023. gada 15. maijā Komisija aktīvi strādā, lai noslēgtu ar Bolīviju, Brazīliju, Ekvadoru, Meksiku un Peru starptautiskus nolīgumus par personas datu apmaiņu ar Eiropolu nolūkā novērst un apkarot smagus noziegumus un terorismu.

*Eiropas Savienības Aģentūra tiesu iestāžu sadarbībai krimināllietās (*Eurojust*)*

Eurojust sniedz valstu iestādēm tiesisko atbalstu dažādu smagu un sarežģītu pārrobežu noziedzīgu nodarījumu apkarošanā vairāk nekā 20 gadus un ir nostiprinājusi savas pozīcijas ES brīvības, drošības un tiesiskuma telpā. Lai stiprinātu plašāka mēroga sadarbību, Komisija risina sarunas par starptautiskiem nolīgumiem, kas atvieglos sadarbību starp *Eurojust* un 13 trešām valstīm personas datu apmaiņā ar mērķi apkarot organizēto noziedzību un terorismu[55]. Sarunas jau ir pabeigtas ar Armēniju un Libānu, turpinās ar Alžīriju un Kolumbiju un ir sāktas ar Bosniju un Hercegovinu. Komisija mudina Eiropas Parlamentu un Padomi pabeigt nolīgumu slēgšanu ar minētajām valstīm līdz pašreizējā Parlamenta sasaukuma pilnvaru termiņa beigām, lai stiprinātu starptautisko tiesisko sadarbību un plašāk apkarotu pārrobežu noziedzību.

*Eiropas Prokuratūra (*EPPO*)*

Kopš darbības sākšanas 2021. gada jūnijā **Eiropas Prokuratūra (*EPPO*)** ir apliecinājusi, ka Savienības instrumentu kopumā tā ir iedarbīgs instruments tādu nodarījumu izmeklēšanā un kriminālvajāšanā, kuri skar Savienības budžetu, — arī tādu nodarījumu, kas ir saistīti ar

[54] https://cybersecurity-centre.europa.eu/strategic-agenda_en.

[55] Alžīrija, Argentīna, Armēnija, Bosnija un Hercegovina, Brazīlija, Ēģipte, Izraēla, Jordānija, Kolumbija, Libāna, Maroka, Tunisija un Turcija.

dalību noziedzīgā organizācijā, ja tie ir galvenokārt noziegumi, kas ir vērsti pret Savienības budžetu. Komisija mudina dalībvalstis, kuras vēl nepiedalās *EPPO* ciešākajā sadarbībā, iesaistīties tajā iespējami ātrāk, lai *EPPO* varētu pilnībā realizēt savu potenciālu ES nodokļu maksātāju naudas aizsargāšanā.

*Eiropas Savienības Narkotiku aģentūra (*EUDA*)*

Likumdevējiestādes 2023. gada jūnijā apstiprināja jaunas pilnvaras, lai pārveidotu esošo Eiropas Narkotiku un narkomānijas uzraudzības centru (*EMCDDA*) par pilnvērtīgu aģentūru — **Eiropas Savienības Narkotiku aģentūru (*EUDA*)** — un stiprinātu tās nozīmi. Aģentūra spēs pilnīgāk novērtēt jaunus veselības un drošības apdraudējumus, ko rada nelikumīgas narkotiskās vielas, un sekmīgāk piedalīties darbā, kas notiek dalībvalstīs un starptautiskā līmenī. Aģentūras galvenais uzdevums joprojām būs datu vākšana, analīze un izplatīšana, bet paplašinātās pilnvaras ļaus tai attīstīt arī vispārējas veselības un drošības apdraudējumu novērtēšanas spējas, lai noteiktu jaunus apdraudējumus, tajā skaitā polinarkomāniju, stiprināt sadarbību, izmantojot valstu kontaktpunktus, un izveidot laboratoriju tīklu, kas sniegs aģentūrai kriminālistikas un toksikoloģisko informāciju. Tas atvieglos aģentūras darbu brīdinājumu izdošanā par īpaši bīstamu vielu parādīšanos tirgū un izpratnes veicināšanā.

Komisija aicina Eiropas Parlamentu un Padomi steidzami, vēlākais līdz pašreizējā Eiropas Parlamenta sasaukuma pilnvaru termiņa beigām, pabeigt iestāžu sarunas par šādiem dokumentiem:

- priekšlikums par Finanšu regulas pārstrādāšanu.

Komisija aicina dalībvalstis:

- proaktīvi sniegt Komisijai informāciju, ja tās konstatē iespējamus riskus attiecībā uz organizācijām, kuras pretendē uz ES finansējumu;
- ātri īstenot 2023.–2024. gada Šengenas cikla prioritātes, lai padarītu Šengenas zonu drošāku un spēcīgāku;
- novērst pārkāpumus, kuru dēļ pret tām ir sākta pārkāpuma procedūru, lai nodrošinātu attiecīgo tiesību aktu pienācīgu transponēšanu.

VII. Secinājums

Pēdējos trīs gados ir pastāvīgi un neatlaidīgi īstenoti centieni faktiski realizēt vērienīgo ieceri par ES drošības savienības izveidi. Visos drošības politikas jomas aspektos ir panākts ļoti liels progress. Papildu motivāciju turpināt šos centienus piešķir aizvien jaunu apdraudējumu reāla parādīšanās. Tiesiskā regulējuma izstrādi ir jāpabeidz laikus — līdz pašreizējā Parlamenta pilnvaru termiņa beigām 2024. gada pavasarī. Transponēt, īstenot un piemērot jaunos tiesību aktus ir dalībvalstu pastāvīgs pienākums. Īstenošanai jānotiek saskaņoti, tajā skaitā ar ES aģentūru atbalstu, un ļoti bieži ir nepieciešama vēl ciešāka sadarbība ar mūsu starptautiskajiem partneriem.

Sasniegt ES iedzīvotāju gaidām atbilstošu drošības līmeni ir iespējams vienīgi ar visu iesaistīto dalībnieku ciešu sadarbību un apņēmīgu rīcību, un pašreizējos apstākļos ikvienam no tiem būtu jāpilda savi uzdevumi ES drošības stiprināšanā prioritārā kārtā.