Eiropas Savienības Padome

Briselē, 2025. gada 3. aprīlī
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2025. gada 2. aprīlis
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretāre *Thérèse BLANCHET*
K-jas dok. Nr.:	COM(2025) 148 final
Temats:	KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI par *ProtectEU*: Eiropas iekšējās drošības stratēģiju

Pielikumā ir pievienots dokuments COM(2025) 148 final.

Pielikumā: COM(2025) 148 final

EIROPAS
KOMISIJA

Strasbūrā, 1.4.2025.
COM(2025) 148 final

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

par *ProtectEU*: Eiropas iekšējās drošības stratēģiju

1. *ProtectEU*: Eiropas iekšējās drošības stratēģija

Drošība ir pamats, uz kura balstās visas mūsu brīvības. Demokrātija, tiesiskums, pamattiesības, Eiropas iedzīvotāju labbūtība, konkurētspēja un labklājība – tas viss ir atkarīgs no mūsu spējas garantēt pamatdrošību. Jaunajā drošības apdraudējumu laikmetā, kurā pašlaik dzīvojam, ES dalībvalstu spēja garantēt savu iedzīvotāju drošību vairāk nekā jebkad agrāk ir atkarīga no **vienotas Eiropas pieejas mūsu iekšējās drošības aizsardzībai**. Mainīgajā ģeopolitiskajā vidē Eiropai ir jāturpina pildīt savs pastāvīgais solījumu par mieru.

Jau ir sperti pirmie soļi ceļā uz Eiropas drošības aparāta izveidi. Pēdējā desmitgadē esam sagatavojuši Savienībai uzlabotus kolektīvos mehānismus, kas paredzēti rīcībai tiesībaizsardzības un tiesu iestāžu sadarbības, robežu drošības, smagās un organizētās noziedzības apkarošanas, terorisma un vardarbīga ekstrēmisma apkarošanas un ES fiziskās un digitālās kritiskās infrastruktūras aizsardzības jomā. Būtiska nozīme joprojām ir iepriekš pieņemto tiesību aktu un izstrādātās politikas pienācīgai īstenošanai.

Mūsdienu draudu raksturs un ciešā saikne starp ES iekšējo un ārējo drošību liek mums virzīties tālāk.

Draudu aina ir nomācoša. Robežas starp **hibrīddraudiem** un atklātu karu ir neskaidras. Krievija īsteno tiešsaistes un bezsaistes hibrīdkampaņu pret ES un tās partneriem, lai izjauktu un grautu sabiedrības kohēziju un demokrātiskos procesus un pārbaudītu ES solidaritāti ar Ukrainu. Naidīgas ārvalstis un valsts sponsorēti aktori cenšas iekļūt mūsu kritiskajā infrastruktūrā un piegādes ķēdēs un sagraut tās, nozagt sensitīvus datus un pozicionēt sevi tā, lai panāktu maksimālus traucējumus nākotnē. Viņi izmanto noziedzību kā pakalpojumu, bet noziedzniekus kā starpniekus. Turklāt mūsu atkarība no trešām valstīm piegādes ķēžu ziņā mūs padara neaizsargātākus pret naidīgu valstu hibrīdkampaņām.

Kā uzsvērts ES smagās un organizētās noziedzības draudu novērtējumā (*SOCTA*), ar ko nesen iepazīstināja Eiropols, Eiropā izplatās spēcīgi **organizētās noziedzības tīkli**, kas, pateicoties internetam, kļūst azivien spēcīgāki un iefiltrējas mūsu ekonomikā un ietekmē mūsu sabiedrību[1]. Kad organizētā noziedzība ir iesakņojusies kopienā vai ekonomikas nozarē, tās izskaušana kļūst par smagu cīņu – viena trešdaļa no visvairāk apdraudošajiem noziedzīgajiem tīkliem darbojas jau vairāk nekā desmit gadus. Kriptovalūtas un paralēlas finanšu sistēmas palīdz tiem legalizēt un slēpt savus noziedzīgi iegūtos līdzekļus.

Terorisma draudu līmenis Eiropā turpina pieaugt. Reģionālas krīzes ārpus ES rada būtisku ietekmi, sniedzot jaunu motivāciju dažādas ideoloģijas pārstāvošām teroristu organizācijām vervēt un mobilizēt teroristus, vai palielināt to spējas. Tās savus radikalizācijas un vervēšanas centienus vērš tieši uz visneaizsargātākajām mūsu sabiedrības grupām un īpaši uz konkrētām jauniešu grupām. Tās iedvesmo vienatnē darbojošos aktoru uzbrukumus un pret sistēmu vērsta ekstrēmisma pieaugumu, kura mērķis ir sagraut demokrātisko tiesisko kārtību.

Straujā un plašā **tehnoloģiju attīstība** ir būtisks instruments mūsu drošības aparāta uzlabošanai. Taču arvien biežāk notiek kiberuzbrukumi un ārvalstu īstenota informācijas manipulācija, izmantojot jaunas tehnoloģijas, piemēram, mākslīgo intelektu. Bērni, jaunieši un vecāka gadagājuma cilvēki ir īpaši apdraudēti tiešsaistē, un naida izplatīšanās tiešsaistē apdraud vārda brīvību un sociālo kohēziju.

Mūsu dzīve ir kļuvusi mazāk droša, un to arvien vairāk izjūt eiropieši, kuru **priekšstats par drošumu un drošību ES** ir pasliktinājies tiktāl, ka uz jautājumu par nākotni 64 % no viņiem

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

atbild, ka ir nobažījušies par ES drošību[2]. Arī uzņēmumu vidū pieaug bažas; maldinoša informācija un dezinformācija, noziedzība un nelikumīgas darbības, kā arī kiberspiegošana ir viens no desmit lielākajiem riskiem, kas apzināti Pasaules Ekonomikas foruma 2025. gada ziņojumā par globālajiem riskiem[3].

Eiropiešiem vajadzētu būt **iespējai dzīvot bez bailēm** gan uz ielām, gan mājās, sabiedriskās vietās, metro vai internetā. ES drošības jomā veiktā darba centrā ir cilvēku aizsardzība, īpaši to cilvēku aizsardzība, kuri ir visneaizsargātākie pret uzbrukumiem, kas nesamērīgi skar bērnus, sievietes un minoritātes, arī ebreju un musulmaņu kopienas. Aizsardzība ir būtiska, lai veidotu noturīgu un saliedētu sabiedrību.

Komisija nāk klajā ar **Eiropas iekšējās drošības stratēģiju**, lai turpmākajos gados labāk novērstu apdraudējumus. Ar stingrāku juridisko instrumentu kopumu, ciešāku sadarbību un plašāku informācijas apmaiņu mēs uzlabosim mūsu noturību un kolektīvo spēju paredzēt, novērst, atklāt drošības apdraudējumus un efektīvi reaģēt uz tiem. Vienota pieeja iekšējai drošībai var palīdzēt dalībvalstīm izmantot tehnoloģiju potenciālu, lai stiprinātu, nevis vājinātu drošību, vienlaikus veicinot drošu digitālo telpu visiem. Turklāt tā atbalsta dalībvalstu kopīgu reakciju uz globālām politiskām un ekonomiskām pārmaiņām, kas ietekmē Savienības iekšējo drošību.

Šīs stratēģijas pamatā ir **trīs principi** un tiesiskuma un pamattiesību ievērošana.

Pirmkārt, tajā ir izvirzīta vērienīga iecere mainīt kultūru drošības jomā. Mums ir vajadzīga **visu sabiedrību aptveroša pieeja**, kurā iesaistīti visi iedzīvotāji un ieinteresētās personas, arī no pilsoniskās sabiedrības, pētniecības un akadēmiskajām aprindām un privātām struktūrām. Tāpēc stratēģijā paredzētajos pasākumos, kad vien iespējams, tiek izmantota integrēta daudzu ieinteresēto personu pieeja.

Otrkārt, **drošības apsvērumi ir jāintegrē un jāiekļauj visos ES tiesību aktos, politikā un programmās**, arī ES ārējā darbībā. Tiesību akti, politika un programmas būs jāsagatavo, jāpārskata un jāīsteno, paturot prātā drošības perspektīvu, un jānodrošina, ka tiek ņemti vērā nepieciešamie drošības apsvērumi, lai veicinātu saskaņotu un visaptverošu pieeju drošībai.

Visbeidzot, drošai un noturīgai Eiropai ir vajadzīgas **būtiskas investīcijas no ES, tās dalībvalstīm un privātā sektora**. Šajā stratēģijā izklāstītajām prioritātēm un darbībām ir vajadzīgi pietiekami cilvēkresursi un finanšu resursi, lai nodrošinātu to īstenošanu. Kā noteikts paziņojumā "Ceļā uz nākamo daudzgadu finanšu shēmu"[4], Eiropai būs jāpalielina publiskie izdevumi drošībai un jāveicina pētniecība un investīcijas drošības jomā, tādējādi palielinot savu stratēģisko autonomiju.

Šī stratēģija papildina **Eiropas sagatavotības savienības stratēģiju**[5], kurā izklāstīta integrēta visu apdraudējumu pieeja sagatavotībai konfliktiem, cilvēku izraisītām un dabas katastrofām, un krīzēm, un **Balto grāmatu par Eiropas aizsardzības gatavību 2030. gadam**[6], kas palīdz pastiprināt aizsardzības spēju attīstību un iegūšanu visā ES nolūkā atturēt ārvalstu pretiniekus. Komisija arī ierosinās izveidot **Eiropas demokrātijas vairogu**, lai stiprinātu demokrātisko noturību Eiropas Savienībā. Šajās iniciatīvās kopā ir formulēts redzējums par drošu, aizsargātu un noturīgu ES.

[2] Eirobarometra zibensaptauja FL550: *EU Challenges and Priorities* (ES uzdevumi un prioritātes).
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, 17. lpp.
[4] COM (2025) 46 final.
[5] JOIN (2025) 130 final.
[6] JOIN (2025) 120 final.

Jauna Eiropas iekšējās drošības pārvaldība

Komisija cieši sadarbosies ar dalībvalstīm un ES aģentūrām, lai uzlabotu ES pieeju iekšējai drošībai gan stratēģiskā, gan operatīvā līmenī.

Šā mērķa sasniegšanai paredzēts:

- **konsekventi apzināt jauno un pārskatīto Komisijas iniciatīvu iespējamo ietekmi uz drošību un sagatavotību jau sarunu procesa sākumā un visā sarunu procesā;**
- **rīkot Komisijas projekta grupas Eiropas iekšējās drošības jautājumos regulāras sanāksmes, ko papildina stratēģiska pārnozaru sadarbība Komisijas ietvaros;**
- **iepazīstināt ar draudu analīzi saistībā ar iekšējo drošību, lai atbalstītu Drošības koledžas darbu;**
- **vest diskusijas ar dalībvalstīm Padomē par mainīgajām iekšējās drošības problēmām, pamatojoties uz draudu analīzi un viedokļu apmaiņu par galvenajām politikas prioritātēm;**
- **regulāri ziņot Eiropas Parlamentam un Padomei, lai sekotu līdzi un atbalstītu svarīgāko drošības iniciatīvu sistemātisku īstenošanu.**

2. Integrētā situācijas apzināšanās un analīze

Mēs radīsim ES jaunus veidus, kā apmainīties ar informāciju un to apvienot, un nodrošināsim regulāru ES iekšējās drošības apdraudējumu analīzi, kas sekmēs visaptverošu risku un draudu novērtējumu.

Drošība sākas ar **efektīvu prognozēšanu**. ES ir jāpaļaujas uz visaptverošu, pietiekami autonomu un atjauninātu situācijas apzināšanos un draudu analīzi. Praktiski izmantojami izlūkdati, kurus dalībvalstis tiek mudinātas vēl vairāk uzlabot, izmantojot vienoto izlūkdatu analīzes procedūru (*SIAC)* kā vienotu piekļuves punktu dalībvalstu izlūkdatiem, ir ļoti svarīgi draudu novērtēšanai un apkarošanai un galu galā palīdz veidot politiskus un likumdošanas pasākumus[7]. Mums ir efektīvāk un sadarbīgāk **jāizmanto uz izlūkdatiem balstīta analīze** un **draudu novērtējumi** ES līmenī.

Pamatojoties uz dažādiem riska un draudu novērtējumiem, kas sagatavoti ES līmenī un konkrētās nozarēs[8], Komisija **regulāri sagatavos ES iekšējās drošības apdraudējumu analīzi**, lai apzinātu galvenās drošības problēmas nolūkā izgaismot politikas prioritātes. Tas palīdzēs izstrādāt elastīgu un reaģētspējīgu iekšējās drošības politiku, kas efektīvi novērš mainīgos apdraudējumus, labāk aizsargā cilvēkus un uzņēmumus pret uzbrukumiem un ļauj savlaicīgi veikt mērķtiecīgus politikas intervences pasākumus. Šī ES iekšējās drošības apdraudējuma analīze arī palīdzēs veikt **visaptverošu ES (pārnozaru, visu apdraudējumu) risku un draudu novērtējumu**, ko izstrādājusi Komisija un Augstais pārstāvis, kā izklāstīts Eiropas sagatavotības savienības stratēģijā.

[7] *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness,* (Drošāk kopā – Eiropas civilās un militārās sagatavotības un gatavības stiprināšana), 23. lpp.

[8] Nozaru draudu novērtējumi, kas palīdzēs sagatavot šo draudu analīzi, ietver ES smagās un organizētās noziedzības draudu novērtējumu (*SOCTA*), ES ziņojumu par terorisma situāciju un tendencēm (*TE-SAT*), Kopīgo kibernovērtējuma ziņojumu (*JCAR*) un turpmākus nelikumīgi iegūtu līdzekļu legalizēšanas un teroristu finansēšanas draudu, risku un metožu novērtējumus, kas jāveic Komisijai un Iestādei nelikumīgi iegūtu līdzekļu legalizēšanas novēršanai.

Uzticamībai un drošai apstrādei ir būtiska nozīme informācijas apmaiņā, un tai ir vajadzīga uzticama un droša infrastruktūra. ES iestādēm, struktūrām un aģentūrām ir jānodrošina spēja izmantot **drošus saziņas kanālus** sensitīvas un klasificētas informācijas apmaiņai savā starpā un ar dalībvalstīm. Investīcijas **sadarbspējīgās drošās sistēmās** un uzticamās tehnoloģijās stiprinās ES autonomiju un spēju pārvarēt krīzes un nodrošināt darbības noturību. Šajā sakarā Komisija mudina abus likumdevējus pabeigt sarunas par **ierosināto regulu par informācijas drošību Savienības iestādēs, struktūrās, birojos un aģentūrās**, īpaši, lai nodrošinātu vienotu sistēmu sensitīvas neklasificētas un klasificētas informācijas apstrādei[9].

Lai nodrošinātu savu darbības drošību un situācijas apzināšanos, Komisija pārskatīs savu korporatīvās drošības pārvaldības sistēmu un izveidos **Integrētu drošības operāciju centru (*ISOC*)**, lai aizsargātu cilvēkus, fiziskos aktīvus un darbības visās Komisijas telpās. Komisija arī palielinās savas operatīvās un analītiskās spējas apzināt hibrīddraudus un mazināt tos.

Saskaņā ar Eiropas sagatavotības savienības stratēģiju sagatavotības un drošības apsvērumi tiks integrēti un iekļauti visos ES tiesību aktos, rīcībpolitikās un programmās. Komisija konsekventi noteiks vēlamā politikas risinājuma iespējamo ietekmi uz sagatavotību un drošību, kad tā gatavos vai pārskatīs tiesību aktus, politiku vai programmas, paturot prātā sagatavotības un drošības perspektīvu. Tas tiks nodrošināts ar regulāru apmācību politikas veidotājiem Komisijā.

Lai palīdzētu dalībvalstīm, Komisija apspriedīs ar Padomi jaunās iekšējās drošības problēmas un galvenās politikas prioritātes un regulāri sniegs tai jaunāko informāciju par stratēģijas īstenošanu. Turklāt Komisija informēs Eiropas Parlamentu un attiecīgās ieinteresētās personas un iesaistīsies visās attiecīgajās darbībās.

Pamatdarbības

Komisija:

- **izstrādās un regulāri sniegs draudu analīzi saistībā ar ES iekšējās drošības problēmām**

Dalībvalstis tiek mudinātas:

- **uzlabot izlūkdatu apmaiņu ar *SIAC* un nodrošināt labāku informācijas apmaiņu ar ES aģentūrām un struktūrām**

Eiropas Parlaments un Padome tiek aicināti:

- **pabeigt sarunas par ierosināto regulu par informācijas drošību Savienības iestādēs, struktūrās, birojos un aģentūrās**

3. Pastiprinātas ES drošības spējas

Mēs izstrādāsim jaunus tiesībaizsardzības instrumentus, piemēram, pārveidotu Eiropolu, un labākus līdzekļus, lai koordinētu un nodrošinātu drošu datu apmaiņu un likumīgu piekļuvi datiem.

Lai efektīvi vērstos pret jauniem apdraudējumiem, ES ir jāuzlabo savas drošības spējas un jāveicina inovācija. Tiesībaizsardzības un tiesu iestādēm kā galvenajiem dalībniekiem, kas vēršas pret iekšējās drošības apdraudējumiem, ir vajadzīgi pareizi operatīvie instrumenti un spējas, lai ātri un efektīvi rīkotos. Ir svarīgi, lai šīs iestādes varētu sazināties un koordinēt darbību pāri robežām un starp dienestiem, lai rezultatīvi novērstu, atklātu, izmeklētu un sauktu pie atbildības.

[9] COM(2022) 119 final.

ES iekšējās drošības aģentūras un struktūras

ES aģentūrām un struktūrām tieslietu, iekšlietu un kiberdrošības jomā ir būtiska loma drošības arhitektūrā, un šī loma turpina palielināties, paplašinoties to pienākumiem.

Tagad – 25 gadus pēc **Eiropola** izveidošanas tas ir kļuvis par vēl svarīgāku ES drošības sistēmas daļu. Tas palīdz veikt sarežģītas pārrobežu izmeklēšanas, atvieglo informācijas apmaiņu, izstrādā inovatīvus policijas darbības rīkus un nodrošina padziļinātas speciālās zināšanas tiesībaizsardzības jomā. Tomēr vairāki faktori neļauj Eiropolam pilnībā izmantot savu operatīvo potenciālu, lai atbalstītu izmeklēšanas un operatīvās darbības pārrobežu noziedzības apkarošanai – to skaitā ir gan nepietiekams resursu līmenis, gan tas, ka Eiropola pašreizējās pilnvaras neattiecas uz jauniem drošības apdraudējumiem, piemēram, sabotāžu, hibrīddraudiem vai manipulācijām ar informāciju. Tāpēc Komisija ierosinās **vērienīgu Eiropola pilnvaru pārskatīšanu**, lai to pārveidotu par patiesi funkcionējošu policijas aģentūru, kas labāk atbalstītu dalībvalstis. Mērķis ir stiprināt Eiropola tehnoloģisko kompetenci un spējas atbalstīt valstu tiesībaizsardzības iestādes, uzlabot koordināciju ar citām aģentūrām un struktūrām, kā arī ar dalībvalstīm, stiprināt stratēģiskās partnerības ar partnervalstīm un privāto sektoru un nodrošināt pastiprinātu Eiropola pārraudzību.

Turklāt Komisija strādās, lai vēl vairāk **uzlabotu ES iekšējās drošības aģentūru un struktūru efektivitāti un papildināmību un stiprinātu netraucētu sadarbību** starp tām.

Eurojust pilnvaras tiks novērtētas un pastiprinātas rezultatīvākai tiesu iestāžu sadarbībai, lai uzlabotu papildināmību un sadarbību ar Eiropolu. Tas ietver *Eurojust* efektivitātes uzlabošanu, kā arī tā spēju sniegt proaktīvu atbalstu un analīzi dalībvalstu tiesu iestādēm. Turklāt, ņemot vērā ***EPPO*** unikālo kompetenci izmeklēt noziegumus, kas skar Savienības finanšu intereses, un saukt pie atbildības par tiem, Komisija apsvērs, kā vislabāk uzlabot *EPPO* spēju aizsargāt Savienības līdzekļus. Tas ietvers *EPPO* un Eiropola sadarbības stiprināšanu.

Efektīvai un drošai informācijas apmaiņai starp aģentūrām ir izšķiroša nozīme sadarbībā. Eiropolam un *Frontex* ir vajadzīga ātra savstarpēja informācijas apmaiņa, arī operatīvos nolūkos, pēc 2024. gada janvāra kopīgā paziņojuma[10]. Aģentūrai ***eu-LISA*** ir centrāla loma datu drošas glabāšanas un pieejamības nodrošināšanā, lai panāktu labāku koordināciju un efektīvāku informācijas apmaiņu starp aģentūrām. **ES Pamattiesību aģentūra** sniedz speciālās zināšanas par pamattiesību aizsardzību drošības politikas izstrādē un īstenošanā.

ES Iestādei nelikumīgi iegūtu līdzekļu legalizēšanas novēršanai (*AMLA*) ir piešķirtas pilnvaras salīdzināt informāciju, pamatojoties uz sakritības/nesakritības principu, ar to informāciju, ko ir sniedzis Eiropols, *EPPO*, *Eurojust* un ES Birojs krāpšanas apkarošanai, lai veiktu pārrobežu lietu kopīgu analīzi.

ENISA ir centrāla loma Eiropas kiberdrošības tiesību aktu īstenošanā. Gaidāmajā **Kiberdrošības akta pārskatīšanā** Komisija izvērtēs savas pilnvaras un ierosinās to modernizēt, lai stiprinātu tā ES pievienoto vērtību.

Sadarbība starp muitu un citām tiesībaizsardzības iestādēm tiks pastiprināta, ES Muitas reformas paketes ietvaros ierosinot izveidot **ES Muitas dienestu** un **ES muitas datu centru**. Informācija no topošā centra un saistītie dati no Eiropola, *Eurojust, EPPO*, *OLAF*, *AMLA* un *Frontex* to attiecīgās kompetences ietvaros uzlabos kopīgu analīzi un veicinās saskaņotākas operatīvās darbības, īpaši pie ārējām robežām. Komisija mudina abus likumdevējus ātri pabeigt sarunas par ES muitas reformu un turpinās tiem palīdzēt šajā nolūkā.

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

Papildināmības uzlabošana starp *EPPO*, *OLAF*, Eiropolu, *Eurojust*, *AMLA* un ierosināto ES Muitas dienestu balstīsies arī uz pašlaik notiekošās **ES krāpšanas apkarošanas arhitektūras** pārskatīšanas rezultātiem. Iekšējā drošība var gūt labumu no šīs holistiskās pieejas, ko var panākt, galveno uzmanību pievēršot gan krimināltiesību, gan administratīvo līdzekļu labākai izmantošanai, IT sistēmu sadarbspējai un uzlabotai sadarbībai.

Kritisko sakaru sistēma

Mūsdienās **kritisko sakaru sistēmas**[11] lielākoties tiek ekspluatētas izolēti valsts līmenī. Tas nozīmē, ka ātrās reaģēšanas dienestu pārstāvji bieži vien nevar sazināties ar saviem kolēģiem, ja šķērso robežu ar citām dalībvalstīm. Dažās dalībvalstīs pastāv arī ierobežojumi saziņai starp dažādiem ātrās reaģēšanas dienestu veidiem (piemēram, policijas un neatliekamās medicīniskās palīdzības dienestiem). Lielākās daļas sistēmu standarti neatbilst mūsdienu prasībām attiecībā uz funkcionalitāti un noturību, un tas ievērojami ierobežo ātrās reaģēšanas dienestu reaģēšanas spējas, īpaši pāri robežām.

Lai uzlabotu ES spēju reaģēt uz krīzēm, Komisija ierosinās tiesību aktus, lai izveidotu **Eiropas kritisko sakaru sistēmu (*EUCCS*)**, kas savienotu dalībvalstu nākamās paaudzes kritisko sakaru sistēmas ES. Mērķis ir panākt, lai *EUCCS* pamatā būtu trīs stratēģiskie pīlāri – operatīvā mobilitāte, spēcīga noturība un stratēģiskā autonomija. Ar *EUCCS* iniciatīvu tiks noteiktas saskaņotas prasības un tas palīdzēs modernizēt dalībvalstu kritisko sakaru sistēmas tā, lai tās varētu netraucēti darboties. Tas arī paplašinās sistēmas pārklājumu, izmantojot topošo *IRIS*^{2} [12] multiorbitālo sistēmu. ES finansēti projekti veidos *EUCCS* tehniskās spējas, galvenokārt paļaujoties uz Eiropas tehnoloģiju nodrošinātājiem, lai veicinātu ES stratēģisko autonomiju šajā jutīgajā nozarē.

Likumīga piekļuve datiem

Tiesībaizsardzības un tiesu iestādēm ir jāspēj izmeklēt noziegumus un veikt pret tiem vērstus pasākumus. Mūsdienās gandrīz visiem smagās un organizētās noziedzības veidiem ir digitālā pēda[13]. Aptuveni 85 % kriminālizmeklēšanu tagad ir atkarīgas no tiesībaizsardzības iestāžu spējas piekļūt digitālajai informācijai[14].

Augsta līmeņa grupa jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos savā noslēguma ziņojumā[15] uzsvēra, ka tiesībaizsardzības un tiesu iestādes pēdējo desmit gadu laikā ir zaudējušas pozīcijas noziedzniekiem, jo noziedznieki izmanto rīkus un produktus, ko nodrošina citas jurisdikcijas un pakalpojumu sniedzēji, kuri ir ieviesuši pasākumus, kas atņem minētajām iestādēm līdzekļus sadarbībai ar iestādēm, kas iesniedz likumīgus pieprasījumus atsevišķās krimināllietās. Tāpēc sistemātiska sadarbība starp tiesībaizsardzības iestādēm un privātā sektora personām, tai skaitā pakalpojumu sniedzējiem, ir būtiska turpmākajiem centieniem sagraut visvairāk apdraudošos noziedzīgos tīklus un personas Savienībā un ārpus tās.

Tā kā digitalizācija kļūst arvien izplatītāka un nodrošina noziedzniekiem arvien plašāku jaunu instrumentu avotu, ir būtiski izveidot tādu regulējumu piekļuvei datiem, kas atbilst vajadzībām panākt mūsu tiesību aktu izpildi un aizsargāt mūsu vērtības. Tajā pašā laikā, lai saglabātu

[11] Tas ir, tīkli, ko izmanto tiesībaizsardzības iestādes, robežsargi, muitas dienesti, civilā aizsardzība, ugunsdzēsēji, neatliekamās medicīniskās palīdzības sniedzēji un citi svarīgi sabiedriskās drošības un drošuma dalībnieki.

[12] ES infrastruktūra noturībai, savienojamībai un drošībai, izmantojot satelītu.

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019PC0070.

[15] Augsta līmeņa grupas jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos noslēguma ziņojums, 15.11.2024., 4802e306-c364-4154-835b-e986a9a49281_en.

kiberdrošību un aizsargātu pret jauniem drošības apdraudējumiem, vienlīdz svarīgi ir nodrošināt digitālo sistēmu drošību pret neatļautu piekļuvi. Minētajos piekļuves regulējumos ir jāievēro arī pamattiesības, cita starpā nodrošinot, ka privātums un personas dati ir pienācīgi aizsargāti.

Pēdējo gadu laikā ES ir rīkojusies, lai apkarotu **noziedzību tiešsaistē un atvieglotu piekļuvi digitālajiem pierādījumiem par visiem noziegumiem**, šajā nolūkā pieņemot elektronisko pierādījumu noteikumus, kas pilnībā tiks piemēroti, sākot ar 2026. gada augustu[16]. Tos papildinās starptautiski informācijas un pierādījumu apmaiņas instrumenti. Komisija drīzumā ierosinās parakstīt un noslēgt jauno **ANO Konvenciju pret kibernoziegumiem**.

Lai izpildītu augsta līmeņa grupas ieteikumus[17], Komisija 2025. gada pirmajā pusē nāks klajā ar **ceļvedi**, **kurā izklāstīti juridiskie un praktiskie pasākumi**, ko tā ierosina veikt, **lai nodrošinātu likumīgu un operatīvu piekļuvi datiem**. Veicot turpmākus pasākumus saistībā ar šo ceļvedi, Komisija par prioritāti noteiks **datu saglabāšanas noteikumu** ietekmes novērtējumu ES līmenī un **šifrēšanas tehnoloģiju ceļveža** sagatavošanu, lai apzinātu un novērtētu tehnoloģiskus risinājumus, kas ļautu tiesībaizsardzības iestādēm likumīgi piekļūt šifrētiem datiem un vienlaikus aizsargātu kiberdrošību un pamattiesības.

Operatīvā sadarbība

Komisija sadarbosies ar dalībvalstīm, ES aģentūrām un struktūrām un partnervalstīm, lai stiprinātu operatīvo sadarbību, kas ir būtiska rezultatīvākai pieejai cīņā pret transnacionālo organizēto noziedzību un terorismu.

Izmantojot **Eiropas daudzdisciplīnu platformu pret noziedzības draudiem (*EMPACT*)**, kas ir galvenais ES satvars kopīgai rīcībai pret smagu un organizētu noziedzību, ir sasniegti būtiski operatīvie rezultāti. Nākamais *EMPACT* cikls 2026.–2029. gadam sniedz iespēju vēl vairāk stiprināt šo satvaru. Lai sagrautu visvairāk apdraudošos noziedzīgos tīklus un personas, Savienībai ir jāracionalizē un jākoncentrē savi centieni uz vissteidzamāk īstenojamām prioritātēm, pastiprinot dalībvalstu saistības un nodrošinot resursu lietderīgu izmantošanu.

Šajā nolūkā Komisija sadarbosies ar Padomes prezidentvalstīm un dalībvalstīm, lai **maksimāli palielinātu *EMPACT* potenciālu un īstenotu galvenās prioritātes nākamajam *EMPACT* ciklam 2026.–2029. gadam.** Visās šajās prioritārajās jomās ir vajadzīgi izlūkdati par visvairāk apdraudošajiem noziedzīgajiem tīkliem, kopīgas izmeklēšanas un operatīvās darba grupas, kā arī spēcīga tiesu iestāžu reakcija, ieskaitot pieeju "seko naudai". Turklāt Savienībai ir jāvēršas pret noziedznieku īstenoto vervēšanu un iefiltrēšanos un jāstiprina daudzaģentūru un starptautiskā tiesībaizsardzības sadarbība un apmācība.

Komisija atbalstīs arī citus **tiesībaizsardzības pārrobežu operatīvās sadarbības veidus starp dalībvalstīm un Šengenas asociētajām valstīm**. Šengenas zonai bez kontroles pie iekšējām robežām ir nepieciešama cieša sadarbība un informācijas apmaiņa starp dalībvalstu tiesībaizsardzības iestādēm, lai nodrošinātu augstu iekšējās drošības līmeni. Pašlaik tiesībaizsardzības iestāžu darbinieki joprojām saskaras ar problēmām, uzraugot vai veicot steidzamus pasākumus pāri robežām[18], un hibrīddraudu apkarošanai ir vajadzīga arī pastiprināta

[16] Eiropas Parlamenta un Padomes Regula (ES) 2023/1543 (2023. gada 12. jūlijs) par Eiropas e-pierādījumu sniegšanas rīkojumiem un Eiropas e-pierādījumu saglabāšanas rīkojumiem e-pierādījumu gūšanai kriminālprocesā un brīvības atņemšanas sodu izpildei pēc kriminālprocesa, OV L 191, 28.7.2023.

[17] Padomes 2024. gada 12. decembra secinājumi par piekļuvi datiem efektīvas tiesībaizsardzības nolūkā https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/en/pdf.

[18] Kā ziņots Komisijas novērtējumā par dalībvalstu pasākumiem Padomes 2022. gada 9. jūnija Ieteikuma (ES) 2022/915 par operatīvo tiesībaizsardzības sadarbību īstenošanai (5909/25).

pārrobežu sadarbība. Būtu jāizveido **augsta līmeņa grupa jautājumos par tiesībaizsardzības operatīvās sadarbības nākotni**, lai izstrādātu kopīgu stratēģisku redzējumu.

Operatīva datu apmaiņa starp tiesībaizsardzības iestādēm ir arī būtiska rezultatīvai pārrobežu sadarbībai. Tiklīdz **sadarbspējas arhitektūra** būs izveidota, tā nodrošinās tiesībaizsardzības iestādēm un Eiropolam operatīvu piekļuvi būtiskai informācijai. Tajā pašā laikā ES un tās dalībvalstīm būtu jāpiešķir prioritāte divpusējai un daudzpusējai informācijas apmaiņai, juridiski un tehniski īstenojot **Prīme II regulu**[19] sadarbībā ar *eu-LISA* un Eiropolu. Tas ļaus droši un automatizēti apmainīties ar pirkstu nospiedumiem, DNS profiliem, transportlīdzekļu reģistrācijas datiem, sejas attēliem un policijas reģistru informāciju, izmantojot ES maršrutētājus. Valstu līmenī dalībvalstīm ir jāīsteno **Informācijas apmaiņas direktīva**[20], ar ko uzlabo informācijas apmaiņas kanālus netraucētai pārrobežu informācijas plūsmai, vienlaikus nodrošinot to integrāciju Savienības līmeņa sistēmās, piemēram, *SIENA*[21].

Rezultatīva pārrobežu sadarbība ir atkarīga arī no **vienotas ES tiesībaizsardzības kultūras** veicināšanas. Lai sasniegtu šo mērķi, būtiska nozīme ir kopīgām mācībām, izcilības centriem un mobilitātes programmām. Komisija pētīs, kā ES var vislabāk palīdzēt dalībvalstīm veikt iestāžu darbinieku apmācību, šim nolūkam izmantojot ***CEPOL*** kā ES tiesībaizsardzības apmācības aģentūru.

Robežu drošības stiprināšana

Ārējo robežu noturības un drošības stiprināšana ir būtiska, lai cīnītos pret hibrīddraudiem, piemēram, migrācijas izmantošanu par ieroci, kā arī novērstu to, ka apdraudētāji un preces nonāk ES, un rezultatīvi apkarotu pārrobežu noziedzību un terorismu. **Šengenas Informācijas sistēmu (*SIS*) ir plānots uzlabot** 2026. gadā, lai dalībvalstis, pamatojoties uz datiem, ko trešās valstis kopīgo ar Eiropolu, varētu ievadīt brīdinājumus par trešo valstu valstspiederīgajiem, arī ārvalstu kaujiniekiem teroristiem, kas iesaistīti terorismā un citos smagos noziegumos.

ES lielapjoma informācijas sistēmu uzlabota **sadarbspēja** nodrošinās dalībvalstīm būtisku informāciju par personām no trešām valstīm, kas šķērso vai plāno šķērsot ārējās robežas, un tas palīdzēs iestādēm izvērtēt nosacījumus, ar kādiem atļauj ieceļot dalībvalstu teritorijā[22]. Komisija turpinās cieši sadarboties ar dalībvalstīm un *eu-LISA*, lai ātri īstenotu šīs sistēmas, īpaši **ieceļošanas/izceļošanas sistēmu (IIS), Eiropas ceļošanas informācijas un atļauju sistēmu (*ETIAS*) un pārskatīto Vīzu informācijas sistēmu (VIS)**, lai nodrošinātu to netraucētu darbību un ieguvumus drošības jomā.

Lai vēl vairāk uzlabotu robežu drošību un stiprinātu ES sadarbību, ņemot vērā mainīgos apdraudējumus, **Komisija ierosinās pastiprināt *Frontex*.** Eiropas robežu un krasta apsardzes darbinieku skaitam laika gaitā būtu jātrīskāršojas līdz 30 000. Aģentūrai vajadzētu būt aprīkotai ar progresīvām uzraudzības un situācijas apzināšanās tehnoloģijām, arī ar izlūkdatiem, kas ir

[19] Eiropas Parlamenta un Padomes Regula (ES) 2024/982 (2024. gada 13. marts) par datu automatizētu meklēšanu un apmaiņu policijas sadarbībai un ar ko groza Padomes Lēmumus 2008/615/TI un 2008/616/TI un Eiropas Parlamenta un Padomes Regulas (ES) 2018/1726, (ES) 2019/817 un (ES) 2019/818 (Prīme II regula), OV L, 2024/982, 5.4.2024.

[20] Eiropas Parlamenta un Padomes Direktīva (ES) 2023/977 (2023. gada 10. maijs) par informācijas apmaiņu starp dalībvalstu tiesībaizsardzības iestādēm un ar ko atceļ Padomes Pamatlēmumu 2006/960/TI, OV L 134, 22.5.2023., 1.–24. lpp.

[21] Drošas informācijas apmaiņas tīkla lietojumprogramma.

[22] Proti, ieceļošanas/izceļošanas sistēma (IIS) ļaus dalībvalstīm identificēt trešo valstu valstspiederīgos pie Šengenas zonas ārējām robežām un reģistrēt viņu ieceļošanu un izceļošanu, lai varētu sistemātiski identificēt personas, kuras pārsniedz atļauto uzturēšanās termiņu. Pirms trešās valsts valstspiederīgā ierašanās pie ārējām robežām Eiropas ceļošanas informācijas un atļauju sistēma (*ETIAS*) un Vīzu informācijas sistēma (VIS) ļaus dalībvalstīm iepriekš novērtēt, vai trešās valsts valstspiederīgā klātbūtne ES teritorijā radītu drošības risku.

būtiski Eiropas integrētajai robežu pārvaldībai un piekļuvei stabiliem ES valdības sniegtiem Zemes novērošanas pakalpojumiem robežkontroles vajadzībām, kas jāizvērš līdz 2027. gadam. Tam būtu vēl vairāk jāuzlabo spēja atklāt, novērst un apkarot pārrobežu noziedzību pie ārējām robežām, kā arī jāpastiprina atbalsts dalībvalstīm atgriešanas īstenošanā, īpaši attiecībā uz trešo valstu valstspiederīgajiem, kas rada drošības risku.

Dokumentu un identitātes viltošana veicina migrantu kontrabandu, cilvēku tirdzniecību, noziedznieku slepenu pārvietošanos un nelikumīgu preču tirdzniecību. **Vairāku identitāšu detektors (*MID*)**[23] pēc tā darbības sākšanas uzlabos valstu iestāžu spēju identificēt personas, kuras izmanto vairākas identitātes, un apkarot identitātes viltošanu. Komisija pētīs veidus, kā uzlabot ES pilsoņiem un trešo valstu valstspiederīgajiem izsniegto ceļošanas un uzturēšanās dokumentu drošību. Turklāt Komisija novērtēs, kā ES digitālās identitātes maki, kas saskaņā ar Eiropas digitālās identitātes satvaru jāievieš līdz 2026. gada beigām, var palīdzēt uzlabot ceļošanas dokumentu drošību un identitātes verifikāciju. Tas papildinās priekšlikumus par digitālajiem ceļotāja identifikatoriem un *EU Digital Travel* lietotni[24].

Ceļošanas informācija ir būtiska iestādēm, lai identificētu un izmeklētu noziedznieku, teroristu un citu personu, kas rada draudus drošībai, pārvietošanos. Lai gan pastāv ES regulējums attiecībā uz komerciālo gaisa pārvadājumu informāciju[25], par citiem transporta veidiem saņemto datu apstrāde tiesībaizsardzības nolūkos ir sadrumstalota. Līdz ar to noziedznieki un teroristi var slepeni izmantot dažādus transporta veidus nelikumīgām darbībām. Komisija sadarbosies ar dalībvalstīm un transporta nozari, lai **stiprinātu ceļošanas informācijas sistēmu**, kas tiks veikts, izpētot Savienības shēmu, saskaņā ar kuru privāto lidojumu operatoriem jāvāc un jānosūta pasažieru dati, kā arī izvērtējot pasažieru datu reģistra apstrādes noteikumus un veidus, kā racionalizēt jūras ceļojumu informācijas apstrādi. Attiecībā uz autotransportu Komisija izvērtēs **automātiskās numura zīmes atpazīšanas (*ANPR*) sistēmu** plašāku izmantošanu un palielinās sinerģijas iespējas ar *SIS*.

Prognozēšana, inovācija un uz spējām balstīta pieeja

Komisija izstrādās **visaptverošu prognozēšanas pieeju attiecībā uz iekšējo drošību ES līmenī**, pamatojoties uz valstu līmenī apzināto paraugpraksi. Šī pieeja atbalstīs politikas veidošanu un virzīs investīcijas attiecīgajā ES finansētajā drošības izpētes un inovāciju jomā.

Pētniecībai un inovācijai ir izšķiroša nozīme iekšējā drošībā, jo tās rada risinājumus, lai novērstu jaunus apdraudējumus, kas rodas arī tehnoloģiju nepareizas izmantošanas dēļ[26]. ES ir jāturpina investēt inovatīvu rīku izstrādē drošības apdraudējumu novēršanai, izmantojot no ES budžeta finansētus drošības pētniecības un inovāciju projektus[27], vienlaikus ievērojot ES noteikumus un pamattiesības. Komisijai būtu jāatbalsta pāreja no pētniecības uz izvēršanu, lai nodrošinātu šo mūsdienīgo spēju sekmīgu ieviešanu, prioritāti piešķirot tādām **progresīvām tehnoloģijām** kā mākslīgais intelekts. Šai pieejai būtu jāietver apmācība, lai uzlabotu mākslīgā intelekta sistēmu un citu tehnisko spēju izmantošanu tiesībaizsardzības un tiesu iestādēs.

[23] *MID* ir viens no sadarbspējas komponentiem, kas ieviests ar Regulu (ES) 2019/818 un Regulu (ES) 2019/817.
[24] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5047.
[25] Pasažieru datu reģistra (PDR) un iepriekšējas pasažieru informācijas (IPI) regulējums, kas izveidots ar Direktīvu (ES) 2016/681 ("PDR direktīva") un Regulu (ES) 2025/12, Regulu (ES) 2025/13 ("IPI regulas").
[26] Sk. Komisijas Kopīgā pētniecības centra ziņojumu *"Emerging risks and opportunities for EU internal security stemming from new technologies"* (Jauni riski un iespējas ES iekšējai drošībai, kas izriet no jaunajām tehnoloģijām) https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] *Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025* (Pētījums par ES finansētas drošības pētniecības un inovācijas stiprināšanu – ES finansētas civilās drošības pētniecības un inovācijas 20 gadi – 2025. gads) https://data.europa.eu/doi/10.2837/0004501.

Turklāt attiecīgā gadījumā tehnoloģiju divējāda lietojuma potenciāls būtu jāizmanto abos virzienos (civilo tehnoloģiju izmantošana aizsardzībā un otrādi)[28].

ES Iekšējās drošības inovācijas centrs[29] – inovācijas laboratoriju tīkls, kas nodrošina jaunākos inovācijas atjauninājumus un iedarbīgus risinājumus iekšējās drošības dalībnieku darba atbalstam ES un dalībvalstīs – palīdzēs integrēt pētniecību praksē un politikā. Lai uzlabotu Eiropola darbības efektivitāti, ir jāstiprina tā rīku repozitorijs (*ETR*), kas Eiropolam dod iespēju identificēt, izstrādāt, kopīgi iepirkt un operatīvi izmantot progresīvas tehnoloģijas. Turklāt Komisija Kopīgajā pētniecības centrā izveidos **drošības pētniecības un inovācijas centru**, kas apvienos pētniekus, lai saīsinātu ciklu no pētniecības rezultātiem līdz inovācijai, izstrādei un sekmīgai īstenošanai, vienlaikus samazinot izstrādes, testēšanas un apstiprināšanas izmaksas.

Mūsu **Eiropas pētniecības telpa** pēc savas būtības ir sadarbīga, un tāpēc tajā ir iespējama ārvalstu iejaukšanās un dezinformācija. Pēc tam, kad Padome būs pieņēmusi ieteikumu par pētniecības drošību[30], Komisija un dalībvalstis veiks pasākumus, lai palielinātu attiecīgo dalībnieku spējas, cita starpā izveidojot pētniecības drošības ekspertīzes centru

Pamatdarbības

Komisija 2026. gadā pieņems:

- **tiesību akta priekšlikumu, lai pārveidotu Eiropolu par patiesi funkcionējošu tiesībaizsardzības aģentūru;**
- **tiesību akta priekšlikumu *Eurojust* stiprināšanai;**
- **tiesību akta priekšlikumu par *Frontex* lomas un uzdevumu pastiprināšanu;**
- **tiesību akta priekšlikumu par Eiropas kritisko sakaru sistēmas izveidi.**

Komisija:

- **2025. gadā nāks klajā ar ceļvedi, kurā izklāstīta turpmākā virzība uz likumīgu un operatīvu piekļuvi datiem tiesībaizsardzības nolūkos;**
- **2025. gadā sagatavos ietekmes novērtējumu, lai vajadzības gadījumā atjauninātu noteikumus par datu saglabāšanu ES līmenī;**
- **2026. gadā nāks klajā ar tehnoloģiju ceļvedi šifrēšanas jomā, lai apzinātu un novērtētu tehnoloģiskus risinājumus, kas ļautu tiesībaizsardzības iestādēm likumīgi piekļūt datiem;**
- **strādās, lai izveidotu augsta līmeņa grupu nolūkā stiprināt operatīvo sadarbību tiesībaizsardzības jomā**
- **2026. gadā izveidos drošības pētniecības un inovācijas centru Kopīgajā pētniecības centrā.**

Komisija sadarbībā ar dalībvalstīm un attiecīgajām ES aģentūrām:

- **stiprinās *EMPACT* arhitektūru;**
- **strādās, lai ātri ieviestu sadarbspējas arhitektūru un īstenotu Prīme II regulu;**
- **stiprinās ceļošanas informācijas sistēmu.**

Dalībvalstis tiek mudinātas:

- **transponēt un pilnībā īstenot Informācijas apmaiņas direktīvu**

[28] Kā noteikts *Niinistö* ziņojumā.
[29] ES Iekšējās drošības inovācijas centrs | Eiropols.
[30] OV C, C/2024/3510, 30.5.2024.

4. Noturība pret hibrīddraudiem un citām naidīgām darbībām

Mēs veidosim noturību pret hibrīddraudiem, uzlabojot kritiskās infrastruktūras aizsardzību, stiprinot kiberdrošību, uzlabojot transporta mezglu un ostu drošību un apkarojot draudus tiešsaistē.

Ir palielinājies tādu naidīgu darbību biežums un sarežģītība, kas apdraud ES drošību, un ļaunprātīgi aktori ir ievērojami paplašinājuši savu arsenālu. Ir pastiprinājušās hibrīdkampaņas, kas vērstas pret ES, tās dalībvalstīm un partneriem, un tās ietver sabotāžas aktus, kas vērsti pret kritisko infrastruktūru, dedzināšanu, kiberuzbrukumus, iejaukšanos vēlēšanās, ārvalstu iejaukšanos un manipulāciju ar informāciju (*FIMI*), arī dezinformāciju, un migrācijas izmantošana par ieroci. Ņemot vērā Savienības iestāžu, struktūru, biroju un aģentūru ("Savienības vienības") politisko un operatīvo lomu un apstrādātās informācijas raksturu, tās nav pasargātas no šādām darbībām.

ES ir **jāuzlabo sava noturība**, efektīvi jāizmanto pašreizējie instrumenti un jāizstrādā jauni veidi, kā stāties pretī šiem mainīgajiem draudiem, ko rada valstiski un nevalstiski aktori gan tagad, gan nākotnē.

Kritiskā infrastruktūra

Draudi **kritiskajai infrastruktūrai**, tai skaitā hibrīddraudi, piemēram, sabotāža un ļaunprātīgas kiberdarbības, rada nopietnas bažas, īpaši attiecībā uz infrastruktūru, kas savieno dalībvalstis – neatkarīgi no tā, vai tie ir enerģētikas savienotāji, pārrobežu sakaru kabeļi vai transporta tīkli. Kopš Krievijas agresijas kara pret Ukrainu ir palielinājies sabotāžas gadījumu skaits, kas vērsti pret kritisko infrastruktūru, īpaši 2024. gadā, un tas skar daudzas dalībvalstis. Sadarbība starp tiesībaizsardzības, drošības un kiberdrošības dienestiem, militāro un civilo aizsardzību un privātajiem operatoriem ir būtiska, lai efektīvi prognozētu, atklātu, novērstu šādas darbības un reaģētu uz tām.

Kritisko vienību neaizsargātības mazināšana un noturības stiprināšana ir obligāta, lai nodrošinātu ekonomikai un sabiedrībai vitāli svarīgu pamatpakalpojumu nepārtrauktu sniegšanu. Tāpēc šajā sakarā ir ļoti svarīgi, lai visas dalībvalstis laikus transponētu un pareizi īstenotu **Kritisko vienību noturības (*CER*) direktīvu**[31] un **Direktīvu, ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā (TID 2)**[32].

Lai nodrošinātu ātru virzību uz priekšu, Komisija sadarbībā ar **Kritisko vienību noturības grupu un TID sadarbības grupu** palīdzēs dalībvalstu kritisko vienību[33] apzināšanā un labas prakses apmaiņā par valstu stratēģijām un riska novērtējumiem attiecībā uz pamatpakalpojumiem. Ja rastos kritiskās infrastruktūras traucējumi ar būtisku pārrobežu ietekmi, ES līmeņa reakcijas koordinēšanai tiks izmantots **ES kritiskās infrastruktūras plāns**. Komisija mudina Padomi ātri pieņemt **ES kiberdrošības plānu**, kas vēl vairāk stiprinās koordināciju krīzes pārvarēšanas kontekstā, veicinot ciešāku sadarbību starp iestādēm fiziskās un digitālās noturības jomā. Pēc sekmīgiem enerģētikas nozares stresa testiem 2023. gadā Komisija veicinās **brīvprātīgus stresa testus** citās būtiskās iekšējās drošības nozarēs. Turklāt Komisija sniegs **Savienības līmeņa pārskatu par pārrobežu un pārnozaru riskiem**

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

[32] Eiropas Parlamenta un Padomes 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) .

[33] Direktīva aptver šādas nozares: enerģētika, transports, banku nozare, finanšu tirgus infrastruktūra, veselība, dzeramais ūdens, notekūdeņi, digitālā infrastruktūra, valsts pārvalde, kosmoss, pārtikas ražošana, pārstrāde un izplatīšana.

pamatpakalpojumiem, lai atbalstītu dalībvalstu riska novērtējumus un sniegtu informāciju visaptverošam ES līmeņa riska novērtējumam. Saskaņā ar Eiropas sagatavotības savienības stratēģiju Komisija sadarbosies ar dalībvalstīm, lai apzinātu citas nozares un pakalpojumus, uz kuriem neattiecas spēkā esošie tiesību akti un attiecībā uz kuriem varētu būt nepieciešams rīkoties.

ES un NATO darba grupa kritiskās infrastruktūras noturības jautājumos ir veicinājusi izcilu sadarbību paraugprakses apmaiņā un noturības uzlabošanā enerģētikas, transporta, digitālās infrastruktūras un kosmosa nozarēs. Šis darbs turpināsies **ES un NATO strukturētā dialoga par noturību** ietvaros. **ES hibrīddraudu novēršanas rīkkopa** piedāvā stabilu atbalstu dalībvalstīm un partneriem, ko tie var izmantot, gatavojoties hibrīddraudiem un tos apkarojot. **Hibrīddraudu novēršanas ātrās reaģēšanas vienības**[34] pēc pieprasījuma sniedz pielāgotu īstermiņa palīdzību dalībvalstīm, dažādām ES misijām un partneriem. Turklāt Komisija turpinās ES sadarbību sabotāžas apkarošanā, izmantojot ekspertu darbības[35], arī **īpašu kopīgu darba programmu**, lai racionalizētu informācijas apmaiņu un apzinātu pretpasākumus.

Incidenti, kas ietekmē **zemūdens kabeļus** Eiropā, liecina, ka ir vajadzīgi stingrāki pasākumi un skaidrāki risinājumi. Kā izklāstīts **ES kabeļu drošības rīcības plānā**[36], Komisija kopā ar Augsto pārstāvi sadarbosies ar dalībvalstīm, ES aģentūrām un tādiem partneriem kā NATO, lai novērstu un atklātu draudus zemūdens kabeļiem, reaģētu uz tiem un atturētu no tiem. Lai izstrādātu integrētu situācijas ainu par apdraudējumiem, Komisija sadarbosies ar dalībvalstīm, lai brīvprātīgi izstrādātu un ieviestu integrētu zemūdens kabeļu uzraudzības mehānismu katrā jūras baseinā, sākot ar Ziemeļvalstu/Baltijas reģionālo centru.

Kiberdrošība

Ļaunprātīgas kiberdarbības, kas bieži vien ir daļa no plašāka daudzdimensionālu draudu un hibrīddraudu klāsta, pastāvīgais raksturs prasa pastāvīgu uzmanību un rīcību Eiropas līmenī. Pēdējos gados Savienība ir pieņēmusi virkni kiberdrošības tiesību aktu, kas stiprina ES kritiskajās nozarēs darbojošos TID 2 vienību, kā arī Savienības vienību[37] kibernoturību, uzlabo digitālo produktu drošību (Kibernoturības akts) un izveido satvaru sagatavotības un reaģēšanas uz incidentiem atbalstam (Kibersolidaritātes akts). 2025. gada janvārī Komisija pieņēma **Eiropas rīcības plānu attiecībā uz slimnīcu un veselības aprūpes sniedzēju kiberdrošību**[38], lai uzlabotu draudu atklāšanu, sagatavotību krīzēm un reaģēšanu uz tām. Būtiska nozīme ir tā pilnīgai īstenošanai. Tajā pašā laikā, lai vērstos pret jauniem apdraudējumiem un norisēm, mums ir jāpastiprina savas darbības, īpaši tādās jomās kā informācijas apmaiņa, piegādes ķēdes drošība, izspiedējprogrammatūra un kiberuzbrukumi, kā arī tehnoloģiskā suverenitāte.

Turklāt īstenošanai ir jānovērš pašreizējais kiberdrošības prasmju trūkums 299 000 cilvēkiem. Komisija sadarbosies ar dalībvalstīm prasmju savienības ietvaros[39], lai paplašinātu kiberdrošības darbaspēku, jo īpaši, izmantojot jauno Kiberdrošības prasmju akadēmiju. *STEM*

[34] ES Stratēģiskais kompass drošībai un aizsardzībai (2022), 22. lpp.
[35] ES aizsardzības drošības padomdevēji, Eiropas Sprādzienbīstamu priekšmetu iznīcināšanas tīkls (*EEODN*), *ATLAS* tīkls, ES Augsta riska drošības tīkls (*EU HRSN*), *CBRN* drošības padomdevēja grupa, Kritisko vienību noturības grupa (*CERG*).
[36] JOIN (2025) 9 final.
[37] Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2023/2841 (2023. gada 13. decembris), kas paredz pasākumus nolūkā panākt vienādu augstu kiberdrošības līmeni Savienības iestādēs, struktūrās, birojos un aģentūrās, OV L, 2023/2841, 18.12.2023.
[38] https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM (2025) 90 final.

izglītības stratēģiskais plāns[40] palīdz uzlabot talantu plūsmu un Eiropas reakciju uz kiberdrošības darba tirgus vajadzībām.

Līdztekus noturības uzlabošanai ES turpinās pilnībā izmantot satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām (**Kiberdiplomātijas rīkkopa**), lai novērstu un nepieļautu kiberdraudus, ko rada valstiski un nevalstiski aktori, un reaģētu uz tiem.

IKT piegādes ķēžu drošība

5G kiberdrošības rīkkopa nodrošina attiecīgo satvaru 5G tīklu aizsardzībai, taču dalībvalstis to pašlaik nepietiekami īsteno. Joprojām pastāv nepieņemami drošības riski, īpaši attiecībā uz augsta riska pakalpojumu sniedzēju aizstāšanu. Saskaņota pieeja IKT piegādes ķēdes drošībai var novērst pašreizējo iekšējā tirgus sadrumstalotību, ko rada dažādas pieejas valstu līmenī, novērst kritisko atkarību un mazināt augsta riska piegādātāju radīto risku mūsu IKT piegādes ķēdēm, tādējādi uzlabojot mūsu kritiskās infrastruktūras drošību.

Saskaņā ar šo pieeju gaidāmajā **Kiberdrošības akta pārskatīšanā** Komisija plašāk aplūkos IKT piegādes ķēžu un infrastruktūras drošību un noturību. Turklāt Komisija ierosinās uzlabot **Eiropas kiberdrošības sertifikācijas satvaru**, lai nodrošinātu, ka turpmākās sertifikācijas shēmas var pieņemt savlaicīgi un reaģēt uz politikas vajadzībām.

Pamatojoties uz esošajiem vai notiekošajiem nozaru novērtējumiem[41], Komisija kopā ar dalībvalstīm izstrādās **koordinētu kiberdrošības riska novērtējumu stratēģisko plānošanu.**

Mākoņdatošanas un telesakaru pakalpojumi ir kļuvuši par pamatproduktu kritisko infrastruktūru, uzņēmumu un publisko iestāžu piegādes ķēdēs. Komisija rīkosies, lai mudinātu kritiskās vienības izvēlēties **mākoņpakalpojumus un telesakaru pakalpojumus, kas nodrošina pienācīgu kiberdrošības līmeni**, ņemot vērā ne tikai tehniskos, bet arī stratēģiskos riskus un atkarību.

Izspiedējprogrammatūra un kiberuzbrukumi

Joprojām liela problēma ES un pasaulē ir **izspiedējprogrammatūra** – vienā ziņojumā tiek lēsts, ka ar tām saistītās globālās gada izmaksas līdz 2031. gadam pārsniegs 250 miljardus EUR[42]. Gan **TID2 direktīva**, gan **Kibernoturības akts** ievērojami uzlabos vienību drošības pozīciju, jo padarīs izspiedējprogrammatūras tīklu uzbrukumu veikšanu dārgāku. Turklāt Komisija cieši sadarbosies ar dalībvalstīm, lai nodrošinātu, ka tiesībaizsardzības iestādēm tiek vairāk ziņots par izspiedējprogrammatūras uzbrukumiem, īpaši progresīviem pastāvīgiem draudiem, un izpirkuma maksas maksājumiem, tādējādi atvieglojot izmeklēšanu.

Lai novērstu un apturētu kiberuzbrukumus, Eiropola un ES Kiberdrošības aģentūras (*ENISA*) aizgādībā ES ir jāstiprina informācijas apmaiņa starp tiesībaizsardzības iestādēm, kiberdrošības iestādēm un subjektiem, kā arī privāto sektoru.

Eiropolam un *Eurojust* būtu jāturpina darbs, par pamatu izmantojot panākumus, ko šīs aģentūras ir guvušas izspiedējprogrammatūras operāciju apturēšanā, tādējādi atbalstot tiesībaizsardzības sadarbību. Šajā nolūkā tiesībaizsardzības iestādēm būtu maksimāli jāizmanto sadarbības mehānismi, arī **Eiropola starptautiskais modelis reaģēšanai uz izspiedējprogrammatūru** un **starptautiskā izspiedējprogrammatūras apkarošanas**

[40] COM (2025) 89 final.

[41] Piemēram, saistībā ar 5G tīkliem, telekomunikācijām, elektroenerģiju, atjaunīgo enerģiju un satīklotiem transportlīdzekļiem.

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

iniciatīva (*CRI*)[43], un *ENISA* un Eiropolam būtu jāsadarbojas, lai paplašinātu izspiedējprogrammatūras paveidu atšifrēšanas rīku repozitoriju[44].

Tehnoloģiskā suverenitāte

Kiberdrošība un tehnoloģiskā suverenitāte ir cieši saistītas, un prioritārā kārtā ir jāpievēršas tehnoloģiskajai atkarībai. Savienībai ir **jāvada jaunu tehnoloģiju izstrāde un ieviešana**, un Komisijai jāstrādā, lai **uzlabotu spējas tādās stratēģiskās tehnoloģijās** kā mākslīgais intelekts, kvantu sistēma, progresīva savienojamība, mākoņdatošana, perifērdatošana un lietu internets[45], izmantojot turpmākās iniciatīvas, piemēram, MI kontinenta rīcības plānu, Kvantu stratēģiju u. c.[46]. Komisija turpinās atbalstīt jaunāko pieejamo starptautiski saskaņoto **interneta protokolu** savlaicīgu izvēršanu, kas ir būtiski, lai uzturētu mērogojamu un efektīvu internetu ar paaugstinātu kiberdrošības līmeni. Ir vajadzīgas arī turpmākas darbības, lai risinātu **ar radiofrekvenču spektru saistītas problēmas**, piemēram, saistībā ar *GNSS* maldināšanu, traucēšanu, piegādes ķēdes riskiem un atkarību, piemēram, kvantu sensoru tehnoloģiju izmantošanu un radiofrekvenču uzraudzības spēju attīstības izpēti.

Pēckvantu kriptogrāfijas (*PQC*) risinājumu izvēršanai būs izšķiroša nozīme, lai aizsargātu sensitīvus sakarus, datus miera stāvoklī un aizsargātu digitālās identitātes jaunajā kvantu laikmetā. Pamatojoties uz 2024. gada Ieteikumu par koordinētu īstenošanas ceļvedi pārejai uz *PQC*[47], Komisija sadarbojas ar dalībvalstīm, lai veicinātu šo pāreju. Šajā sakarā dalībvalstīm būtu jāapzina augsta riska gadījumi kritiskajās vienībās un jānodrošina kvantu droša šifrēšana šiem augsta riska gadījumiem pēc iespējas drīzāk un ne vēlāk kā līdz 2030. gada beigām. Komisija arī sadarbojas ar dalībvalstīm un Eiropas Kosmosa aģentūru (EKA), lai Savienības drošas savienojamības programmas ***IRIS*²** ietvaros **izstrādātu un izvērstu Eiropas kvantiskās komunikācijas infrastruktūru (*EuroQCI*)**[48], kuras pamatā ir kvantu atslēgu izdalīšana (*QKD*). Abas iniciatīvas galu galā ļaus vienībām droši nosūtīt datus un glabāt informāciju.

Kvantu tehnoloģijām būs arī būtiska nozīme drošības lietojumprogrammās: kā daļa no **Kvantu stratēģijas** tiks izstrādāts **ceļvedis kvantiskai detektēšanai drošības lietojumprogrammās**. Tāpat Komisija strādā, lai nodrošinātu savu korporatīvo drošībai kritiski svarīgo sistēmu, tai skaitā klasificēto IT sistēmu, kvantizturību.

Uzņēmējdarbībai labvēlīgs kiberdrošības satvars

Gaidāmā Kiberdrošības akta pārskatīšana ir iespēja **vienkāršot ES kiberdrošības tiesību aktus** saskaņā ar Konkurētspējas kompasu. Komisija cieši sadarbosies ar dalībvalstīm, lai nodrošinātu TID 2 direktīvā, Kibernoturības aktā un Kibersolidaritātes aktā noteiktā horizontālā kiberdrošības satvara ātru, saskaņotu un uzņēmējdarbībai draudzīgu īstenošanu, veicinot vienkāršību un saskaņotību un izvairoties no kiberdrošības noteikumu sadrumstalotības vai dublēšanās ES un valstu tiesību aktos.

Lai nodrošinātu drošu piekļuvi tiešsaistes pakalpojumiem un stiprinātu digitālo drošību visā ES, **Eiropas digitālās identitātes regulējums** līdz 2026. gada beigām piedāvās visiem ES pilsoņiem un iedzīvotājiem uzticamus digitālās identitātes makus. Gaidāmais **Eiropas darījumdarbības maks** veicinās drošu pārrobežu mijiedarbību starp uzņēmumiem un valsts

[43] https://counter-ransomware.org/.
[44] Pieejams projektā *No More Ransom* https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] Piemēram, kopuzņēmums *EuropHPC* https://eurohpc-ju.europa.eu/index_en, Kvantu pamatiniciatīva Kvantu pamatiniciatīvas tīmekļa vietne | Kvantu pamatiniciatīva, 3C tīkli (COM(2024) 81 final) un ES kabeļu rīcības drošības plāns (JOIN(2025) 9 final).
[47] Ieteikums par koordinētas īstenošanas ceļvedi pārejai uz kvantizturīgu šifrēšanu | Eiropas digitālās nākotnes veidošana.
[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

pārvaldes iestādēm. Abi ir priekšnoteikumi uz datiem balstīta vienotā tirgus drošai un efektīvākai darbībai, kas tiks panākta, izmantojot tādus rīkus kā vienotā digitālā vārteja, e-rēķini, e-iepirkums un digitālā produkta pase.

Drošība internetā

Daži no nopietnākajiem hibrīddraudiem, kas apdraud cilvēku drošību un drošumu Eiropā un vēršas pret ES demokrātijas sfēru, notiek tiešsaistē. Šie draudi ietver nelikumīgas darbības un nelikumīgu saturu tiešsaistē, manipulācijas ar informāciju, kas ietver mākslīgu pastiprināšanu, maldinošu informāciju un ārvalstu īstenotu informācijas manipulāciju un iejaukšanos (*FIMI*).

Digitālo pakalpojumu akta (DPA) stingra izpilde ir ārkārtīgi svarīga, lai nodrošinātu drošu un pieejamu tiešsaistes vidi ar atbildīgiem dalībniekiem, kura ir noturīga arī pret hibrīddraudiem. DPA uzliek pienākumu ļoti lielu tiešsaistes platformu (*VLOP*) un ļoti lielu tiešsaistes meklētājprogrammu (*VLOSE)* nodrošinātājiem veikt riska novērtējumus un ieviest riska mazināšanas pasākumus attiecībā uz sistēmiskiem riskiem, kas izriet no to pakalpojumu izstrādes, darbības vai izmantošanas. Šādi riski var ietvert negatīvu ietekmi uz pilsonisko diskursu un vēlēšanu procesiem, kā arī uz sabiedrisko drošību, piemēram, ļaunprātīgu ārvalstu valsts aktoru tālejošu iejaukšanos, piemēram, vēlēšanu procesos. Ir svarīgi apmācīt dalībvalstu kompetentās iestādes par juridisko instrumentu izmantošanu, lai nekavējoties izņemtu nelikumīgu saturu tiešsaistē, īpaši attiecībā uz ar dzimumu saistītu kibervardarbību. DPA paredz mehānismu reaģēšanai krīzes situācijās, ko var aktivizēt, ja ārkārtēji apstākļi rada nopietnu apdraudējumu sabiedrības drošībai vai sabiedrības veselībai Savienībā vai nozīmīgā tās daļā. Lai papildinātu šo mehānismu, Komisija un valstu kompetentās iestādes, kas izraudzītas par digitālo pakalpojumu koordinatoriem, ir izstrādājušas arī brīvprātīgu **satvaru reaģēšanai uz DPA incidentiem**. Digitālo pakalpojumu koordinatori ir arī veikuši pasākumus, lai palīdzētu aizsargāt vēlēšanu integritāti, piemēram, organizējot vēlēšanu apaļā galda sanāksmes un stresa testus[49]. DPA kopā ar Politiskās reklāmas regulu[50] nodrošina vienu no vairākiem virzieniem, kas saistīti ar demokrātijas un demokrātisko procesu integritātes aizsardzību, kuri ir neaizsargāti pret naidīgu aktoru uzbrukumiem, arī izmantojot digitālos rīkus un sociālos medijus.

Vēl viens svarīgs komponents, kas piedāvā būtisku atbalstu ES līmenī, ir ***FIMI*** rīkkopas īstenošana. Šajos centienos būtiska nozīme ir arī digitālās un medijpratības un kritiskās domāšanas atbalstam[51].

Cīņa pret migrācijas izmantošanu par ieroci

Krievija ar Baltkrievijas palīdzību un būtisku atbalstu ir mērķtiecīgi izmantojusi migrāciju par ieroci un nelikumīgi veicinājusi migrācijas plūsmas uz ES ārējām robežām, lai destabilizētu mūsu sabiedrību un grautu Eiropas Savienības vienotību. Tas apdraud ne tikai dalībvalstu drošību un suverenitāti, bet arī Šengenas zonas drošību un integritāti, kā arī visas Savienības drošību. 2024. gada oktobrī pieņemtajos secinājumos Eiropadome uzsvēra, ka ne Krievijai, ne Baltkrievijai, ne jebkurai citai valstij nedrīkst atļaut aizskart mūsu vērtības, tai skaitā tiesības uz patvērumu, un graut mūsu demokrātiju.

Kā norādīts Komisijas 2024. gada paziņojumā par migrācijas izmantošanu par ieroci, Savienība papildus spēcīgam politiskajam atbalstam ir veikusi finansiālus, operatīvus un diplomātiskus

[49] DPA vēlēšanu rīkkopa digitālo pakalpojumu koordinatoriem, 2025. gadshttps://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.

[50] Eiropas Parlamenta un Padomes Regula (ES) 2024/900 (2024. gada 13. marts) par politiskās reklāmas pārredzamību un mērķorientēšanu, OV L, 2024/900, 20.3.2024.

[51] Digitālās izglītības rīcības plāns (2021–2027) – Eiropas izglītības telpa.

pasākumus, ieskaitot sadarbību ar izcelsmes un tranzīta valstīm, lai efektīvi novērstu šos draudus[52]. Šī reakcija ietver Padomes izveidotā jaunā satvara izmantošanu, lai, nosakot aktīvu iesaldēšanu un ceļošanas aizliegumus, sodītu personas un organizācijas, kas iesaistītas tādās darbībās un politikā kā Krievijas veiktā migrācijas izmantošana par ieroci[53]. ES vajadzības gadījumā turpinās izmantot šo satvaru un atbalstīs dalībvalstis šā apdraudējuma novēršanā.

Transporta drošība

Jūras ostas, lidostas un sauszemes infrastruktūra ir izšķiroši svarīgi ieejas un izejas punkti. Tiem ir būtiska nozīme ES ekonomikā un sabiedrībā, kā arī militārajā mobilitātē. Tomēr šie transporta mezgli un līdzekļi ir arī vieni no galvenajiem mērķiem, pret kuriem vērsti ārēji draudi un noziedzīgas darbības. Nesenie incidenti, tai skaitā aviācijas kravu drošības pārkāpumi un uzbrukumi dzelzceļa infrastruktūrai, liecina par nopietniem riskiem. **Pārvadātāji** var būt gan mērķi, gan instrumenti ļaunprātīgiem aktoriem. Spēkā esošie ES juridiskie instrumenti ir uzlabojuši aviācijas drošību[54], tomēr augstais civilās aviācijas apdraudējuma līmenis prasa līdzekļus, kas ļautu paredzēt incidentus un ātri apspriesties ar attiecīgajām dalībvalstīm. Komisija sadarbosies ar dalībvalstīm, lai grozītu spēkā esošos īstenošanas tiesību aktus aviācijas drošības jomā nolūkā apmainīties ar klasificētu informāciju par **atgadījumiem aviācijas drošības jomā**. Turklāt Komisija apsvērs **regulatīvus pasākumus**, lai novērstu jaunus apdraudējumus, piemēram, **gaisa kravu incidentus**, un pastiprinātu aviācijas drošības standartus. Tas ietvers arī **aviācijas drošības tiesību aktu (*AVSEC)***, lai nodrošinātu tūlītējus reaģēšanas pasākumus, vienlaikus saglabājot vienas pieturas drošības zonu ES lidostās.

Izstrādājot gaidāmo **ES ostu stratēģiju**, pamatojoties uz **ES Ostu aliansi**, Komisija pētīs veidus, kā vēl vairāk stiprināt jūras drošības tiesību aktus, lai efektīvi novērstu jaunus apdraudējumus, nodrošinātu ostas un uzlabotu ES piegādes ķēdes drošību. Šajā nolūkā Komisija nodrošinās tās stingru īstenošanu un strādās, lai saskaņotu valstu praksi un pastiprinātu iepriekšējās darbības pārbaudes ostās. Papildus gaisa kravu drošības protokoliem Komisija sadarbosies ar dalībvalstīm un privāto sektoru, lai paplašinātu šos protokolus nolūkā uzlabot jūras transporta ķēžu drošību.

Lai palīdzētu dalībvalstīm novērst to, ka ļaunprātīgi aktori izmanto starptautiskās piegādes ķēdes, ierosinātais ES Muitas dienests analizēs un novērtēs riskus, pamatojoties uz **muitas informāciju**, kas saistīta ar precēm, kuras ieved ES, izved no tās un ved tranzītā. Saskaņā ar ES Jūras drošības stratēģiju[55] gaidāmajam **Eiropas Okeānu paktam** būs būtiska nozīme jūras drošības stiprināšanā jūras baseinos ap ES un ārpus tās, arī veicinot daudzfunkcionālu jūras operāciju un mācību izvēršanu.

Piegādes ķēžu noturība

Eiropai ir jāsamazina atkarība no trešo valstu tehnoloģijām, kas var radīt atkarības un drošības riskus. Komisijas mērķis ir mazināt atkarību no atsevišķiem ārvalstu piegādātājiem, mazināt risku, ko augsta riska piegādātāji rada mūsu piegādes ķēdēm, un nodrošināt kritisko infrastruktūru un rūpnieciskās spējas ES teritorijā, kā norādīts **Konkurētspējas kompasā[56]** un **tīras rūpniecības kursā[57]**. Komisija veicinās **rūpniecības politiku iekšējās drošības jomā**,

[52] COM (2024) 570 final.
[53] Padomes Regula (ES) 2024/2642 (2024. gada 8. oktobris) par ierobežojošiem pasākumiem saistībā ar Krievijas veiktajām destabilizējošajām darbībām, ST/8744/2024/INIT, OV L, 2024/2642, 9.10.2024.
[54] Eiropas Parlamenta un Padomes Regula (EK) Nr. 300/2008 (2008. gada 11. marts) par kopīgiem noteikumiem civilās aviācijas drošības jomā, OV L 97, 9.4.2008., 72.–84. lpp.
[55] JOIN (2023) 8 final.
[56] COM (2025) 30 final.
[57] COM (2025) 85 final.

sadarbojoties ar ES rūpniecību galvenajās nozarēs (piemēram, transporta mezgli, kritiskā infrastruktūra), lai ražotu drošības risinājumus, piemēram, atklāšanas iekārtas, biometriskās tehnoloģijas un dronus, kuros iekļauti integrēti drošības elementi. **Pārskatot ES iepirkuma noteikumus**, Komisija novērtēs, vai 2009. gada Aizsardzības un drošības iepirkuma direktīvā[58] paredzētie drošības apsvērumi ir pietiekami, lai apmierinātu tiesībaizsardzības un kritisko vienību noturības vajadzības.

Komisija atbalstīs dalībvalstis **ārvalstu tiešo ieguldījumu (ĀTI)** un loģistikas centru aprīkojuma iepirkuma izvērtēšanā, lai nodrošinātu, ka kritiskā infrastruktūra un tehnoloģijas joprojām ir drošas.

Kad **Iekšējā tirgus ārkārtējā stāvokļa un noturības akts (ITĀSNA)** būs stājies spēkā, tas palīdzēs ES pārvarēt krīzes, kas traucē kritiski svarīgas piegādes ķēdes un preču un pakalpojumu brīvu apriti un personu brīvu pārvietošanos. Tas ļaus ātri koordinēt krīzi, identificēt krīzes gadījumā būtiskas preces un pakalpojumus un nodrošinās rīkkopu to pieejamības nodrošināšanai. Turklāt ciešā sadarbībā ar dalībvalstīm Komisija ierosinās izveidot **daudzaģentūru transporta un piegādes ķēdes drošības brīdināšanas mehānismu**, lai garantētu drošu un savlaicīgu apmaiņu ar attiecīgo informāciju, kas vajadzīga draudu prognozēšanai un novēršanai.

Turklāt, īstenojot Kritiski svarīgo izejvielu aktu un Neto nulles emisiju industrijas aktu, ilgtspējas, noturības un Eiropas priekšrokas kritēriju plašāka izmantošana ES publiskajā iepirkumā veicinās pirmtirgu attīstību. Pastiprinātas tirdzniecības saites, piemēram, izmantojot izejvielu partnerības un tīras tirdzniecības un investīciju partnerības, palīdzēs dažādot piegādes ķēdes.

Noturība un sagatavotība ķīmiskiem, bioloģiskiem, radioloģiskiem un nukleāriem draudiem

Krievijas agresijas karš pret Ukrainu ir palielinājis **ķīmisko, bioloģisko, radioloģisko un nukleāro draudu (*CBRN*)** risku. Lai risinātu jautājumu par *CBRN* materiālu iespējamo iegādi un izmantošanu par ieroci, Komisija ar īpašu apmācību un mācībām atbalstīs dalībvalstis un partnervalstis. Komisija arī uzlabos *CBRN* sagatavotību un reaģēšanas spējas, nosakot prioritāros apdraudējumus, inovācijas finansējumu pretpasākumiem, *rescEU* spējas un medicīnisko pretlīdzekļu krājumu veidošanu saskaņā ar jaunu ***CBRN* sagatavotības un reaģēšanas rīcības plānu**. Turklāt **ES Medicīnisko pretpasākumu stratēģija** atbalstīs medicīnisko pretlīdzekļu izstrādi no pētniecības līdz ražošanai un izplatīšanai, lai aizsargātu ES no pandēmijām un *CBRN* apdraudējumiem.

Pamatojoties uz *Covid*-19 pandēmijas pieredzi, ES ir nostiprinājusi veselības drošības satvaru[59]. Komisija izraugās ES references laboratorijas sabiedrības veselības jomā, lai stiprinātu ES un valstu uzraudzības un ātras atklāšanas spējas. 2025. gadā tiks publicēts Savienības plāns par sagatavotību, profilaksi un reaģēšanu veselības drošības jomā.

Pamatdarbības

Komisija:

- **2025. gadā pārskatīs un pārstrādās Kiberdrošības aktu;**
- **izstrādās pasākumus, lai nodrošinātu mākoņdatošanas pakalpojumu kiberdrošu izmantošanu;**

[58] Direktīva 2009/81/EK, ar kuru koordinē procedūras attiecībā uz to, kā līgumslēdzējas iestādes vai subjekti, kas darbojas drošības un aizsardzības jomā, piešķir noteiktu būvdarbu, piegādes un pakalpojumu līgumu slēgšanas tiesības, OV L 216, 20.8.2009.

[59] Īpaši ar Regulu (ES) 2022/2371 par nopietniem pārrobežu veselības apdraudējumiem.

- **2025. gadā ierosinās ES ostu stratēģiju;**
- **2026. gadā pārskatīs ES iepirkuma noteikumus aizsardzības un drošības jomā;**
- **2026. gadā nāks klajā ar jaunu *CBRN* sagatavotības un reaģēšanas rīcības plānu.**

Komisija sadarbībā ar dalībvalstīm:

- **izstrādās un izvērsīs Eiropas kvantiskās komunikācijas infrastruktūru (*EuroQCI*);**
- **nodrošinās Digitālo pakalpojumu akta rezultatīvu izpildi;**
- **strādās, lai novērstu migrācijas izmantošanu par ieroci;**
- **izveidos aviācijas drošības atgadījumu sistēmu;**
- **strādās, lai izveidotu daudzaģentūru transporta un piegādes ķēdes drošības brīdināšanas mehānismu.**

Padome tiek mudināta:

- **pieņemt Padomes ieteikumu par ES kiberdrošības plānu**

Dalībvalstis tiek mudinātas:

- **transponēt un pilnībā īstenot *CER* un TID 2 direktīvu**

5. Tīkla smagās un organizētas noziedzības apkarošanai stiprināšana

Mēs palīdzēsim izskaust organizēto noziedzību, ierosinot stingrākus noteikumus organizētās noziedzības grupējumu apkarošanai, arī attiecībā uz izmeklēšanām, lai padarītu jauniešus ES mazāk neaizsargātus pret vervēšanu noziedzībā, un pastiprināsim pasākumus, lai liegtu piekļuvi noziedzības rīkiem un līdzekļiem.

Organizētā noziedzība izmanto mainīgo vidi un eksponenciāli vairojas. Tā gūst labumu no progresīvām tehnoloģijām, darbojas vairākās jurisdikcijās un tai ir ciešas saiknes ārpus ES robežām. Ņemot vērā šos sarežģītos un transnacionālos apdraudējumus, ļoti svarīga ir ES līmeņa koordinācija un atbalsts.

Noziedzības novēršana

Jauniešu vervēšana organizētajā noziedzībā Eiropas Savienībā rada arvien lielākas bažas. Lai apkarotu organizēto noziedzību, ir jānovērš tās **pamatcēloņi**, piedāvājot izglītību un alternatīvas noziedzības dzīvei, izmantojot visas sabiedrības pieeju. Komisija atbalstīs drošības apsvērumu integrēšanu ES izglītības, sociālajā, nodarbinātības un reģionālajā politikā. ES **veicinās uz pierādījumiem balstītu noziedzības novēršanas politiku**[60], kas pielāgota vietējiem apstākļiem.

Lai aizsargātu tiešsaistes pakalpojumu saņēmējus, īpaši nepilngadīgos, cita starpā no seksuālas vardarbības pret bērniem, cilvēku tirgotājiem un vervēšanas tiešsaistē noziedzības vai vardarbīga ekstrēmisma nolūkā, pasākumi saskaņā ar **Digitālo pakalpojumu aktu** paredz, ka nepilngadīgajiem pieejamu tiešsaistes platformu nodrošinātājiem ir jāpārvalda riski un jāreaģē uz nelikumīgu saturu, arī uz naida runu. Komisija plāno izdot **pamatnostādnes par nepilngadīgo aizsardzību**, lai palīdzētu tiešsaistes platformu nodrošinātājiem nodrošināt augsta līmeņa privātumu, drošumu un drošību nepilngadīgajiem tiešsaistē. Pamatnostādnes ietvers ieteikumu kopumu visiem digitālajiem pakalpojumiem, kas darbojas Savienībā, lai uzlabotu nepilngadīgo aizsardzību tiešsaistē. 2025. gadā Komisija plāno arī veicināt ES **privātuma aizsardzības vecuma apstiprināšanas** risinājumu, kas novērsīs šo trūkumu pirms

[60] https://www.eucpn.org/.

EUDI maka piedāvāšanas 2026. gada beigās. Komisija arī nāks klajā ar rīcības plānu cīņai pret iebiedēšanu tiešsaistē.

Turklāt Komisija turpinās atbalstīt daudzu ieinteresēto personu brīvprātīgu iesaisti sadarbībā ar tiešsaistes platformām un citiem attiecīgiem dalībniekiem, arī izmantojot ES Interneta forumu un mērķtiecīgus rīcības kodeksus saskaņā ar Digitālo pakalpojumu aktu, piemēram, 2025. gada Rīcības kodeksu cīņai pret nelikumīgiem naidīgiem izteikumiem tiešsaistē. Mērķis ir palielināt informētību, kopīgi reaģēt uz pašreizējiem un jauniem apdraudējumiem, kā arī sagatavot labu praksi ietekmes mazināšanas pasākumu jomā un dalīties ar to.

Vietējā līmenī organizētās noziedzības ietekme liecina, ka ir vajadzīgi reģionāli risinājumi, lai mazinātu neaizsargātību un nelikumīgu darbību pievilcību. ES programma pilsētām pievērsīsies drošības problēmām pilsētās, pamatojoties uz iniciatīvu "ES pilsētas pret radikalizāciju". Komisija atbalstīs dalībvalstis pilsētu un reģionālās drošības uzlabošanā, izmantojot Eiropas Reģionālās attīstības fondu.

Spēcīgāki izglītības pamati un prasmes ir noturīgas un saliedētas sabiedrības pamatā. Izmantojot **prasmju savienību** un **Integrācijas un iekļaušanas rīcības plānu**, Savienība strādās, lai palīdzētu cilvēkiem kļūt noturīgākiem pret maldinošu informāciju un dezinformāciju, radikalizāciju un vervēšanu noziedzībā.

Bērnu aizsardzība pret visu veidu vardarbību, arī noziedzību, fizisku vai garīgu vardarbību, tiešsaistē tāpat kā bezsaistē, ir viens no ES pamatmērķiem. Lai risinātu īpašās vajadzības, kas ir īpaši neaizsargātām grupām, piemēram, bērniem, kuri arvien vairāk pakļauti vervēšanai un radikalizācijai, iedraudzināšanai un seksuālai vardarbībai pret bērniem, kiberiebiedēšanai, dezinformācijai un citiem draudiem, ES izstrādās **rīcības plānu bērnu aizsardzībai pret noziedzību**, un tas aptvers tiešsaistes un bezsaistes dimensiju. Tajā tiks izklāstīta saskaņota un koordinēta pieeja, kuras pamatā ir pieejamie satvari un instrumenti, tai skaitā topošais ES centrs seksuālas vardarbības pret bērniem novēršanai un apkarošanai un citas ES struktūras un aģentūras, un tiks ierosināti veidi, kā virzīties uz priekšu jomās, kurās joprojām pastāv nepilnības.

Noziedzīgo tīklu un to veicinātāju likvidēšana

Ir jāpastiprina cīņa pret augsta riska noziedzīgajiem tīkliem, vadoņiem un veicinātājiem. Lai gan nesenie panākumi ir ievērojami[61], novecojuši noteikumi un nekonsekventas noziedzīgu tīklu definīcijas kavē efektīvu krimināltiesisko reaģēšanu un pārrobežu sadarbību. Komisija pārskatīs novecojušus tiesību aktus šajā jomā un ierosinās atjaunināt **regulējumu organizētās noziedzības jomā**, lai stiprinātu reaģēšanu.

Kā liecina *EPPO* un Eiropas Birojs krāpšanas apkarošanai (*OLAF*), administratīvā izpilde var papildināt tiesībaizsardzību ātrāku rezultātu gūšanai, vēršoties pret **pārrobežu krāpšanu un noziegumiem pret ES finanšu interesēm**. Subsīdiju krāpnieki koncentrējas uz tādām nozarēm kā atjaunīgā enerģija, pētniecības programmas un lauksaimniecības nozare[62]. Komisija pētīs veidus, kā koordinēt krimināltiesību un administratīvo instrumentu izmantošanu, uzlabojot sadarbību ar Eiropolu, *Eurojust* un *EPPO*. Komisija arī turpinās atbalstīt **administratīvās pieejas** plašāku piemērošanu, lai vietējām un citām administratīvajām iestādēm dotu iespēju novērst noziedznieku iefiltrēšanos[63].

[61] Ieskaitot nesenās *EMPACT* lietas.
[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

ES strādā, lai stiprinātu savu tiesisko regulējumu **korupcijas**[64] apkarošanai. Eiropas Parlamentam un Padomei būtu ātri jāpabeidz sarunas par Komisijas ierosināto atjaunināto pretkorupcijas regulējumu. Komisija nāks klajā ar ES pretkorupcijas stratēģiju, lai veicinātu integritāti un stiprinātu koordināciju starp visām attiecīgajām iestādēm un ieinteresētajām personām šajā jomā.

Šaujamieroči ir viens no galvenajiem faktoriem, kas veicina organizētās noziedzības grupējumu pieaugošo vardarbību. Komisija ierosinās kopējus krimināltiesību standartus attiecībā uz šaujamieroču nelikumīgu tirdzniecību. Jaunajā **ES rīcības plānā cīņai pret šaujamieroču nelikumīgu tirdzniecību** galvenā uzmanība tiks pievērsta likumīgā tirgus aizsardzībai, noziedzīgu darbību ierobežošanai, pamatojoties uz labākiem izlūkdatiem un starptautiskās sadarbības stiprināšanu, īpašu uzmanību pievēršot Ukrainai un Rietumbalkāniem.

Ir vajadzīgi pasākumi, lai uzlabotu profilaksi attiecībā uz nelikumīgi tirgotiem pirotehnikas izstrādājumiem, ko izmanto noziegumos, un to izsekojamību. Komisija pašlaik izvērtē pirotehnikas direktīvu un apsvērs arī **krimināLsodus par pirotehnikas izstrādājumu nelikumīgu tirdzniecību**.

Naudas plūsmas izsekošana

Naudas plūsmas izsekošanai ir izšķiroša nozīme organizētās noziedzības un terorisma apkarošanā, tomēr tā joprojām ir ļoti sarežģīta. Saikne starp organizēto noziedzību un naudas plūsmām prasa intensīvus un apvienotus centienus, lai apturētu noziedzīgo tīklu piekļuvi finansējuma avotiem un labāk aizsargātu cilvēkus, uzņēmumus un publiskos budžetus.

ES ir pastiprinājusi savus centienus ar jaunajiem nelikumīgi iegūtu līdzekļu legalizēšanas novēršanas noteikumiem, arī izveidojot **ES Iestādi nelikumīgi iegūtu līdzekļu legalizēšanas novēršanai (*AMLA*)**[65]. Sadarbība starp *AMLA*, *OLAF*, *EPPO*, *Eurojust* un Eiropolu ir būtiska, lai īstenotu efektīvu finanšu izmeklēšanu. Komisija atbalstīs **partnerību** izveidi – gan to, kuras veicina aģentūru sadarbību, gan to, kurās iesaistīts privātais sektors.

Lai likvidētu organizētās noziedzības finansiālos motīvus, ir būtiski uzlikt arestu aktīviem un konfiscēt noziedzīgi iegūtus līdzekļus. Nesen pieņemtie stingrākie noteikumi par **aktīvu atgūšanu un konfiskāciju**[66] dalībvalstīm būtu nekavējoties jātransponē un pilnībā jāizmanto to potenciāls. Lai cīnītos pret paralēlām finanšu sistēmām, arī uz kriptogrāfiskām tehnoloģijām balstītām sistēmām, kas apiet ES nelikumīgi iegūtu līdzekļu legalizēšanas novēršanas regulējumu, ir vajadzīgas arī inovatīvas darbības, paraugprakses apmaiņa starp dalībvalstīm un lielāks Eiropola un *Eurojust* atbalsts. Komisija izpētīs jaunas ES mēroga sistēmas iespējamību, lai izsekotu organizētās noziedzības gūto peļņu un teroristu finansēšanu, kā arī veicinās savlaicīgu un paplašinātu informācijas plūsmu no **finanšu izlūkošanas vienībām** uz tiesībaizsardzības iestādēm. Komisija pētīs veidus, kā novērst nepilnības, atbalstīt dalībvalstis spēju veidošanā un turpinās darbu, lai stiprinātu sadarbību ar trešām valstīm, ko noziedznieki ļaunprātīgi izmanto pagrīdes banku operācijās.

[64] Priekšlikums – Eiropas Parlamenta un Padomes Direktīva par korupcijas apkarošanu, ar ko aizstāj Padomes Pamatlēmumu 2003/568/TI un Konvenciju par Eiropas Kopienu ierēdņu vai Eiropas Savienības dalībvalstu ierēdņu korumpētības apkarošanu un ar ko groza Eiropas Parlamenta un Padomes Direktīvu (ES) 2017/1371, COM(2023) 234 final, Briselē, 3.5.2023.

[65] https://www.amla.europa.eu/index_en.

[66] Eiropas Parlamenta un Padomes Direktīva (ES) 2024/1260 (2024. gada 24. aprīlis) par aktīvu atgūšanu un konfiskāciju, OV L, 2024/1260, 2.5.2024.

Smagu noziegumu apkarošana

Papildus noziedzīgo tīklu likvidēšanai smagu noziegumu apkarošanai ir vajadzīgi mērķtiecīgi centieni. Lai stiprinātu mūsu spēju apkarot **krāpšanu tiešsaistē**, kas rada ļoti būtisku finansiālu kaitējumu[67], Komisija atbalstīs preventīvus pasākumus un iedarbīgākus tiesībaizsardzības pasākumus un sadarbosies ar dalībvalstīm un ieinteresētajām personām, lai atbalstītu un aizsargātu cietušos, arī palīdzot atgūt viņu līdzekļus. Šie centieni tiks **formalizēti rīcības plānā cīņai pret krāpšanu tiešsaistē.**

Pamatojoties uz ES 2020.–2025. gada stratēģiju **seksuālas vardarbības pret bērniem**[68] apkarošanai, Komisija atbalstīs likumdevējus abu tiesību aktu priekšlikumu[69] izstrādē, lai novērstu un apkarotu seksuālu vardarbību pret bērniem tiešsaistē un padarītu iedarbīgākus tiesībaizsardzības pasākumus pret seksuālu vardarbību pret bērniem un bērnu seksuālu izmantošanu. Tā kā pagaidu noteikumi ir spēkā līdz 2026. gada aprīlim, ir būtiski izveidot pastāvīgu tiesisko regulējumu, un Komisija mudina likumdevējus sākt sarunas par projektu regulai, ar ko paredz noteikumus seksuālas vardarbības pret bērniem novēršanai un apkarošanai. Likumdevēji tiek arī aicināti virzīties uz priekšu sarunās par Direktīvu par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un materiālu, kuros atspoguļota seksuāla vardarbība pret bērniem, apkarošanu, ar kuru tiks noteikti minimālie noteikumi noziedzīgu nodarījumu un sodu definēšanai bērnu seksuālās izmantošanas jomā.

Puse no ES bīstamākajiem noziedzīgajiem tīkliem ir iesaistīta vardarbīgā **narkotiku tirdzniecībā**. Lai gan ES nesen ir pastiprinājusi cīņu pret šo noziegumu[70], jo īpaši, paplašinot **ES Narkotiku aģentūras** pilnvaras, ir vajadzīgas turpmākas darbības. Komisija cieši sadarbosies ar dalībvalstīm, lai ierosinātu jaunu **ES stratēģiju narkotiku jomā**. Tā arī pārskatīs **tiesisko regulējumu par narkotisko vielu prekursoriem** un ierosinās **ES rīcības plānu narkotiku tirdzniecības apkarošanai**, lai sagrautu maršrutus un darbības modeļus. **ES Ostu alianses publiskā un privātā sektora partnerība** ostu aizsardzības pastiprināšanas jomā tiks paplašināta, iekļaujot mazākas un iekšzemes ostas un nodrošinot jūras drošības noteikumu izpildi. Atzīstot narkotiku tirdzniecības smago vietējo ietekmi, Komisija turpinās atbalstīt līdzsvarotu, uz pierādījumiem balstītu un daudzdisciplīnu narkotiku apkarošanas politiku, kas ir gatava narkotisko vielu, it īpaši sintētisko opioīdu, pēkšņam pieplūdumam.

Lai apkarotu cilvēku ekspluatāciju, ES ir pieņēmusi jaunus noteikumus[71] un ieviesīs **atjauninātu ES stratēģiju cilvēku tirdzniecības apkarošanai** (2026.–2030. gadam), kas aptver visus posmus no novēršanas līdz kriminālvajāšanai, galveno uzmanību pievēršot cietušo atbalstam gan ES, gan starptautiskā līmenī.

Cīņā pret **migrantu kontrabandu** Komisija vadīs centienus ar galvenajiem partneriem, izmantojot jauno Globālo aliansi migrantu kontrabandas apkarošanai sadarbībā ar Eiropolu, *Eurojust* un *Frontex*, arī tiešsaistes dimensijā. Komisijas priekšlikumi par kontrabandas apkarošanu[72] būtu jāpieņem un jāīsteno nekavējoties. Turklāt Komisija pēc **pārvadātāju rīkkopas**[73] pieņemšanas ir palielinājusi saziņu ar ārvalstu iestādēm un ekspluatantiem un

[67] *Global Anti-Scam Report 2024* (2024. gada globālais krāpniecības apkarošanas ziņojums).
[68] COM (2020) 607 final
[69] COM (2022) 209 final un COM (2024) 60 final.
[70] COM (2023) 641 final.
[71] Direktīva (ES) 2024/1712 (2024. gada 13. jūnijs), ar ko groza Direktīvu 2011/36/ES par cilvēku tirdzniecības novēršanu un apkarošanu un cietušo aizsardzību (OV L, 2024/1712, 24.6.2024.)
[72] COM (2023) 755 final un COM (2023) 754 final.
[73] Instrumentu kopums pret komercpārvadājumu ļaunprātīgu izmantošanu neatbilstīgai migrācijai uz ES.

turpinās sadarboties ar aviācijas nozari un civilās aviācijas organizācijām[74] palielinātu informētību par migrantu kontrabandu pa gaisu.[75].

Noziegumi pret vidi ilgtermiņā apdraud vidi, sabiedrības veselību un ekonomiku. Komisija atbalstīs dalībvalstis Direktīvas par vides krimināltiesisko aizsardzību[76] īstenošanā un stiprinās operatīvos tīklus un darbības šajā jomā[77]. Būtiska ir stingra izpilde. Turklāt nesen pieņemtā Eiropas Padomes Konvencija par vides krimināltiesisko aizsardzību[78] palīdzēs nodrošināt spēcīgus un salīdzināmus centienus apkarot noziegumus pret vidi gan Eiropā, gan ārpus tās.

Krimināltiesiskā reakcija

Noziedzība un terorisms var ietekmēt ikvienu, tāpēc ir būtiski atbalstīt un aizsargāt **cietušo** tiesības, lai samazinātu kaitējumu un palielinātu vispārējo drošību un uzticēšanos iestādēm. Pamatojoties uz Cietušo tiesību direktīvu, Komisija ieviesīs jaunu **ES stratēģiju par cietušo tiesībām**.

ES krimināltiesību sistēmām ir vajadzīgi iedarbīgi instrumenti, lai novērstu jaunus apdraudējumus. Lai to panāktu, Komisija ir uzsākusi **augsta līmeņa forumu par ES krimināltiesību nākotni**. Šis forums pulcē dalībvalstis, Eiropas Parlamentu, ES aģentūras un struktūras un citas attiecīgās ieinteresētās personas. Tā mērķis ir apspriest veidus, kā nodrošināt, ka mūsu krimināltiesību sistēmas joprojām ir efektīvas, taisnīgas un noturīgas, ņemot vērā mainīgās problēmas, vienlaikus stiprinot tiesu iestāžu sadarbību un uzlabojot savstarpējo uzticēšanos, arī ar digitalizācijas palīdzību[79].

Pamatdarbības

Komisija:

- **2026. gadā nāks klajā ar tiesību akta priekšlikumu modernizētiem noteikumiem par organizēto noziedzību;**
- **2025. gadā nāks klajā ar tiesību akta priekšlikumu, lai pārskatītu tiesisko regulējumu par narkotisko vielu prekursoriem;**
- **2025. gadā nāks klajā ar tiesību akta priekšlikumu par vienotiem krimināltiesību standartiem attiecībā uz šaujamieroču nelikumīgu tirdzniecību;**
- **izvērtēs nepieciešamību pārskatīt direktīvas par pirotehniku un civilām vajadzībām paredzētām sprāgstvielām;**
- **izvērtēs nepieciešamību vēl vairāk stiprināt Eiropas izmeklēšanas rīkojumu un Eiropas apcietināšanas orderi;**
- **2026. gadā nāks klajā ar jaunu ES stratēģiju cilvēku tirdzniecības apkarošanai;**
- **2026. gadā nāks klajā ar jaunu ES stratēģiju par cietušo tiesībām;**
- **līdz 2027. gadam nāks klajā ar ES rīcības plānu bērnu aizsardzībai pret noziedzību;**
- **2025. gadā nāks klajā ar ES rīcības plānu narkotiku tirdzniecības apkarošanai;**

[74] Ieskaitot Starptautisko Civilās aviācijas organizāciju (*ICAO*).

[75] Komisija arī atbalstīs to, ka tiek pabeigta Regula par pasākumiem pret pārvadātājiem, kuri sekmē cilvēku tirdzniecību vai migrantu kontrabandu vai iesaistās šajās darbībās (COM(2021) 753 final).

[76] Eiropas Parlamenta un Padomes Direktīva (ES) 2024/1203 (2024. gada 11. aprīlis), kas paredz noteikumus par vides krimināltiesisko aizsardzību, OV L, 2024/1203, 30.4.2024.

[77] ES Vides tiesību aktu īstenošanas un izpildes tīkls (*IMPEL*), Eiropas Prokuroru tīkls vides tiesībaizsardzībai (*ENPE*), *EnviCrimeNet* un ES Tiesnešu forums vides tiesībaizsardzībai (*EUFJE*).

[78] Ekspertu komiteja vides krimināltiesiskās aizsardzības jautājumos (*PC-ENV*) – Eiropas Krimināltiesisko problēmu komiteja.

[79] Jo īpaši, izveidojot e-tiesiskuma paziņojumu, izmantojot tiešsaistes datu apmaiņu (*eCODEX*) un Eiropas Sodāmības reģistru informācijas sistēmu par trešo valstu valstspiederīgajiem (*ECRIS-TCN*).

- **2026. gadā nāks klajā ar ES rīcības plānu cīņai pret šaujamieroču nelikumīgu tirdzniecību;**
- **no 2025. gada pakāpeniski paplašinās ES Ostu aliansi;**
- **2026. gadā pieņems DPA pamatnostādnes par nepilngadīgo aizsardzību;**
- **2026. gadā nāks klajā ar ES rīcības plānu cīņai pret iebiedēšanu tiešsaistē.**

Dalībvalstis tiek mudinātas:

- **līdz 2026. gada beigām pilnībā transponēt jaunos noteikumus par aktīvu atgūšanu un konfiskāciju un pilnībā izmantot to potenciālu;**
- **īstenot administratīvo pieeju cīņā pret noziedznieku iefiltrēšanos;**
- **izveidot publiskā un privātā sektora partnerību cīņai pret nelikumīgi iegūtu līdzekļu legalizēšanu;**
- **transponēt un pilnībā īstenot direktīvu par vardarbības pret sievietēm un vardarbības ģimenē novēršanu un apkarošanu.**

Eiropas Parlaments un Padome tiek mudināti:

- **virzīties uz priekšu sarunās par regulu, ar ko paredz noteikumus seksuālas vardarbības pret bērniem novēršanai un apkarošanai, un par direktīvu par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un materiālu, kuros atspoguļota seksuāla vardarbība pret bērniem, apkarošanu;**
- **pabeigt sarunas attiecībā uz direktīvu par korupcijas apkarošanu.**

6. Terorisma un vardarbīga ekstrēmisma apkarošana

Mēs ieviesīsim visaptverošu pretterorisma programmu, lai novērstu radikalizāciju, nodrošinātu drošību tiešsaistē un sabiedriskās vietās, ierobežotu finansēšanas kanālus un reaģētu uz uzbrukumiem, kad tie notiek.

ES joprojām ir augsts terorisma draudu līmenis. Tas ir cieši saistīts ar ģeopolitisko notikumu, jauno tehnoloģiju un jaunu terorisma finansēšanas līdzekļu plašāku ietekmi. Mums ir jānodrošina, ka ES ir labi sagatavota, lai prognozētu apdraudējumus, novērstu radikalizāciju (gan bezsaistē, gan tiešsaistē), aizsargātu iedzīvotājus un sabiedriskās vietas no uzbrukumiem un iedarbīgi reaģētu uz uzbrukumiem, kad tie notiek. **2025. gadā tiks iesniegta jauna ES programma terorisma un vardarbīga ekstrēmisma novēršanai un apkarošanai**, kurā izklāstīta ES turpmākā rīcība. Saskaņā ar jauno programmu ES un Rietumbalkānu valstis 2025. gadā parakstīs jauno **kopīgo rīcības plānu** terorisma un vardarbīga ekstrēmisma novēršanai un apkarošanai.

Radikalizācijas novēršana un cilvēku aizsardzība tiešsaistē

Līdzīgi cīņai pret organizēto noziedzību arī terorisma un vardarbīga ekstrēmisma apkarošana sākas ar **to pamatcēloņu novēršanu**. **ES Radikalizācijas novēršanas zināšanu centrs** pastiprinās atbalstu praktiķiem un politikas veidotājiem ar jaunu **visaptverošu novēršanas instrumentu kopumu**, kas ļaus agrīnā posmā identificēt neaizsargātas personas, īpaši nepilngadīgos, un veikt uz tiem vērstus intervences pasākumus. Radikalizācija bieži notiek cietumos, un, lai atbalstītu dalībvalstis šā jautājuma risināšanā, Komisija nāks klajā ar jauniem ieteikumiem.

Teroristi un vardarbīgi ekstrēmisti izmanto tiešsaistes platformas, lai izplatītu teroristisku un kaitīgu saturu, vāktu līdzekļus un vervētu. Neaizsargāti lietotāji, īpaši nepilngadīgie, tiek radikalizēti tiešsaistē satraucošā ātrumā. **Regula par vēršanos pret teroristiska satura izplatīšanu tiešsaistē** ir palīdzējusi apkarot teroristiska satura izplatīšanu tiešsaistē un ļāvusi

ātri izņemt šausminošāko un bīstamāko materiālu[80]. Komisija pašlaik izvērtē tās darbību un novērtēs, kā vislabāk stiprināt šo sistēmu.

ES krīzes protokols par kopīgu un ātru tiesībaizsardzības un tehnoloģiju nozares reakciju saistībā ar teroristu uzbrukumu tiks grozīts, lai nodrošinātu mērogojamību un elastību, reaģējot uz teroristu uzbrukumu pieaugošo tiešsaistes dimensiju. ES Interneta forums arī turpmāk būs galvenā iespēja brīvprātīgai sadarbībai ar tehnoloģiju nozari, lai apkarotu teroristisku un kaitīgu saturu tiešsaistē. Turklāt Komisija iesaistās starptautiskās iniciatīvās, piemēram, *Christchurch Call Foundation* un Globālajā Interneta forumā terorisma apkarošanai (*GIFCT*).

Terorisma finansēšanas apkarošana

Teroristi savas darbības finansē ar kolektīvās finansēšanas kampaņām, kriptoaktīviem, neobankām vai tiešsaistes maksājumu platformām. Tiesībaizsardzības iestādēm ir jāatklāj un jāizmeklē šīs finanšu plūsmas. Tam ir vajadzīgi līdzekļi, rīki un speciālās zināšanas. Svarīga loma ir **Terorisma apkarošanas finanšu izmeklētāju tīklam**. Komisija izpētīs **jaunas ES mēroga sistēmas izveidi, lai izsekotu teroristu finansēšanu**, kas aptvers ES iekšējos un *SEPA* darījumus, kriptoaktīvu pārvedumus, tiešsaistes un elektroniskos maksājumus un papildinās ES un ASV Teroristu finansēšanas izsekošanas programmas (*TFTP*) nolīgumu.

ES budžets ir **jāaizsargā pret ļaunprātīgu izmantošanu ar nolūku veicināt radikālu/ekstrēmistisku uzskatu veidošanos** dalībvalstīs. Pārskatītā **Finanšu regula** tagad ietver notiesāšanu par "kūdīšanu uz diskrimināciju, naidu vai vardarbību" kā pamatu izslēgšanai no ES finansējuma. Komisija turpinās pētīt labāko veidu, kā pilnībā izmantot rīkkopu, arī tad, kad tiek atlasīti potenciālie saņēmēji. ES budžeta aizsardzība ir atkarīga arī no ciešas sadarbības un informācijas apmaiņas ar valstu iestādēm, ES aģentūrām un struktūrām.

Aizsardzība pret uzbrukumiem

Papildus investīcijām radikalizācijas novēršanā būtiska pilsoņu aizsardzības sastāvdaļa ir līdzekļu ierobežošana teroristiem un noziedzniekiem uzbrukumu veikšanai. Ir jārīkojas gan attiecībā uz instrumentiem, ko izmanto teroristi, gan lai aizsargātu uzbrukuma riskam pakļautos mērķus.

Papildus darbībām attiecībā uz šaujamieročiem Komisija arī **pārskatīs noteikumus** par **sprāgstvielu prekursoriem**, lai tajos iekļautu augsta riska ķīmiskās vielas. **Sabiedriskas vietas** joprojām ir visbiežākie teroristu uzbrukumu mērķi, īpaši aktoriem, kas darbojas vienatnē. Lai aizsargātu iedzīvotājus no kaitējuma, tiks stiprināta **ES Konsultatīvā programma aizsardzības drošības jautājumos**, lai pēc dalībvalstu pieprasījuma veiktu sabiedrisko vietu, kritiskās infrastruktūras un augsta riska notikumu neaizsargātības novērtējumus, ko finansē no ES budžeta no Iekšējās drošības fonda. ES centīsies palielināt pieejamo finansējumu publiskās telpas aizsardzībai. Komisija piedāvā atbalstu dalībvalstu iestādēm un privātajiem operatoriem, šim nolūkam izmantojot īpašus norādījumus un rīkus, piemēram, sabiedrisko vietu aizsardzības zināšanu centru[81], un kopš 2020. gada publiskās telpas aizsardzības atbalstam jau ir darīti pieejami 70 miljoni EUR.

Komisija arī izpētīs iespēju ieviest prasības organizācijām apsvērt vai izmantot drošības pasākumus publiski pieejamās vietās, sadarbojoties ar vietējām iestādēm un privātiem partneriem.

[80] Līdz 2024. gada 31. decembrim ir izdoti 1426 izņemšanas rīkojumi, lai izņemtu teroristisku saturu vai bloķētu piekļuvi tam, un lielākā daļa no tiem ir vērsti uz džihādistu teroristisku saturu, bet daļa arī uz labējo teroristisko saturu.

[81] Sabiedrisku vietu aizsardzības zināšanu centrs.

Ņemot vērā acīmredzamo neaizsargātību, **ES stratēģija antisemītisma apkarošanai un ebreju dzīvesvides atbalstam (2021.–2030. gadam)** turpinās virzīt Komisijas darbības ebreju kopienas aizsardzībai. Komisija arī nodrošinās, ka ir ieviesti piemēroti instrumenti, lai palīdzētu dalībvalstīm apkarot **naidu pret musulmaņiem**.

Dronu izmantošana spiegošanā un uzbrukumos rada arvien lielāku drošības problēmu. Komisija izstrādās **saskaņotu testēšanas metodiku pretdronu sistēmām**, izveidos **pretdronu izcilības centru** un izvērtēs nepieciešamību saskaņot dalībvalstu tiesību aktus un procedūras.[82].

Ārvalstu kaujinieki teroristi

Lai identificētu ārvalstu kaujiniekus teroristus, kas atgriežas vai ieceļo pie ES ārējām robežām, ir vajadzīgi dati par personām, kas rada terorisma draudus. Šajā nolūkā Komisija kopā ar Eiropolu stiprinās **sadarbību ar galvenajām trešām valstīm, lai iegūtu biogrāfiskus un biometriskos datus par personām, kas varētu radīt terorisma draudus**, tai skaitā par ārvalstu kaujiniekiem teroristiem, kurus pēc tam var iekļaut Šengenas Informācijas sistēmā, pilnībā ievērojot piemērojamo ES un valstu tiesisko regulējumu. Tāpēc ir ļoti svarīgi, lai dalībvalstis izmantotu visus esošos instrumentus. Tas ietver visas attiecīgās informācijas ievadīšanu ***SIS***, biometrisko pārbaužu uzlabošanu un obligātu sistemātisku pārbaužu veikšanu visām personām pie ES ārējām robežām[83]. Turklāt *Frontex* izstrādātie **kopīgie riska rādītāji (KRR)** turpinās palīdzēt dalībvalstu robežkontroles iestādēm identificēt un novērtēt iespējamo ārvalstu kaujinieku teroristu aizdomīgas ceļošanas risku.

Turklāt, lai nodrošinātu, ka dalībvalstis saglabā piekļuvi **kaujas lauka pierādījumiem**, ko savākusi ANO Izmeklēšanas grupa ar mērķi veicināt saukšanu pie atbildības par *Da'esh/ISIL* pastrādātajiem noziegumiem (*UNITAD*) ārvalstu kaujinieku teroristu kriminālvajāšanai, Komisija kopā ar *Eurojust* izvērtēs iespēju glabāt šos pierādījumus *Eurojust* Galveno starptautisko noziegumu pierādījumu datubāzē. Turklāt jaunais Eiropas **Tiesu iestāžu pretterorisma reģistrs** turpinās palīdzēt dalībvalstu tiesu iestādēm ātri identificēt pārrobežu saiknes terorisma lietās.

Pamatdarbības

Komisija:

- **2025. gadā pieņems jaunu ES programmu terorisma un vardarbīga ekstrēmisma novēršanai un apkarošanai;**
- **2025. gadā parakstīs ar Rietumbalkānu valstīm jaunu kopīgu rīcības plānu terorisma un vardarbīga ekstrēmisma novēršanai un apkarošanai;**
- **kopā ar ES zināšanu centru izstrādās jaunu visaptverošu novēršanas instrumentu kopumu;**
- **2026. gadā izvērtēs Regulas par vēršanos pret teroristiska satura izplatīšanu tiešsaistē piemērošanu;**
- **2025. gadā grozīs ES krīzes protokolu;**
- **2026. gadā nāks klajā ar tiesību akta priekšlikumu pārskatīt Regulu par sprāgstvielu prekursoru tirdzniecību un lietošanu;**
- **izpētīs iespējas izveidot jaunu ES mēroga sistēmu teroristu finansēšanas izsekošanai.**

Dalībvalstis tiek mudinātas:

[82] Saskaņā ar pamatdarbību kopumu 2023. gada paziņojumā par dronu radīto potenciālo apdraudējumu novēršanu, COM(2023) 659 final.
[83] Pilnībā ievērojot Šengenas Robežu kodeksu un Skrīninga regulu.

- **uzlabot biometriskās pārbaudes un veikt obligātas sistemātiskas pārbaudes pie ES ārējām robežām;**
- **pilnībā izmantot Eiropas Tiesu iestāžu pretterorisma reģistru.**

7. ES kā spēcīga pasaules mēroga dalībniece drošības jomā

Lai uzlabotu ES drošību, mēs veicināsim operatīvo sadarbību, izmantojot partnerības ar tādiem svarīgiem reģioniem kā paplašināšanās un kaimiņattiecību partneri, Latīņamerika un Vidusjūras reģions. Starptautiskajā sadarbībā tiks ņemtas vērā ES drošības intereses, arī izmantojot ES rīkus un instrumentus.

Pēdējie gadi ir apliecinājuši nesaraujamo saikni starp ES ārējo un iekšējo drošību. Krievijas agresijas karam pret Ukrainu, konfliktam Gazā, situācijai Sīrijā un jauniem konfliktiem visā pasaulē ir bijusi nopietna plašāka ietekme uz ES iekšējo drošību. **ES ir aktīvi jāaizstāv savas drošības intereses**, lai vērstos pret globālās nestabilitātes ietekmi uz tās iekšējo drošību, novēršot ārējos draudus, ko var veikt, pārtraucot nelikumīgas tirdzniecības maršrutus un aizsargājot stratēģisku interešu koridorus, piemēram, tirdzniecības maršrutus. Vienlaikus ES turpinās būt spēcīga sabiedrotā tās partnervalstīm un sadarbosies, lai uzlabotu globālo drošību un veidotu savstarpēju noturību pret apdraudējumiem.

Pēdējos gados ES ir veikusi nozīmīgus pasākumus, lai uzlabotu sadarbību drošības jomā. Tā ir noslēgusi operatīvas tiesībaizsardzības un tiesu iestāžu sadarbības nolīgumus, kā arī cita veida vienošanās ar partnervalstīm. Tā aktīvi īsteno papildu starptautiskus nolīgumus saskaņā ar Padomes sarunu norādēm un spēju veidošanas iniciatīvas, ko veicina ES aģentūras un struktūras. Sadarbības instrumentam *NDICI*-"Eiropa pasaulē" arī ir izšķiroša nozīme drošības stiprināšanā ar partnervalstīm.

Uz noteikumiem balstīta daudzpusēja kārtība ir stūrakmens globālās drošības stiprināšanai. Drošības dialogi, tai skaitā tematiski dialogi, ir būtiski šo centienu stiprināšanai. Lai izstrādātu rezultatīvus drošības risinājumus, izšķiroša nozīme ir **Stratēģiskā kompasa drošībai un aizsardzībai** īstenošanai, kā arī divpusējiem un daudzpusējiem sadarbības satvariem, piemēram, stabilizācijas un asociācijas nolīgumiem un asociācijas nolīgumiem, un sadarbībai ar tādām organizācijām kā ANO un NATO. ES turpinās piedalīties daudzpusējos forumos[84] un pastiprinās sadarbību ar attiecīgām starptautiskām un reģionālām organizācijām un struktūrām, tai skaitā NATO, Apvienoto Nāciju Organizāciju, Eiropas Padomi, Interpolu, G7, EDSO un pilsonisko sabiedrību.

Reģionālā sadarbība

Prioritārs uzdevums un politiska un ģeostratēģiska nepieciešamība ir turpināt ES nelokāmo atbalstu **Ukrainai** un stiprināt **ES paplašināšanās procesā iesaistīto valstu** drošību un noturību. ES drošības atbalstam būtu jāiet roku rokā ar **kandidātvalstu paātrinātu integrāciju ES drošības arhitektūrā**, vienlaikus konsolidējot to reģionālo sadarbību. Komisija izmantos ES paplašināšanās politiku, lai atbalstītu ES kandidātvalstu un potenciālo kandidātvalstu spējas reaģēt uz apdraudējumiem, palielinātu operatīvo sadarbību un informācijas apmaiņu un nodrošinātu saskaņotību ar ES principiem, tiesību aktiem un instrumentiem. Pirmspievienošanās palīdzības instrumentam (*IPA III*), kā arī Ukrainas, Moldovas un Rietumbalkānu mehānismiem ir izšķiroša nozīme drošības stiprināšanā gan kandidātvalstīs, gan potenciālajās kandidātvalstīs.

[84] Globālais terorisma apkarošanas forums, globālā koalīcija pret *Da'esh*, Globālais interneta forums terorisma apkarošanai (*GIFCT*), *Christchurch Call Foundation*, Globālā koalīcija sintētisko narkotiku radīto draudu novēršanai.

ES arī turpinās integrēt **kaimiņattiecību partnerus** ES drošības arhitektūrā. Izmantojot **jauno Vidusjūras reģiona paktu** un gaidāmo **stratēģisko pieeju Melnajai jūrai**, Savienība centīsies arī turpmāk veidot reģionālo sadarbību un divpusējas stratēģiskas visaptverošas partnerības ar drošības dimensiju, attiecīgā gadījumā regulāri rīkojot augsta līmeņa drošības dialogus. Tiks stiprināta operatīvā sadarbība ar Ziemeļāfriku, **Tuvajiem Austrumiem un Persijas līča valstīm**, īpaši tādās jomās kā terorisma apkarošana, nelikumīgi iegūtu līdzekļu legalizēšanas novēršana, šaujamieroču nelikumīga tirdzniecība un narkotiku, īpaši kaptagona, tirdzniecība.

Lai pievērstos teroristu un noziedzīgu darbību pieaugumam un to iespējamai plašākai ietekmei **Subsahāras Āfrikā, īpaši Sāhelā, Āfrikas ragā**, **un Rietumāfrikā**, ES pastiprinās atbalstu Āfrikas Savienībai, reģionālajām ekonomikas kopienām (*REC*) un reģiona valstīm. Saskaņā ar ES Jūras drošības stratēģiju[85] ES stiprinās sadarbību **Gvinejas līcī, Sarkanajā jūrā un Indijas okeānā**, lai apkarotu cilvēku tirdzniecību un pirātismu, atbalstot Āfrikas un reģionālo sadarbību un atbalstot ES koordinētu klātbūtni jūrā (*CMP*) un Narkotiku jūras ceļu izpētes un operatīvo centru (*MAOC-N*).

ES stiprinās operatīvo sadarbību ar **Latīņameriku un Karību jūras reģionu**, lai likvidētu augsta riska noziedzīgos tīklus un sauktu pie atbildības par tiem un izjauktu nelikumīgas darbības un tirdzniecības maršrutus, kas tiks panākts, uzlabojot sadarbības satvarus, piemēram, ES un *CLASI* (Latīņamerikas Iekšējās drošības komiteja) un ES un *CELAC* koordinācijas un sadarbības mehānismu narkotiku apkarošanas jomā. Viena no prioritātēm būs loģistikas centru noturība un partnerības, kā arī pieeja "seko naudai". ES turpinās atbalstīt Ziemeļamerikas un Dienvidamerikas policijas savienības (*AMERIPOL*) attīstību, lai tā kļūtu par Eiropola reģionālo ekvivalentu un stiprinātu tiesu iestāžu sadarbību starp dalībvalstīm un reģionu. ES arī sadarbosies ar **Dienvidāziju un Vidusāziju**, lai risinātu kopīgas drošības problēmas, kas saistītas ar terorismu, nelikumīgu preču, arī narkotiku, tirdzniecību, cilvēku tirdzniecību un migrantu kontrabandu.

Turklāt ES atbalstīs reģionālās sadarbības satvarus trešās valstīs, lai vēl vairāk palīdzētu tām apturēt nelikumīgu tirdzniecību izcelsmes vietā saskaņā ar kopīgas atbildības principu par visu noziedzīgo piegādes ķēdi. Turklāt ES sniegs savu ieguldījumu, lai palīdzētu stiprināt loģistikas centru drošību ārvalstīs, koordinējot **kopīgas inspekcijas trešo valstu ostās**.

Operatīvā sadarbība

Global Gateway atbalstīs ilgtspējīgus un kvalitatīvus infrastruktūras projektus digitālajā, klimata un enerģētikas, transporta, veselības aprūpes, izglītības un pētniecības nozarē. Komisija tagad attiecīgā gadījumā iekļaus drošības apsvērumus turpmākajās *Global Gateway* investīcijās. Tas ietvers iniciatīvas, kas ir būtiskas ES un tās partnervalstu stratēģiskajai autonomijai, piemēram, infrastruktūras projektus, kas ietver drošības novērtējumus un riska mazināšanas pasākumus.

Komisija īstenos turpmākus **nolīgumus starp ES un trešām valstīm par sadarbību ar Eiropolu un *Eurojust***, it īpaši ar Latīņamerikas valstīm.

Turklāt trešo valstu proaktīva dalība ***EMPACT*** ir viens no iedarbīgākajiem operatīvās sadarbības stiprināšanas līdzekļiem. ES arī turpmāk veicinās trešo valstu, īpaši Rietumbalkānu, austrumu kaimiņreģiona, Subsahāras Āfrikas, Ziemeļāfrikas, Tuvo Austrumu, Latīņamerikas un Karību jūras reģiona valstu iesaisti. Vēl viens instruments sadarbības stiprināšanai ar trešām valstīm noziedzības apkarošanas jomā ir operatīvās darba grupas starp dalībvalstīm, kuras koordinē Eiropols un kurās var piedalīties trešās valstis. Komisijas mērķis ir arī pabeigt sarunas

[85] JOIN (2023) 8 final.

par **ES un Interpola** starptautisko nolīgumu[86], tādējādi nodrošinot vienotāku pieeju globālajiem drošības apdraudējumiem un apkarojot transnacionālos noziegumus.

Eiropas komandas pieejā Savienībai ir jābūt pārstāvētai uz vietas. Specializētiem Savienības un dalībvalstu darbiniekiem ir izšķiroša nozīme, lai nodrošinātu, ka Savienības ārējā darbība ir labi informēta, koordinēta un reaģētspējīga. Lai šo pieeju paaugstinātu līdz nākamajam līmenim, Komisija ar Augstā pārstāvja ārlietās un drošības politikas jautājumos atbalstu stiprinās **sadarbības tīklus** un veicinās reģionālo **Eiropola un *Eurojust* sadarbības koordinatoru** izvietošanu saskaņā ar dalībvalstu operatīvajām vajadzībām.

ES centīsies panākt ciešāku operatīvo tiesībaizsardzības un tiesu iestāžu sadarbību, veicinās reāllaika informācijas apmaiņu un kopīgas operācijas, izmantojot **kopējas izmeklēšanas grupas** trešās valstīs ar Eiropola un *Eurojust* atbalstu. Komisija arī atbalstīs dalībvalstis **kopīgu informācijas apkopošanas centru** izveidē, apvienojot ekspertus un vietējās tiesībaizsardzības iestādes stratēģiskās trešās valstīs.

Kopējās ārpolitikas un drošības politikas (KĀDP) instrumenti

Kopējās drošības un aizsardzības politikas (KDAP) misijas arī tiks pilnībā izmantotas, lai labāk apzinātu un novērstu ārējos draudus ES iekšējai drošībai saskaņā ar to pilnvarām, ko tām noteikusi Padome. Lai veidotu trešo valstu spējas, Augstais pārstāvis ārlietās un drošības politikas jautājumos un Komisija atbalstīs KDAP darbības ar īpašiem finansēšanas instrumentiem un izpētīs visus piemērotos finansējuma veidus.

ES ierobežojošie pasākumi ir vispāratzīts KĀDP instruments, ko izmanto arī cīņā pret terorismu. Pamatojoties uz Augstā pārstāvja ārlietās un drošības politikas jautājumos, dalībvalstu vai Komisijas ierosinājumiem, Padome varētu izvērtēt, kā ES spēkā esošos autonomos ierobežojošos pasākumus (ES teroristu sarakstu) varētu padarīt iedarbīgākus, operatīvākus un dinamiskākus. Turklāt saskaņā ar KĀDP mērķiem varētu apsvērt iespēju izpētīt papildu ierobežojošus pasākumus, kas vērsti pret noziedznieku tīkliem.

Vīzu politika un informācijas apmaiņa

ES vīzu politika ir svarīgs instruments sadarbībai ar trešām valstīm un mūsu robežu drošībai, kontrolējot ieceļošanu ES un paredzot tai nosacījumus. Komisija pilnībā integrēs **drošības apsvērumus ES vīzu politikā**, izmantojot gaidāmo ES vīzu politikas stratēģiju. Komisija sadarbosies ar abiem likumdevējiem, lai pieņemtu priekšlikumu pārskatīt un racionalizēt vīzu režīma atcelšanas apturēšanas mehānismu, īpaši konkrētos bezvīzu režīma ļaunprātīgas izmantošanas gadījumos[87]. Trešās valstis tiks mudinātas apmainīties ar informāciju par personām, kuras var radīt drošības apdraudējumus, un šī informācija tiks ievadīta ES informācijas sistēmās un datubāzēs.

Lai panāktu politikas koordināciju un veiktu agrīnus preventīvus pasākumus, atraisot efektīvāku, ātrāku un raitāku sadarbību, Komisija strādās, lai izveidotu **datu plūsmas kārtību** un izpētītu veidus, kā **uzlabot informācijas apmaiņu** tiesībaizsardzības un robežu pārvaldības nolūkos ar uzticamām trešām valstīm, ievērojot pamattiesības un datu aizsardzības noteikumus.

Pamatdarbības
Komisija:

[86] Padomes 2021. gada 19. jūlija Lēmums (ES) 2021/1312 un Padomes 2021. gada 19. jūlija Lēmums (ES) 2021/1313.
[87] COM (2023) 642.

- **noslēgs starptautiskus nolīgumus starp ES un prioritārām trešām valstīm par sadarbību ar Eiropolu un *Eurojust*;**
- **mudinās partnervalstis piedalīties *EMPACT* cīņā pret organizēto noziedzību un terorismu;**
- **atbalstīs ES aģentūras un struktūras sadarbības mehānismu ar partnervalstīm izveidē un stiprināšanā;**
- **turpinās atspoguļot drošības apsvērumus ES vīzu politikā, šim mērķim izmantojot gaidāmo vīzu stratēģiju;**
- **stiprinās informācijas apmaiņu ar uzticamām trešām valstīm tiesībaizsardzības un robežu pārvaldības nolūkos.**

Komisija sadarbībā ar Augsto pārstāvi ārlietās:

- **pilnībā izmantos civilās kopējās drošības un aizsardzības politikas (KDAP) misijas;**
- **līdz 2027. gadam sāks koordinēt kopīgas inspekcijas trešo valstu ostās.**

Komisija sadarbībā ar Augsto pārstāvi ārlietās un dalībvalstu jautājumos:

- **stiprinās sadarbības tīklus un sadarbību, izmantojot Eiropas komandas pieeju;**
- **no 2025. gada izveidos kopīgas operatīvās vienības un informācijas apkopošanas centrus trešās valstīs.**

Eiropas Parlaments un Padome tiek mudināti:

- **pabeigt sarunas par vīzu režīma atcelšanas apturēšanas mehānisma pārskatīšanu.**

8. Nobeigums

Nenoteiktības apstākļos ir jāuzlabo Savienības spēja paredzēt un novērst drošības apdraudējumus un reaģēt uz tiem.

Nepietiek ar reaģēšanu uz krīzēm tikai tad, kad tās rodas. Mums ir jāuzlabo mūsu informētība, sniedzot pilnīgu priekšstatu par apdraudējumiem, kad tie attīstās. Tāpat jānodrošina, ka mūsu rīki un spējas atbilst uzdevumam.

Visaptverošais pasākumu kopums, kas sīki izklāstīts šajā stratēģijā, palīdzēs izveidot spēcīgāku Savienību pasaulē – Savienību, kas spēj paredzēt, plānot un rūpēties par savām drošības vajadzībām, kas var efektīvi reaģēt uz draudiem iekšējai drošībai un saukt vainīgos pie atbildības un kas aizsargā atvērtu, brīvu un pārticīgu sabiedrību un demokrātiju.

Tāpēc ir jāmaina mūsu domāšanas veids attiecībā uz iekšējo drošību. Mēs strādāsim, lai palīdzētu veicināt jaunu ES drošības kultūru, kurā drošības apsvērumi tiek ņemti vērā visos mūsu tiesību aktos, politikā un programmās – no sākuma līdz īstenošanai. Un kur sadarbība starp politikas jomām mums ļauj pavērt jaunas iespējas.

Tas nav tikai vienas iestādes, valdības vai dalībnieka uzdevums. Tie ir Eiropas kopīgie centieni.