EIROPAS
KOMISIJA

Briselē, 24.7.2020.
COM(2020) 605 final

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

par ES Drošības savienības stratēģiju

I. Ievads

Komisijas politikas pamatnostādnēs ir skaidri norādīts, ka attiecībā uz mūsu iedzīvotāju aizsardzību mums ir jāizmanto visas iespējas. Drošība ir ne tikai personīgās drošības pamats, tā aizsargā arī pamattiesības un nodrošina pamatu ticībai mūsu ekonomikai, mūsu sabiedrībai un demokrātijai un dinamikai tajās. Šodien eiropieši saskaras ar mainīgu drošības situāciju, ko ietekmē jauni apdraudējumi, kā arī citi faktori, tostarp klimata pārmaiņas, demogrāfiskās tendences un politiskā nestabilitāte ārpus mūsu robežām. Globalizācija, brīva pārvietošanās un digitālā pārveide turpina nodrošināt labklājību, atvieglot mūsu dzīvi un veicināt inovāciju un izaugsmi. Taču līdztekus šiem ieguvumiem rodas arī riski un izmaksas. Tos var manipulēt terorisms, organizētā noziedzība, narkotiku tirdzniecība un cilvēku tirdzniecība — tie visi ir tieši draudi iedzīvotājiem un mūsu dzīvesveidam Eiropā. Kiberuzbrukumi un kibernoziedzība turpina pieaugt. Arvien sarežģītāki kļūst arī drošības apdraudējumi: tos veicina spēja strādāt pāri robežām un savstarpēja savienojamība; tie izmanto robežšķirtnes izzušanu starp fizisko un digitālo pasauli; tie izmanto neaizsargātās grupas, sociālās un ekonomiskās atšķirības. Uzbrukumi var notikt jebkurā brīdī, un tie var atstāt minimālas pēdas vai tādas neatstāt nemaz; gan valsts, gan nevalstiskie dalībnieki var izmantot dažādus hibrīddraudus[1]; un tas, kas notiek ārpus ES, var izšķiroši ietekmēt drošību ES iekšienē.

Covid-19 krīze ir pārveidojusi arī mūsu izpratni par drošuma un drošības apdraudējumiem un attiecīgās rīcībpolitikas. Tā ir uzsvērusi nepieciešamību garantēt drošību gan fiziskajā, gan digitālajā vidē. Tā ir uzsvērusi atvērtas stratēģiskas autonomijas nozīmību mūsu piegādes ķēdēm attiecībā uz kritiski svarīgiem produktiem, pakalpojumiem, infrastruktūrām un tehnoloģijām. Tā ir pastiprinājusi nepieciešamību iesaistīt visas nozares un visas personas kopīgos centienos nodrošināt, ka ES pirmām kārtām ir labāk sagatavota un izturētspējīgāka un ka tai ir labāki instrumenti, lai vajadzības gadījumā reaģētu.

Iedzīvotājus nevar aizsargāt, dalībvalstīm rīkojoties tikai vienpusēji. Mūsu priekšrocību strādāt kopā pilnveidošana nekad nav bijusi tik svarīga, un ES nekad nav bijis lielāka potenciāla panākt pārmaiņas. ES var rādīt piemēru, uzlabojot savu vispārējo krīzes pārvarēšanas sistēmu un darbojoties gan savā teritorijā, gan ārpus tās, lai veicinātu globālo stabilitāti. Kaut arī galvenā atbildība par drošību ir dalībvalstīm, pēdējos gados ir veidojusies arvien lielāka izpratne par to, ka vienas dalībvalsts drošība nozīmē visu dalībvalstu drošību. ES var sniegt daudznozaru, integrētu atbildi, palīdzot drošības jomas dalībniekiem dalībvalstīs ar vajadzīgajiem rīkiem un informāciju[2].

ES var arī nodrošināt, ka drošības politika arī turpmāk balstās uz mūsu kopīgajām Eiropas vērtībām — tiesiskuma, vienlīdzības[3] un pamattiesību ievērošanu un pārredzamības, pārskatatbildības un demokrātiskas kontroles garantēšanu —, lai nodrošinātu rīcībpolitikām atbilstošu uzticības pamatu. Tā var izveidot efektīvu un patiesu drošības savienību, kurā personu tiesības un brīvības ir labi aizsargātas. Drošība un pamattiesību ievērošana nav pretrunīgi mērķi, bet gan saskanīgi un papildinoši. Mūsu vērtībām un pamattiesībām ir jābūt

[1] Lai gan hibrīddraudu definīcijas atšķiras, tās mērķis ir aptvert piespiedu un graujošu darbību, tradicionālu un netradicionālu (t. i., diplomātisku, militāru, ekonomisku, tehnoloģisku) metožu apvienojumu, ko koordinēti var izmantot valsts vai nevalstiski dalībnieki, lai panāktu konkrētus mērķus (bet nepārkāpjot oficiāli pieteikta kara robežu). Skatīt JOIN(2016)18 (final).

[2] Piemēram, izmantojot pakalpojumus, ko sniedz tāda ES kosmosa programma kā *Copernicus*, kas nodrošina Zemes novērošanas datus un lietojumprogrammas robežu uzraudzībai, jūras drošībai, tiesībaizsardzībai, pirātisma apkarošanai, narkotiku kontrabandas novēršanai un ārkārtas situāciju pārvaldībai.

[3] Savienība, kurā valda līdztiesība: dzimumu līdztiesības stratēģija 2020.–2025. gadam, COM(2020) 152.

drošības politikas pamatā, nodrošinot nepieciešamības, proporcionalitātes un likumības principu ievērošanu, kā arī atbilstošas garantijas attiecībā uz pārskatatbildību un tiesisko aizsardzību, vienlaikus dodot iespēju efektīvi reaģēt, lai aizsargātu privātpersonas, jo īpaši visneaizsargātākās.

Jau ir ieviesti nozīmīgi juridiskie, praktiskie un atbalsta instrumenti, taču tie ir gan jāstiprina, gan labāk jāīsteno. Ir panākts liels progress, lai uzlabotu informācijas apmaiņu un sadarbību izlūkdatu jomā ar dalībvalstīm un lai slēgtu telpu, kurā darbojas teroristi un noziedznieki. Tomēr joprojām pastāv sadrumstalotība.

Darbam jānotiek arī ārpus ES robežām. Savienības un tās iedzīvotāju aizsardzība vairs nav saistīta tikai ar drošības nodrošināšanu ES robežās, bet arī ar pievēršanos drošības ārējai dimensijai. ES pieeja ārējai drošībai saistībā ar kopējo ārpolitiku un drošības politiku (KĀDP) un kopējo drošības un aizsardzības politiku (KDAP) joprojām būs būtiska sastāvdaļa ES centienos uzlabot drošību Eiropas Savienībā. Sadarbība ar trešām valstīm un pasaules līmenī, lai risinātu kopīgas problēmas, ir ļoti svarīga efektīvai un visaptverošai reakcijai, un stabilitātei un drošībai ES kaimiņvalstīs ir izšķiroša nozīme pašas ES drošībai.

Pamatojoties uz Eiropas Parlamenta[4], Padomes[5] un Komisijas[6] iepriekšējo darbu, šī jaunā stratēģija parāda, ka patiesas un efektīvas drošības savienības pamatā ir jāapvieno spēcīgi instrumenti un rīcībpolitikas, lai nodrošinātu drošību praksē, un jāatzīst, ka drošība ietekmē visas sabiedrības daļas un visas sabiedriskās politikas jomas. ES ir jānodrošina droša vide ikvienam neatkarīgi no rases vai etniskās izcelsmes, reliģijas, ticības, dzimuma, vecuma vai seksuālās orientācijas.

Šī stratēģija aptver laikposmu no 2020. līdz 2025. gadam, un tās uzmanības centrā ir spēju un kapacitātes veidošana, lai nodrošinātu nākotnes prasībām atbilstošu drošības vidi. Tajā izklāstīta visu sabiedrību aptveroša pieeja drošībai, kas koordinētā veidā var efektīvi reaģēt uz strauji mainīgo apdraudējumu ainu. Tajā definētas stratēģiskās prioritātes un atbilstošās darbības, lai integrētā veidā visā drošības savienības ekosistēmā novērstu digitālos un fiziskos riskus, koncentrējoties uz jomām, kurās ES var sniegt papildu vērtību. Tās mērķis ir piedāvāt ieguvumu drošības jomā ar mērķi aizsargāt ikvienu ES iedzīvotāju.

II. Strauji mainīga Eiropas drošības apdraudējumu aina

Iedzīvotāju drošība, labklājība un labbūtība ir atkarīga no būšanas drošībā. Šīs drošības apdraudējumi ir atkarīgi no tā, cik lielā mērā viņu dzīvība un iztikas līdzekļi ir neaizsargāti. Jo lielāka neaizsargātība, jo lielāks risks, ka tā var tikt izmantota. Gan neaizsargātība, gan apdraudējumi pastāvīgi attīstās, un ES ir jāpielāgojas.

Mūsu ikdienas dzīve ir atkarīga no visdažādākajiem pakalpojumiem, piemēram, enerģētikas, transporta un finanšu, kā arī veselības aprūpes pakalpojumiem. To pamatā ir gan fiziskā, gan digitālā infrastruktūra, kas palielina neaizsargātību un traucējumu iespējamību. Covid-19 pandēmijas laikā jaunās tehnoloģijas ir nodrošinājušas daudzu uzņēmumu un sabiedrisko pakalpojumu darbību — gan uzturot sakarus, izmantojot attālinātu darbu, gan saglabājot

[4] Piemēram, Eiropas Parlamenta *TERR* komitejas darbs, kura sniedza ziņojumu 2018. gada novembrī.

[5] No Padomes 2015. gada jūnija secinājumiem par "atjauninātu iekšējās drošības stratēģiju" līdz jaunākajiem Padomes 2019. gada decembra rezultātiem.

[6] "Eiropas Drošības programmas īstenošana cīņā pret terorismu un virzībā uz efektīvu un patiesu drošības savienību", COM (2016) 230 final, 2016. gada 20. aprīlis. Skatīt neseno novērtējumu par tiesību aktu īstenošanu iekšējās drošības jomā: Iekšlietu tiesību aktu īstenošana iekšējās drošības jomā — 2017.–2020. gads, SWD(2020)135.

piegādes ķēžu loģistiku. Tomēr tas ir arī pavēris iespēju nepieredzēti lielam ļaunprātīgu uzbrukumu skaitam, ar kuriem tiek mēģināts kriminālos nolūkos gūt labumu no pandēmijas radītajiem traucējumiem un pārejas uz digitālo tāldarbu no mājām[7]. Preču trūkums ir radījis organizētajai noziedzībai jaunas iespējas. Sekas varēja būt nāvējošas, traucējot veselības pamatpakalpojumus laikā, kad spiediens bija vislielākais.

Arvien lielākais to veidu skaits, kādos digitālās tehnoloģijas uzlabo mūsu dzīvi, ir arī padarījis tehnoloģiju **kiberdrošību** par stratēģiskas nozīmes jautājumu[8]. Kiberuzbrukumi smagi skar mājokļus, bankas, finanšu pakalpojumus un uzņēmumus (jo īpaši mazos un vidējos uzņēmumus). Iespējamo kaitējumu vēl vairāk pavairo fizisko un digitālo sistēmu savstarpējā atkarība: jebkura fiziska ietekme neizbēgami ietekmēs digitālās sistēmas, savukārt kiberuzbrukumi informācijas sistēmām un digitālajām infrastruktūrām var apturēt pamatpakalpojumus[9]. Lietu interneta izvirzīšanās un mākslīgā intelekta plašāka izmantošana dos jaunus ieguvumus, kā arī jaunus riskus.

Mūsu pasaule paļaujas uz digitālajām infrastruktūrām, tehnoloģijām un tiešsaistes sistēmām, kas ļauj mums radīt uzņēmumus, patērēt produktus un izmantot pakalpojumus. Tie visi ir atkarīgi no saziņas un mijiedarbības. Atkarība no interneta ir pavērusi ceļu **kibernoziedzības** vilnim[10]. "Kibernoziedzība kā pakalpojums" un pagrīdes kibernoziedzības ekonomika nodrošina vieglu piekļuvi kibernoziedzības produktiem un pakalpojumiem tiešsaistē. Noziedznieki ātri pielāgojas jauno tehnoloģiju izmantošanai saviem mērķiem. Piemēram, viltotas un falsificētas zāles ir iefiltrētas zāļu likumīgajā piegādes ķēdē[11]. Materiālu ar seksuālu vardarbību pret bērniem skaita eksponenciālais pieaugums tiešsaistē[12] ir parādījis mainīgo noziedzības modeļu sociālās sekas. Nesen veikta aptauja parādīja, ka lielākā daļa iedzīvotāju ES (55 %) ir nobažījušies par to, ka viņu datiem piekļūst noziedznieki un krāpnieki[13].

Šos apdraudējumus arī pastiprina **globālā vide**. Uzstājīga trešo valstu rūpniecības politika apvienojumā ar pastāvīgu intelektuālā īpašuma zādzību, ko padara iespējamu kibertelpa, maina stratēģisko paradigmu Eiropas interešu aizsardzībai un veicināšanai. To uzsver divējāda lietojuma tehnoloģiju pieaugums, padarot spēcīgu civilo tehnoloģiju nozari par spēcīgu aizsardzības un drošības spēju. Rūpnieciskajai spiegošanai ir būtiska ietekme uz ES ekonomiku, nodarbinātību un izaugsmi: tiek lēsts, ka komercnoslēpumu kiberzādzība

---

7 Eiropols, *Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU* ("Pēc pandēmijas — kā Covid-19 ietekmēs smago noziegumu un organizētās noziedzības ainu Eiropas Savienībā"), (2020. gada aprīlis).

8 Komisijas ieteikums par 5G tīklu kiberdrošību, C(2019) 2335; Paziņojums "Droša 5G ieviešana ES – ES rīkkopas īstenošana", COM (2020) 50.

9 2020. gada martā Brno Universitātes slimnīca Čehijā cieta no kiberuzbrukuma, kas piespieda to novirzīt pacientus un atcelt operācijas (Eiropols, *Pandemic Profiteering. How criminals exploit the COVID-19 crisis* ("Pelnīšana uz pandēmijas rēķina. Kā noziedznieki ekspluatē Covid-19 krīzi")). Mākslīgo intelektu var ļaunprātīgi izmantot digitāliem, politiskiem un fiziskiem uzbrukumiem, kā arī novērošanai. Lietu interneta datu vākšanu var izmantot privātpersonu novērošanai (viedpulksteņi, virtuālie asistenti utt.).

10 Saskaņā ar dažām prognozēm datu aizsardzības pārkāpumu radītās izmaksas līdz 2024. gadam ik gadu sasniegs 5 triljonus ASV dolāru salīdzinājumā ar 3 triljoniem ASV dolāru 2015. gadā (*Juniper Research, The Future of Cybercrime & Security* ("Kibernoziedzības un drošības nākotne")).

11 Vienā 2016. gada pētījumā (*Legiscript*) tika lēsts, ka pasaulē tikai 4 % interneta aptieku darbojas likumīgi, un ES patērētāji ir galvenie mērķi 30 000–35 000 nelikumīgo interneta aptieku, kas darbojas tiešsaistē.

12 ES stratēģija seksuālas vardarbības pret bērniem efektīvākai apkarošanai, COM(2020) 607.

13 Eiropas Savienības Pamattiesību aģentūra (2020), *Your rights matter: Security concerns and experiences — Fundamental Rights Survey* ("Jūsu tiesības ir svarīgas: drošības problēmas un pieredze — pamattiesību apsekojums"), Luksemburga, Publikāciju birojs.

Eiropas Savienībai izmaksā 60 miljardus EUR[14]. Tādēļ ir rūpīgi jāapsver, kā atkarība un lielāka pakļautība kiberdraudiem ietekmē ES spēju aizsargāt gan privātpersonas, gan uzņēmumus.

Covid-19 krīze ir uzsvērusi arī to, kā sociālā šķelšanās un nenoteiktība rada drošības ievainojamību. Tas palielina iespēju, ka valsts un nevalstiski dalībnieki varētu veikt sarežģītākus un **hibrīduzbrukumus**, un ievainojamības tiek izmantotas, apvienojot kiberuzbrukumus, kaitējumu kritiskajai infrastruktūrai[15], dezinformācijas kampaņas un politiskā vēstījuma radikalizāciju.[16]

Tajā pašā laikā turpina attīstīties senāki apdraudējumi. **Teroristu uzbrukumu** skaitam 2019. gadā ES bija tendence samazināties. Tomēr apdraudējums ES iedzīvotājiem, ko rada džihādistu uzbrukumi, kurus veic vai kurus iedvesmojuši *Da'esh* un *al-Qaeda* un to atzari, joprojām ir liels[17]. Līdztekus pieaug arī vardarbīga labējā spārna ekstrēmisma draudi[18]. Rasisma iedvesmotiem uzbrukumiem jābūt par iemeslu nopietnām bažām: nāvējošie antisemītiskie terora akti Hallē bija atgādinājums par nepieciešamību pastiprināt reakciju saskaņā ar Padomes 2018. gada deklarāciju[19]. Katrs piektais ES iedzīvotājs ir ļoti noraizējies par teroristu uzbrukumu nākamo 12 mēnešu laikā[20]. Vairākums neseno teroristu uzbrukumu bija "zemo tehnoloģiju" uzbrukumi, vientuļi izpildītāji, kuru mērķis ir privātpersonas sabiedriskās vietās, savukārt teroristu propaganda tiešsaistē ieguva jaunu nozīmību, tiešraidē straumējot Kraistčērčas uzbrukumus[21]. Radikalizēto personu radītais apdraudējums joprojām ir liels – to, iespējams, pastiprina ārvalstu kaujinieki teroristi, kas atgriežas, un ekstrēmisti, kas atbrīvoti no cietuma[22].

Krīze ir arī parādījusi, kā pastāvošie apdraudējumi var attīstīties jaunos apstākļos. **Organizētās noziedzības** grupējumi ir izmantojuši preču trūkumu, tādējādi atverot jaunus nelikumīgus tirgus. Nelegālo narkotisko vielu tirdzniecība joprojām ir lielākais noziedzīgais tirgus ES, un tiek lēsts, ka tā mazumtirdzniecības vērtība ES ir vismaz 30 miljardi EUR gadā[23]. Turpina pastāvēt cilvēku tirdzniecība: aplēses liecina, ka gada peļņa pasaulē no visiem ekspluatācijas veidiem sasniedz gandrīz 30 miljardus EUR[24]. Viltotu zāļu

---

[14] *The scale and impact of industrial espionage and theft of trade secrets through cyber* ("Rūpnieciskās spiegošanas un komercnoslēpumu zādzību kibertelpā mērogs un ietekme"), 2018. gads.

[15] Kritiskās infrastruktūras ir būtiskas vitāli svarīgām sabiedrības funkcijām, veselībai, drošumam, drošībai, ekonomiskajai vai sociālajai labbūtībai, un šo infrastruktūru traucējumi/iznīcināšana rada ievērojamu ietekmi (Padomes Direktīva 2008/114/EK).

[16] 97 % ES iedzīvotāju ir saskārušies ar viltus ziņām, 38 % ar tām saskaras ikdienā. Skatīt JOIN (2020) 8 final.

[17] 13 ES dalībvalstis ziņoja par 119 pabeigtiem, neveiksmīgiem un izjauktiem teroristu uzbrukumiem, kuros gāja bojā desmit cilvēki un 27 cilvēki guva ievainojumus (Eiropols, *European Union Terrorism Situation and Trend Report* ("Ziņojums par terorisma situāciju un tendencēm Eiropas Savienībā"), 2020. gads).

[18] 2019. gadā tika apzināti seši labējo teroristu uzbrukumi (viens pabeigts, viens neveiksmīgs, četri izjaukti: trīs dalībvalstis) salīdzinājumā ar tikai vienu 2018. gadā, un papildu nāves gadījumi lietās, kas netika klasificētas kā terorisms (Eiropols, 2020. gads).

[19] Skatīt arī Padomes paziņojumu par antisemītisma apkarošanu un vienotas drošības pieejas izstrādi, lai labāk aizsargātu ebreju kopienas un institūcijas Eiropā.

[20] ES Pamattiesību aģentūra (2020), *Your rights matter: Security concerns and experiences*

[21] No 2015. gada jūlija līdz 2019. gada beigām Eiropols atrada teroristisku saturu 361 platformā (Eiropols, 2020. gads).

[22] Eiropols (2019), *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism* ("Transatlantiskās paraugprakses apskats radikalizācijas cietumos un teroristu recidīvisma apkarošanā").

[23] *EMCDDA* un Eiropols (2019), *EU Drug Markets Report* ("Ziņojums par ES narkotiku tirgiem").

[24] Eiropols (2015), *Report on Trafficking in Human Beings, Financial Business Model* ("Ziņojums par cilvēku tirdzniecības finanšu uzņēmējdarbības modeli").

starptautiskā tirdzniecība sasniedza 38,9 miljardus EUR[25]. Tajā pašā laikā zemais konfiskācijas līmenis ļauj noziedzniekiem turpināt izvērst savas noziedzīgās darbības un iefiltrēties likumīgajā ekonomikā[26]. Noziedzniekiem un teroristiem ir vieglāk piekļūt šaujamieročiem — tiešsaistes tirgū un izmantojot jaunas tehnoloģijas, piemēram, 3-D drukāšanu[27]. Mākslīgā intelekta, jauno tehnoloģiju un robotikas izmantošana vēl vairāk palielinās risku, ka noziedznieki ļaunprātīgi izmanto inovācijas sniegtās priekšrocības[28].

Šie apdraudējumi aptver dažādas kategorijas un dažādos veidos skar dažādas sabiedrības daļas. Tie visi ir nopietni draudi privātpersonām un uzņēmumiem, un ir vajadzīga visaptveroša un saskaņota reakcija ES līmenī. Ja drošības ievainojamības var rasties pat no mazām, savstarpēji saistītām mājsaimniecības precēm, piemēram, ar internetu savienota ledusskapja vai kafijas automāta, mēs vairs nevaram paļauties tikai uz tradicionālajiem valsts dalībniekiem savas drošības nodrošināšanā. Uzņēmējiem jāuzņemas lielāka atbildība par to produktu un pakalpojumu kiberdrošību, kurus tie laiž tirgū; bet privātpersonām ir jābūt vismaz pamata izpratnei par kiberdrošību, lai varētu sevi aizsargāt.

III. Koordinēta ES reakcija visas sabiedrības labā

ES jau ir parādījusi, kā tā spēj sniegt reālu pievienoto vērtību. Kopš 2015. gada drošības savienība ir radījusi jaunas saiknes attiecībā uz to, kā drošības politika tiek aplūkota ES līmenī. Taču ir jādara vairāk, lai iesaistītu visu sabiedrību, ieskaitot valdības visos līmeņos, uzņēmumus visās nozarēs un privātpersonas visās dalībvalstīs. Pieaugošā informētība par atkarības riskiem[29] un nepieciešamība pēc spēcīgas Eiropas industriālās stratēģijas[30] norāda uz Eiropas Savienību, kurai ir rūpniecības, tehnoloģiju ražošanas un piegādes ķēžu izturētspējas kritiskā masa. Spēks nozīmē arī pamattiesību un ES vērtību pilnīgu ievērošanu: tās ir priekšnoteikums likumīgai, efektīvai un ilgtspējīgai drošības politikai. Šajā Drošības savienības stratēģijā ir izklāstītas konkrētas darbplūsmas, kas jāvirza uz priekšu. Tās pamatā ir šādi kopīgi mērķi:

- ***Spēju un kapacitātes veidošana krīžu agrīnai atklāšanai, novēršanai un ātrai reaģēšanai uz tām:*** Eiropa ir jābūt izturētspējīgākai, lai novērstu turpmākus satricinājumus, pasargātu no tiem un spētu tos izturēt. Mums ir jāveido spējas un kapacitāte agrīnai drošības krīžu atklāšanai un ātrai reaģēšanai uz tām, izmantojot integrētu un koordinētu pieeju gan globālā mērogā, gan ar nozaru iniciatīvu palīdzību (piemēram, finanšu, enerģētikas, tiesu, tiesībaizsardzības, veselības aprūpes, jūrlietu un transporta nozarēs) un pamatojoties uz esošajiem instrumentiem un iniciatīvām[31].

---

[25] ES Intelektuālā īpašuma biroja un ESAO ziņojums "Trade in counterfeit pharmaceutical products" ("Tirdzniecība ar viltotiem farmaceitiskiem produktiem").

[26] Ziņojums par līdzekļu atgūšanu un konfiskāciju: Noziedzība nedrīkst "atmaksāties", COM (2020) 217.

[27] 2017. gadā šaujamieroči tika izmantoti 41 % no visiem teroristu uzbrukumiem (Eiropols, 2018. gads).

[28] Francijas un Nīderlandes tiesībaizsardzības un tiesu iestādes kopā ar Eiropolu un *Eurojust* 2020. gada jūlijā nāca klajā ar kopīgu izmeklēšanu, lai likvidētu šifrētu telefonu tīklu *EncroChat*, ko izmanto noziedzīgi tīkli, kas iesaistīti vardarbīgos uzbrukumos, korupcijā, slepkavību mēģinājumos un liela mēroga narkotisko vielu pārvadāšanā.

[29] Ārvalstu atkarības riski ir saistīti ar lielāku pakļautību potenciāliem apdraudējumiem, sākot ar IT infrastruktūru ievainojamību izmantošanu, kas apdraud kritiskās infrastruktūras (piemēram, enerģētiku, transportu, banku nozari, veselības aizsardzību) vai pārņemot kontroli pār rūpnieciskām vadības sistēmām, un beidzot ar lielāku datu zādzības vai spiegošanas kapacitāti.

[30] Komisijas paziņojums "Jauna Eiropas industriālā stratēģija", COM (2020) 102.

[31] Piemēram, integrētie krīzes situāciju politiskās reaģēšanas (*IPCR*) mehānismi, Ārkārtas reaģēšanas koordinēšanas centrs, Eiropas Komisijas ieteikums par koordinētu reaģēšanu uz plašapmēra kiberdrošības

Komisija arī nāks klajā ar priekšlikumiem par plašu krīzes pārvarēšanas sistēmu Eiropas Savienībā, kas varētu būt nozīmīga arī drošībai.

- ***Orientēšanās uz rezultātiem***: Uz rezultātu panākšanu vērsta stratēģija ir jābalsta uz rūpīgu draudu un risku novērtējumu, lai mūsu centieni būtu pēc iespējas efektīvāki. Tajā ir jādefinē un jāpiemēro pareizie noteikumi un pareizie instrumenti. Tai nepieciešami uzticami stratēģiskie izlūkdati, uz kuriem balstīt ES drošības rīcībpolitikas. Gadījumā, ja nepieciešami ES tiesību akti, stratēģija ir jāņem vērā tā, lai tā tiktu pilnībā īstenota ar nolūku novērst sadrumstalotību un nepilnības, kuras iespējams izmantot. Šīs stratēģijas efektīva īstenošana būs atkarīga arī no atbilstoša finansējuma nodrošināšanas nākamajā plānošanas periodā no 2021. līdz 2027. gadam, tai skaitā attiecīgajām ES aģentūrām.
- ***Visu publiskā un privātā sektora dalībnieku apvienošana kopīgos centienos:*** Galvenie dalībnieki gan publiskajā, gan privātajā sektorā nelabprāt dalījās ar drošībai būtisku informāciju, baidoties apdraudēt vai nu valsts drošību, vai arī konkurētspēju.[32]

  Mēs esam visefektīvākie tad, kad visi iesaistāmies, lai sniegtu atbalstu viens otram. Pirmkārt, tas nozīmē intensīvāku sadarbību dalībvalstu starpā, iesaistot tiesībaizsardzības iestādes, tiesu un valsts pārvaldes iestādes, kā arī ar ES iestādēm un aģentūrām, lai veidotu izpratni un apmaiņas, kas nepieciešamas kopīgu risinājumu rašanai. Būtiska nozīme ir arī sadarbībai ar privāto sektoru, vēl jo vairāk tāpēc, ka nozarei pieder nozīmīga digitālās un nedigitālās infrastruktūras daļa, kas ir būtiska efektīvai noziedzības un terorisma apkarošanai. Arī privātpersonas var dot savu ieguldījumu, piemēram, pilnveidojot prasmes un izpratni nolūkā apkarot kibernoziedzību vai dezinformāciju. Visbeidzot, šiem kopīgajiem centieniem ir jābūt plašākiem par mūsu robežām, veidojot ciešākas saites ar līdzīgi domājošiem partneriem.

IV. Aizsardzība visiem ES: drošības savienības stratēģiskās prioritātes

ES ir unikālas iespējas reaģēt uz šiem jaunajiem, globālajiem apdraudējumiem un problēmām. Iepriekš minētā apdraudējumu analīze norāda uz četrām savstarpēji atkarīgām stratēģiskām prioritātēm, kas jāīsteno ES līmenī, pilnībā ievērojot pamattiesības: i) nākotnes prasībām atbilstoša drošības vide, ii) vēršanās pret jauniem apdraudējumiem, iii) Eiropas iedzīvotāju aizsardzība pret terorismu un organizēto noziedzību, iv) spēcīga Eiropas drošības ekosistēma.

1. Nākotnes prasībām atbilstoša drošības vide

Kritiskās infrastruktūras aizsardzība un izturētspēja

Cilvēki ikdienā paļaujas uz būtiskām infrastruktūrām, lai ceļotu, strādātu, izmantotu tādus nozīmīgus sabiedriskos pakalpojumus kā slimnīcas, transports, energoapgāde vai lai izmantotu savas demokrātiskās tiesības. Ja šīs infrastruktūras nav pietiekami aizsargātas un izturētspējīgas, uzbrukumi var radīt milzīgus fiziskus vai digitālus traucējumus gan atsevišķās dalībvalstīs, gan potenciāli visā ES.

---

incidentiem un krīzēm (C(2017)6100), ES operatīvais protokols hibrīddraudu apkarošanai (*EU Playbook*) (SWD(2016)227).

[32] Kopīgs paziņojums "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību", JOIN(2017) 450.

ES pašreizējais regulējums kritisko infrastruktūru aizsardzībai un izturētspējai[33] nav gājis kopsolī ar mainīgajiem riskiem. Arvien lielāka savstarpējā atkarība nozīmē to, ka traucējumi vienā nozarē var nekavējoties ietekmēt darbības citās nozarēs: uzbrukums elektroenerģijas ražošanai varētu sagraut telesakaru, slimnīcu, banku vai lidostu darbību, savukārt uzbrukums digitālajai infrastruktūrai varētu izraisīt traucējumus elektroenerģijas vai finanšu tīklos. Tā kā mūsu ekonomika un sabiedrība arvien vairāk darbojas tiešsaistē, šādi riski kļūst arvien aktuālāki. Tiesiskajam regulējumam ir jārisina jautājums par šo pieaugošo savstarpējo mijiedarbību un savstarpējo atkarību, izmantojot stingrus kritiskās infrastruktūras aizsardzības un izturētspējas pasākumus — gan kiberpasākumus, gan fiziskus pasākumus. Pamatpakalpojumiem, tostarp tiem, kas balstās uz kosmosa infrastruktūru, jābūt pienācīgi aizsargātiem pret pašreizējiem un gaidāmiem draudiem, taču tiem jābūt arī izturētspējīgiem. Tas nozīmē sistēmas spēju sagatavoties un plānot nevēlamus notikumus, absorbēt tos, atgūties no tiem un sekmīgāk pielāgoties tiem.

Tajā pašā laikā dalībvalstis ir izmantojušas savu rīcības brīvības rezervi, atšķirīgi īstenojot spēkā esošos tiesību aktus. No tā izrietošā sadrumstalotība var iedragāt iekšējo tirgu un apgrūtināt pārrobežu koordināciju, jo īpaši pierobežas reģionos. Operatoriem, kas sniedz pamatpakalpojumus dažādās dalībvalstīs, it jāievēro atšķirīgi ziņošanas režīmi. Komisija pēta, vai **jauns satvars gan fiziskajai, gan digitālajai infrastruktūrai** varētu nodrošināt lielāku konsekvenci un saskaņotāku pieeju uzticamu pamatpakalpojumu sniegšanas nodrošināšanai. Šis satvars ir jāpapildina ar **konkrētām nozarēm paredzētām iniciatīvām**, lai novērstu konkrētos riskus, ar kuriem saskaras kritiskās infrastruktūras, piemēram, transporta, kosmosa, enerģētikas, finanšu un veselības jomā[34]. Ņemot vērā finanšu nozares lielo atkarību no IT pakalpojumiem un tās lielo ievainojamību pret kiberuzbrukumiem, pirmais solis būs iniciatīva par finanšu nozares digitālās darbības izturētspēju. Ņemot vērā energosistēmas īpašo jutīgumu un ietekmi, īpaša iniciatīva atbalstīs kritiskās energoinfrastruktūras lielāku izturētspēju pret fiziskiem draudiem, kiberdraudiem un hibrīddraudiem, nodrošinot vienlīdzīgus konkurences apstākļus energooperatoriem pāri robežām.

Drošībai nozīmīgās sekas, ko rada ārvalstu tiešie ieguldījumi un kas varētu ietekmēt kritiskās infrastruktūras vai kritiskās tehnoloģijas, arī būs atkarīgas no novērtējumiem, ko ES dalībvalstis un Komisija veiks saskaņā ar jauno Eiropas satvaru ārvalstu tiešo ieguldījumu izvērtēšanai[35].

ES var arī izveidot jaunus instrumentus, lai atbalstītu kritisko infrastruktūru izturētspēju. Globālais internets līdz šim ir uzrādījis augstu izturētspējas līmeni, jo īpaši attiecībā uz spēju atbalstīt datplūsmas apjoma pieaugumu. Tomēr mums ir jābūt gataviem iespējamām nākotnes krīzēm, kas apdraud interneta drošību, stabilitāti un izturētspēju. Lai nodrošinātu, ka internets turpina darboties, jābūt noturībai pret kiberincidentiem un ļaunprātīgām

[33] Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā, OV L 194, 19.7.2016.; Padomes Direktīva 2008/114/EK par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību.

[34] Ņemot vērā to, ka veselības nozare ir bijusi pakļauta spriedzei, jo īpaši Covid-19 krīzes laikā, Komisija arī apsvērs iniciatīvas, lai stiprinātu ES veselības drošības sistēmu un atbildīgās ES aģentūras, lai reaģētu uz nopietniem pārrobežu veselības apdraudējumiem.

[35] Līdz ar tās pilnīgu piemērošanu 2020. gada 11. oktobrī Eiropas Parlamenta un Padomes 2019. gada 19. marta Regula (ES) 2019/452, ar ko izveido satvaru ārvalstu tiešo ieguldījumu Savienībā izvērtēšanai, nodrošinās ES jaunu sadarbības mehānismu attiecībā uz tiešajiem ieguldījumiem no trešām valstīm, kuri varētu ietekmēt drošību vai sabiedrisko kārtību. Saskaņā ar regulu dalībvalstis un Komisija novērtēs potenciālos riskus, kas saistīti ar šādiem ĀTI, un, ja tas būs lietderīgi un būtiski vairākām dalībvalstīm, ierosinās piemērotus līdzekļus šo risku mazināšanai.

tiešsaistes darbībām, un jāierobežo atkarība no infrastruktūras un pakalpojumiem, kas atrodas ārpus Eiropas. Tam būs nepieciešama tiesību aktu kombinācija un spēkā esošo noteikumu pārskatīšana, lai nodrošinātu vienādi augsta līmeņa tīklu un informācijas sistēmu drošību ES; papildu investīcijas pētniecībā un inovācijā; un jāizskata interneta pamatinfrastruktūru un resursu, jo īpaši domēnu nosaukumu sistēmas[36], izvēršana vai nostiprināšana.

Svarīgs elements, lai aizsargātu galvenos ES un valstu digitālos resursus, ir piedāvāt kritiskajām infrastruktūrām kanālu drošai saziņai. Komisija sadarbojas ar dalībvalstīm, lai ieviestu sertificētu drošu zemes un kosmosa gala-gala kvantu infrastruktūru apvienojumā ar drošu valdības satelītsakaru sistēmu, kas noteikta Kosmosa programmas regulā[37].

Kiberdrošība

Kiberuzbrukumu skaits turpina pieaugt[38]. Šie uzbrukumi ir sarežģītāki nekā jebkad agrāk, tos veic no dažādiem avotiem Eiropas Savienībā un ārpus tās, un tie ir vērsti uz jomām ar maksimālu ievainojamību. Bieži ir iesaistīti valsts vai valstu atbalstīti dalībnieki, kuru mērķis ir būtiskās digitālās infrastruktūras, piemēram, lielākie mākoņdatošanas pakalpojumu sniedzēji[39]. Kiberriski ir kļuvuši par nozīmīgu apdraudējumu arī finanšu sistēmai. Starptautiskais Valūtas fonds ir aplēsis, ka kiberuzbrukumu radītie ikgadējie zaudējumi ir 9 % no banku neto ienākumiem pasaulē jeb aptuveni 100 miljardi EUR[40]. Pāreja uz savienotām ierīcēm lietotājiem sniegs lielas priekšrocības: taču, tā kā datu centros tiek glabāts un apstrādāts mazāk datu un tie tiek apstrādāti tuvāk lietotājam "perifērijā"[41], kiberdrošība vairs nespēs koncentrēties uz centrālo punktu aizsardzību[42].

2017. gadā ES nāca klajā ar pieeju kiberdrošībai, kuras pamatā ir izturētspējas veidošana, ātra reaģēšana un efektīva atturēšana[43]. ES tagad ir jānodrošina, ka tās kiberdrošības spējas iet kopsolī ar realitāti, lai panāktu izturētspēju un spēju reaģēt. Lai to panāktu, ir vajadzīga patiesa visas sabiedrības pieeja, saskaņā ar kuru ES iestādes, aģentūras un struktūras, dalībvalstis, rūpniecība, akadēmiskās aprindas un privātpersonas piešķir kiberdrošībai vajadzīgo prioritāti[44]. Šī horizontālā pieeja savukārt ir jāpapildina ar konkrētām nozarēm paredzētām kiberdrošības pieejām tādās jomās kā enerģētika, finanšu pakalpojumi, transports vai veselība. Nākamais ES darba posms būtu jāapvieno pārskatītajā Eiropas kiberdrošības stratēģijā.

---

[36] Domēnu nosaukumu sistēma (DNS) ir hierarhiska un decentralizēta nosaukumu sistēma datoriem, pakalpojumiem vai citiem resursiem, kas pieslēgti internetam vai privātam tīklam. Tā pārvērš domēnu vārdus IP adresēs, kas vajadzīgas, lai atrastu un identificētu datorpakalpojumus un ierīces.

[37] Priekšlikums Regulai, ar ko izveido Savienības kosmosa programmu un Eiropas Savienības kosmosa programmas aģentūru. COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Izkliedētās pakalpojumatteices uzbrukumi joprojām ir pastāvīgs apdraudējums: Lielākajiem pakalpojumu sniedzējiem nācās mazināt masveida *DDoS* uzbrukumus, piemēram, uzbrukumu pret *Amazon* tīmekļa pakalpojumiem 2020. gada februārī.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

[41] Perifērdatošana ir izvērsta, atvērta IT arhitektūra, kurai ir decentralizēta datu apstrādes jauda, kas ļauj izmantot mobilās datošanas un lietu interneta tehnoloģijas. Perifērdatošanā datus apstrādā pati ierīce vai vietējais dators vai serveris, nevis tos pārsūta datu centram.

[42] Paziņojums "Eiropas datu stratēģija", COM(2020) 66 final.

[43] Kopīgais paziņojums "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" (*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*), JOIN(2017) 450.

[44] Kopīgā pētniecības centra ziņojums "Kiberdrošība – mūsu digitālais enkurs" sniedz daudzdimensionālu ieskatu kiberdrošības izaugsmē pēdējo 40 gadu laikā.

Jaunu un uzlabotu sadarbības veidu izpētei starp izlūkdienestiem, ES *INTCEN* un citām drošības jomā iesaistītām organizācijām vajadzētu būt daļai no centieniem uzlabot kiberdrošību, kā arī apkarot terorismu, ekstrēmismu, radikālismu un hibrīddraudus.

Ņemot vērā **5G infrastruktūras** notiekošo izvēršanu visā ES un daudzu kritiski svarīgu pakalpojumu potenciālo atkarību no 5G tīkliem, sistēmisku un plaši izplatītu traucējumu sekas būtu īpaši nopietnas. Process, ko Komisija ieviesa ar 2019. gada ieteikumu par 5G tīklu kiberdrošību[45], tagad ir novedis pie konkrētas dalībvalstu rīcības attiecībā uz galvenajiem pasākumiem, kas izklāstīti 5G instrumentu kopumā[46].

Viena no svarīgākajām ilgtermiņa vajadzībām ir attīstīt **ieprojektētas kiberdrošības** kultūru, jau no paša sākuma iekļaujot drošību produktos un pakalpojumos. Svarīgs ieguldījums tajā būs jaunais kiberdrošības sertifikācijas satvars saskaņā ar Kiberdrošības aktu[47]. Satvars jau ir izstrādāts, divas sertifikācijas shēmas jau tiek gatavotas, un prioritātes turpmākām shēmām tiks noteiktas vēlāk šā gada laikā. Šajā jomā ļoti svarīga ir sadarbība starp ES Kiberdrošības aģentūru (*ENISA*), datu aizsardzības iestādēm un Eiropas Datu aizsardzības kolēģiju[48].

Komisija ir arī apzinājusi nepieciešamību pēc **kopējas kibervienības** , lai nodrošinātu strukturētu un koordinētu sadarbību. Tas varētu ietvert savstarpējas palīdzības mehānismu krīzes laikā ES līmenī. Pamatojoties uz konceptuālā ieteikuma[49] īstenošanu, kopējā kibervienība varētu veidot uzticēšanos starp dažādiem Eiropas kiberdrošības ekosistēmas dalībniekiem un piedāvāt būtisku pakalpojumu dalībvalstīm. Komisija sāks diskusijas ar attiecīgajām ieinteresētajām personām (sākot ar dalībvalstīm) un līdz 2020. gada beigām noteiks skaidru procesu, starpposma mērķus un grafiku.

Svarīgi ir arī vienoti noteikumi par informācijas drošību un kiberdrošību ES iestādēm, struktūrām un aģentūrām. Mērķim vajadzētu būt izveidot obligātus un augstus kopējus standartus drošai informācijas apmaiņai un digitālo infrastruktūru un sistēmu drošībai visās ES iestādēs, struktūrās un aģentūrās. Šim jaunajam regulējumam vajadzētu veidot pamatu spēcīgai un efektīvai operatīvajai sadarbībai kiberdrošības jomā visās ES iestādēs, struktūrās un aģentūrās, galveno uzmanību pievēršot ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienībai (*CERT-EU*).

Ņemot vērā tās globālo raksturu, ir būtiski veidot un uzturēt spēcīgas **starptautiskas partnerības**, lai vēl vairāk novērstu kiberuzbrukumus, atturētu no tiem un reaģētu uz tiem. Satvars vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām ("kiberdiplomātijas instrumentu kopums")[50] paredz pasākumus saskaņā ar kopējo ārpolitiku un drošības politiku, ieskaitot ierobežojošus pasākumus (sankcijas), kurus var izmantot pret darbībām, kas kaitē tās politiskajām, drošības un ekonomiskajām interesēm. ES būtu arī jāpadziļina darbs, izmantojot attīstības un sadarbības fondus, lai nodrošinātu kapacitātes veidošanu ar mērķi atbalstīt partnervalstis to digitālo ekosistēmu stiprināšanā, valsts likumdošanas reformu pieņemšanā un starptautisko standartu ievērošanā. Tas palielina visas

[45] Komisijas ieteikums par 5G tīklu kiberdrošību, C(2019) 2335 final. Ieteikums paredz tā pārskatīšanu 2020. gada pēdējā ceturksnī.

[46] Skatīt TID sadarbības grupas 2020. gada 24. jūlija ziņojumu par instrumentu kopuma īstenošanu.

[47] Regula (ES) 2019/881 par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju (Kiberdrošības akts).

[48] Datu aizsardzība kā iedzīvotāju tiesību nodrošināšanas un ES digitālās pārkārtošanās pīlārs — Vispārīgās datu aizsardzības regulas piemērošanas divi gadi, COM(2020) 264.

[49] Komisijas Ieteikums (ES) 2017/1584 par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm.

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/lv/pdf

sabiedrības izturētspēju un spēju pretoties kiberdraudiem un efektīvi reaģēt uz tiem. Tas ietver īpašu darbu pie ES standartu un attiecīgo tiesību aktu popularizēšanas, lai palielinātu kaimiņos esošo partnervalstu kiberdrošību[51].

Sabiedrisku vietu aizsardzība

Nesenie teroristu uzbrukumi bija vērsti uz **sabiedriskām vietām**, tostarp lūgšanu namiem un transporta mezgliem, izmantojot to atvērtību un pieejamību. Terorisma pieaugums, ko izraisīja politiski vai ideoloģiski motivēts ekstrēmisms, ir padarījis šo apdraudējumu vēl aktuālāku. Tāpēc nepieciešama gan šādu vietu spēcīgāka fiziskā aizsardzība, gan atbilstošas atklāšanas sistēmas, neapdraudot iedzīvotāju brīvības[52]. Komisija pastiprinās publiskā un privātā sektora sadarbību sabiedrisko vietu aizsardzībai, izmantojot finansējumu, pieredzes un labas prakses apmaiņu, īpašus norādījumus[53] un ieteikumus[54]. Pieeja ietvers arī informētības palielināšanu, prasības attiecībā uz darbības rezultātiem un atklāšanas iekārtu testēšanu, kā arī iepriekšējās darbības pārbaužu uzlabošanu, lai novērstu iekšnieku draudus. Svarīgs aspekts, kas jāņem vērā, ir tas, ka minoritātes un neaizsargātas personas var tikt nesamērīgi ietekmētas, tostarp personas, pret kurām uzbrukumi vērsti viņu reliģijas vai dzimuma dēļ, un tādēļ tām jāpievērš īpaša uzmanība. Reģionālajām un vietējām publiskajām iestādēm ir svarīga loma sabiedrisko vietu drošības uzlabošanā. Komisija arī palīdz veicināt pilsētu inovācijas sabiedrisko vietu drošības jomā[55]. Jaunas pilsētprogrammas[56] partnerības saistībā ar "drošību sabiedriskās vietās" uzsākšana 2018. gada novembrī atspoguļo dalībvalstu, Komisijas un pilsētu stingro apņemšanos labāk novērst draudus drošībai pilsētu teritorijā.

Dronu tirgus turpina paplašināties, un tiem ir daudz vērtīgu un likumīgu lietojumu. Tomēr tos var potenciāli ļaunprātīgi izmantot arī noziedznieki un teroristi, un sabiedriskās vietas ir īpaši apdraudētas. Mērķi var būt privātpersonas, cilvēku pulcēšanās, kritiskā infrastruktūra, tiesībaizsardzības iestādes, robežas vai sabiedriskas vietas. Zināšanas par dronu izmantošanu konflikta laikā varētu nonākt atpakaļ Eiropā vai nu tieši (ar ārvalstu kaujinieku teroristu, kuri atgriežas, starpniecību), vai tiešsaistē. Eiropas Aviācijas drošības aģentūras jau izstrādātie noteikumi ir svarīgs pirmais solis tādās jomās kā dronu ekspluatantu reģistrācija un dronu obligāta attālināta identifikācija. Tā kā droni kļūst arvien plašāk pieejami, lētāki un spējīgāki, ir vajadzīga papildu rīcība. Tā varētu ietvert informācijas apmaiņu, norādījumus un labu praksi, ko varētu izmantot visi, tai skaitā tiesībaizsardzības iestādes, kā arī dronu pretpasākumu lielāku testēšanu[57]. Turklāt būtu sīkāk jāanalizē un jārisina ietekme uz privātumu un datu aizsardzību, ko rada dronu izmantošana sabiedriskās vietās.

---

[51] Skatīt Padomes 2018. gada 26. jūnija secinājumos pieņemtās nostādnes ES ārējo kiberspēju veidošanai.

[52] Attālinātas biometriskās identifikācijas sistēmas ir īpaši rūpīgi jāpārbauda. Komisijas sākotnējie uzskati ir izklāstīti Komisijas 2020. gada 19. februāra Baltajā grāmatā par mākslīgo intelektu, COM(2020) 65.

[53] Piemēram, Norādījumi par piemērotu drošības barjeru risinājumu izvēli sabiedrisko vietu aizsardzībai (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Norādījumi par labu praksi ir sniegti SWD(2019) 140, tai skaitā iedaļā par publiskā un privātā sektora sadarbību. Finansējums no IDF–Policija ir īpaši vērsts uz publiskā un privātā sektora sadarbības uzlabošanu.

[55] Trīs pilsētas (Pireja Grieķijā, Tampere Somijā un Turīna Itālijā) izmēģinās jaunus risinājumus kā daļu no inovatīvām pilsētvides darbībām, ko līdzfinansē Eiropas Reģionālās attīstības fonds (ERAF).

[56] ES pilsētprogramma ir jauna vairāklīmeņu darba metode, kas veicina sadarbību starp dalībvalstīm, pilsētām, Eiropas Komisiju un citām ieinteresētajām personām, lai veicinātu izaugsmi, apdzīvojamību un inovāciju Eiropas pilsētās un lai apzinātu un sekmīgi risinātu sociālās problēmas.

[57] Nesen tika izveidota daudzgadu testēšanas programma, lai palīdzētu dalībvalstīm izstrādāt kopīgu metodiku un testēšanas platformu šajā jomā.

Galvenās darbības
• Tiesību akti par kritiskās infrastruktūras aizsardzību un izturētspēju • Tīklu un informācijas sistēmu direktīvas pārskatīšana • Iniciatīva par finanšu nozares darbības izturētspēju • Kritiskās enerģētikas infrastruktūras aizsardzība un kiberdrošība un tīkla kodekss par pārrobežu elektroenerģijas plūsmu kiberdrošību • Eiropas kiberdrošības stratēģija • Turpmākie pasākumi kopējas kibervienības izveidošanai • Vienoti noteikumi par informācijas drošību un kiberdrošību ES iestādēm, struktūrām un aģentūrām • Pastiprināta sadarbība sabiedrisko vietu, ieskaitot lūgšanu namu, aizsardzībai • Paraugprakses apmaiņa par dronu ļaunprātīgas izmantošanas novēršanu

2. Vēršanās pret jauniem apdraudējumiem

Kibernoziedzība

Tehnoloģija sniedz jaunas iespējas sabiedrībai. Tā piedāvā arī jaunus instrumentus tiesu iestādēm un tiesībaizsardzībai. Taču tajā pašā laikā tas paver iespējas noziedzniekiem. Pieaug gan ļaunprogrammatūras izmantošana, gan personas vai uzņēmējdarbības datu zādzība uzlaušanas ceļā un digitālās darbības pārtraukšana, kas rada finansiālu vai reputācijas kaitējumu. Spēcīgas kiberdrošības radītā izturētspējīgā vide ir pirmā aizsardzība. Tiesībaizsardzības iestādēm jāspēj strādāt digitālās izmeklēšanas jomā ar skaidriem noteikumiem, lai izmeklētu noziegumus, sauktu pie atbildības par tiem un sniegtu cietušajiem nepieciešamo aizsardzību. Šā darba pamatā vajadzētu būt Eiropola Kopīgajai kibernoziedzības apkarošanas darba grupai un tiesībaizsardzības iestāžu ārkārtas reaģēšanas protokolam, kas izveidots, lai koordinētu reaģēšanu uz liela mēroga kiberuzbrukumiem. Svarīgi ir arī efektīvi mehānismi, kas nodrošina publiskā un privātā sektora partnerības un sadarbību.

Līdztekus cīņai pret kibernoziedzību vajadzētu kļūt par stratēģiskās komunikācijas prioritāti visā ES, lai brīdinātu Eiropas iedzīvotājus par riskiem un preventīvajiem pasākumiem, ko viņi varētu veikt. Tam vajadzētu būt daļai no proaktīvas pieejas. Būtisks solis ir arī pašreizējā tiesiskā regulējuma[58] pilnīga īstenošana: Komisija būs gatava vajadzības gadījumā izmantot pārkāpuma procedūras, kā arī pastāvīgi pārskatīt šo regulējumu, lai nodrošinātu, ka tas joprojām atbilst paredzētajam mērķim. Komisija kopā ar Eiropolu un ES Kiberdrošības aģentūru (*ENISA*) arī pētīs, vai ir iespējams izveidot ar kibernoziedzību saistītu ES ātrās brīdināšanas sistēmu, kas varētu nodrošināt informācijas plūsmu un ātru reakciju kibernoziedzības pieauguma gadījumā.

Kibernoziedzība ir globāla problēma, kurā ir vajadzīga efektīva starptautiskā sadarbība. ES atbalsta Eiropas Padomes Budapeštas Konvenciju par kibernoziedzību, kas ir efektīvs un labi izstrādāts satvars, kurš ļauj visām valstīm noteikt, kādas sistēmas un saziņas kanāli tām ir jāievieš, lai varētu efektīvi sadarboties savā starpā.

Gandrīz puse ES iedzīvotāju raizējas par datu ļaunprātīgu izmantošanu[59] un **identitātes zādzību**[60]. Viens no aspektiem ir identitātes krāpnieciska izmantošana finansiāla labuma

[58] Direktīva 2013/40/ES par uzbrukumiem informācijas sistēmām.

[59] 46 % (Eirobarometrs par eiropiešu attieksmi pret kiberdrošību, 2020. gada janvāris).

gūšanai, taču tam var būt arī ievērojama personiska un psiholoģiska ietekme, jo identitātes zagļa nelikumīgi izvietotā informācija tiešsaistē var saglabāties gadiem ilgi. Komisija izpētīs iespējamos praktiskos pasākumus cietušo aizsardzībai pret visu veidu identitātes zādzībām, ņemot vērā gaidāmo Eiropas digitālās identitātes iniciatīvu[61].

Kibernoziedzības apkarošana nozīmē raudzīšanos nākotnē. Tā kā sabiedrība izmanto jaunu tehnoloģiju attīstību, lai stiprinātu ekonomiku un sabiedrību, noziedznieki var arī mēģināt izmantot šos instrumentus negatīviem mērķiem. Piemēram, noziedznieki var izmantot mākslīgo intelektu, lai atklātu un identificētu paroles vai vienkāršotu ļaunprogrammatūras radīšanu, izmantotu attēlus un audioierakstus, kurus pēc tam var izmantot identitātes zādzībai vai viltošanai.

Moderna tiesībaizsardzība

Tiesībaizsardzības un tiesu iestāžu darbiniekiem ir jāpielāgojas jaunajām tehnoloģijām. Tehnoloģiju attīstība un jauni apdraudējumi nozīmē, ka tiesībaizsardzības iestādēm ir jāpiekļūst jauniem rīkiem, jāapgūst jaunas prasmes un jāizstrādā alternatīvas izmeklēšanas metodes. Lai papildinātu likumdošanas darbības, kuru mērķis ir uzlabot pārrobežu piekļuvi elektroniskiem pierādījumiem kriminālizmeklēšanā, ES var palīdzēt tiesībaizsardzības iestādēm attīstīt vajadzīgās spējas identificēt, nodrošināt un lasīt datus, kas vajadzīgi noziegumu izmeklēšanai, un izmantot šos datus kā pierādījumus tiesā. Komisija izpētīs pasākumus, ar kuriem **uzlabot tiesībaizsardzības spējas digitālās izmeklēšanas jomā**, nosakot, kā vislabāk izmantot pētniecību un izstrādi, lai radītu jaunus instrumentus tiesībaizsardzībai, un kā apmācība var piedāvāt pareizo prasmju kopumu tiesībaizsardzības un tiesu iestādēm. Tas ietvers arī stingru zinātnisku novērtējumu un testēšanas metožu nodrošināšanu ar Komisijas Kopīgā pētniecības centra starpniecību.

Kopīgas pieejas var arī nodrošināt, ka **mākslīgais intelekts, spējas kosmosa jomā, lielie dati** un **augstas veiktspējas datošana tiek integrēti** drošības politikā veidā, kas ir efektīvs gan noziedzības apkarošanā, gan pamattiesību nodrošināšanā. Mākslīgais intelekts varētu būt iedarbīgs instruments noziedzības apkarošanai, kas rada milzīgas izmeklēšanas spējas, analizējot lielu informācijas apjomu un identificējot modeļus un anomālijas[62]. Tas var arī nodrošināt konkrētus instrumentus, piemēram, palīdzēt identificēt teroristisku saturu tiešsaistē, atklāt aizdomīgus darījumus bīstamu produktu pārdošanā vai piedāvāt palīdzību iedzīvotājiem ārkārtas situācijās. Lai realizētu šo potenciālu, ir jāapvieno pētniecība, inovācija un mākslīgā intelekta lietotāji ar pareizo pārvaldību un tehnisko infrastruktūru, aktīvi iesaistot privāto sektoru un akadēmiskās aprindas. Tas nozīmē arī to, ka ir jānodrošina visaugstākie standarti pamattiesību ievērošanai, vienlaikus nodrošinot iedzīvotāju efektīvu aizsardzību. Proti, lēmumi, kas ietekmē privātpersonas, ir jāpārbauda cilvēkiem, un tiem ir jāatbilst attiecīgajiem piemērojamajiem ES tiesību aktiem[63].

---

[60] Vairākums respondentu 2018. gada Eirobarometra aptaujā "Eiropiešu attieksme pret interneta drošību" (95 %) uzskata, ka identitātes zādzība ir smags noziedzīgs nodarījums, un septiņi no desmit apgalvo, ka tas ir ļoti smags noziedzīgs nodarījums. Eirobarometrs, kas publicēts 2020. gada janvārī, apstiprināja bažas par kibernoziedzību, krāpšanu tiešsaistē un identitātes zādzību: divas trešdaļas respondentu ir norūpējušies par krāpšanos banku darījumos (67 %) vai identitātes zādzību (66 %).

[61] 2020. gada 19. februāra Paziņojums "Eiropas digitālās nākotnes veidošana", COM(2020)67.

[62] Piemēram, finanšu noziegumos.

[63] Tas nozīmē atbilstību spēkā esošajiem tiesību aktiem, tostarp Vispārīgajai datu aizsardzības regulai (ES) 2016/679, kā arī Datu aizsardzības tiesībaizsardzības direktīvai (ES) 2016/680, kas reglamentē personas datu apstrādi, lai atklātu, novērstu, izmeklētu noziedzīgus nodarījumus un sauktu pie atbildības par tiem vai izpildītu krimināsodus.

Elektroniskā informācija un pierādījumi ir vajadzīgi aptuveni 85 % smagu noziegumu izmeklēšanās, savukārt 65 % no visiem pieprasījumiem tiek nosūtīti pakalpojumu sniedzējiem, kas atrodas citā jurisdikcijā[64]. Tas, ka tradicionālās fiziskās pēdas ir pārvietojušās tiešsaistē, vēl vairāk palielina plaisu starp tiesībaizsardzības iestāžu un noziedznieku spējām. Ir svarīgi ieviest skaidrus noteikumus par pārrobežu piekļuvi elektroniskiem pierādījumiem kriminālizmeklēšanā. Tāpēc Eiropas Parlamentam un Padomei ir svarīgi ātri pieņemt priekšlikumus par e-pierādījumiem, lai praktiķiem nodrošinātu efektīvu rīku. Pārrobežu piekļuve e-pierādījumiem, izmantojot daudzpusējas un divpusējas starptautiskas sarunas, arī ir būtiska, lai starptautiskā līmenī izveidotu saderīgus noteikumus[65].

Piekļuve digitālajiem pierādījumiem arī ir atkarīga no informācijas pieejamības. Ja datus izdzēš pārāk ātri, var pazust svarīgi pierādījumi, tāpēc vairs nav iespējams identificēt un atrast aizdomās turētos un noziedzīgos tīklus (kā arī cietušos). No otras puses, datu saglabāšanas shēmas rada jautājumus par privātuma aizsardzību. Atkarībā no Eiropas Savienības Tiesā izskatāmo lietu iznākuma Komisija izvērtēs datu saglabāšanas turpmāko virzību.

Piekļuve interneta domēna nosaukumu reģistrācijas informācijai ("*WHOIS* dati")[66] ir svarīga kriminālizmeklēšanai, kiberdrošībai un patērētāju aizsardzībai. Tomēr piekļuve šai informācijai kļūst arvien sarežģītāka, kamēr Piešķirto nosaukumu un numuru interneta korporācija (*ICANN*) nav pieņēmusi jaunu *WHOIS* politiku. Komisija turpinās sadarboties ar *ICANN* un daudzpusējo ieinteresēto personu kopienu, lai nodrošinātu, ka likumīgie piekļuves prasītāji, tostarp tiesībaizsardzības iestādes, var iegūt efektīvu piekļuvi *WHOIS* datiem saskaņā ar ES un starptautiskajiem datu aizsardzības noteikumiem. Tas ietvers iespējamo risinājumu izvērtēšanu, tai skaitā to, vai var būt vajadzīgi tiesību akti, lai precizētu noteikumus par piekļuvi šādai informācijai.

Pēc **mobilo telekomunikāciju 5G arhitektūras** pilnīgas ieviešanas Eiropas Savienībā, ievērojot sakaru konfidencialitāti, tiesībaizsardzības un tiesu iestādēm arī jābūt aprīkotām, lai iegūtu vajadzīgos datus un pierādījumus. Komisija atbalstīs uzlabotu un koordinētu pieeju, izstrādājot starptautiskus standartus, definējot paraugpraksi, procesu un tehnisko sadarbspēju tādās svarīgās tehnoloģiju jomās kā mākslīgais intelekts, lietu internets vai blokķēžu tehnoloģijas.

Patlaban ievērojama daļa izmeklēšanu, kas vērstas pret visu veidu noziedzību un terorismu, ir saistīta ar **šifrētu informāciju**. Šifrēšana ir būtiska digitālajai pasaulei, nodrošinot digitālās sistēmas un darījumus, kā arī aizsargājot vairākas pamattiesības, tostarp vārda brīvību, privātumu un datu aizsardzību. Tomēr, ja to izmanto noziedzīgiem mērķiem, tā var arī slēpt noziedznieku identitāti un viņu saziņas saturu. Komisija izpētīs un atbalstīs līdzsvarotus tehniskus, operatīvus un juridiskus problēmu risinājumus un veicinās tādu pieeju, kas saglabā šifrēšanas efektivitāti privātuma un sakaru drošības aizsardzībā, vienlaikus efektīvi reaģējot uz noziedzību un terorismu.

Cīņa pret nelikumīgu saturu tiešsaistē

Lai saskaņotu tiešsaistes un fiziskās vides drošību, ir vajadzīgi nepārtraukti pasākumi **cīņā pret nelikumīgu saturu tiešsaistē**. Arvien vairāk un vairāk galvenie apdraudējumi

[64] Komisijas SWD (2018) 118 final.

[65] Proti, Eiropas Padomes Budapeštas konvencijas par kibernoziegumiem Otrais papildprotokols un nolīgums starp ES un Amerikas Savienotajām Valstīm par pārrobežu piekļuvi e-pierādījumiem.

[66] Glabāti datubāzēs, ko uztur 2500 reģistru un reģistratoru operatori, kas atrodas visā pasaulē.

iedzīvotājiem, piemēram, terorisms, ekstrēmisms vai seksuāla vardarbība pret bērniem, ir atkarīgi no digitālās vides: ir vajadzīga konkrēta rīcība un regulējums, lai nodrošinātu pamattiesību ievērošanu. Būtisks pirmais solis ir ātri pabeigt sarunas par ierosināto tiesību aktu par teroristisku saturu tiešsaistē[67] un nodrošināt tā īstenošanu. Lai cīnītos pret to, ka teroristi, vardarbīgi ekstrēmisti un noziedznieki ļaunprātīgi izmanto internetu, būtiski ir arī stiprināt tiesībaizsardzības iestāžu un privātā sektora brīvprātīgu sadarbību **ES Interneta forumā**. Eiropola ES vienībai ziņošanai par interneta saturu arī turpmāk būs izšķiroša nozīme, uzraugot teroristu grupējumu darbību tiešsaistē un platformu veiktos pasākumus[68], kā arī turpinot pilnveidot **ES Krīžu protokolu**[69]. Turklāt Komisija turpinās sadarboties ar starptautiskajiem partneriem, tai skaitā piedaloties **Globālajā Interneta forumā terorisma apkarošanai**, lai risinātu šīs problēmas pasaules mērogā. Turpināsies darbs, lai atbalstītu alternatīvu vēstījumu un atbildes vēstījumu izstrādi, izmantojot programmu "Iespējas pilsoniskajai sabiedrībai"[70].

Lai novērstu un apkarotu nelikumīgu naidīgu izteikumu izplatīšanos tiešsaistē, Komisija 2016. gadā nāca klajā ar Rīcības kodeksu cīņai pret nelikumīgiem naidīgiem izteikumiem tiešsaistē, un tiešsaistes platformas brīvprātīgi apņēmās dzēst saturu ar naidīgiem izteikumiem. Jaunākais novērtējums liecina, ka uzņēmumi izvērtē 90 % no iezīmētā satura 24 stundu laikā un izņem 71 % no satura, kas tiek uzskatīts par nelikumīgiem naidīgiem izteikumiem. Tomēr platformām vēl vairāk jāuzlabo pārredzamība un atgriezeniskā saite ar lietotājiem, kā arī jānodrošina iezīmēta satura konsekventa novērtēšana[71].

ES Interneta forums arī sekmēs informācijas apmaiņu par esošajām un topošajām tehnoloģijām, lai risinātu problēmas, kas saistītas ar seksuālu vardarbību pret bērniem tiešsaistē. Cīņa pret seksuālu vardarbību pret bērniem tiešsaistē ir pamats jaunai stratēģijai, kuras mērķis ir pastiprināt **cīņu pret seksuālu vardarbību pret bērniem**[72] un maksimāli izmantot ES līmenī pieejamos instrumentus, lai apkarotu šos noziegumus. Uzņēmumiem ir jāspēj turpināt darbu, lai atklātu un izņemtu materiālus tiešsaistē, kuros atspoguļota seksuāla vardarbība pret bērniem, un šo materiālu radītais kaitējums prasa izveidot satvaru, kurā būtu noteikti skaidri un pastāvīgi pienākumi risināt šo problēmu. Stratēģijā arī tiks paziņots, ka Komisija arī sāks sagatavot nozaru tiesību aktus, lai efektīvāk risinātu jautājumu par seksuālu vardarbību pret bērniem tiešsaistē, vienlaikus pilnībā ievērojot pamattiesības.

Vispārīgāk runājot, gaidāmajā digitālo pakalpojumu tiesību aktā tiks precizēti un atjaunināti arī atbildības un drošības noteikumi attiecībā uz digitālajiem pakalpojumiem un novērsti šķēršļi, kas kavē rīcību, lai vērstos pret nelikumīgu saturu, precēm vai pakalpojumiem.

Turklāt Komisija turpinās sadarboties ar starptautiskajiem partneriem un **Globālo interneta forumu terorisma apkarošanai**, tostarp ar neatkarīgās padomdevējas komitejas starpniecību, lai apspriestu, kā risināt šīs problēmas globālā līmenī, vienlaikus saglabājot ES vērtības un pamattiesības. Būtu jāpievēršas arī jauniem tematiem, piemēram, algoritmiem vai tiešsaistes azartspēlēm[73].

---

[67] Priekšlikums par to, kā novērst teroristiska satura izplatīšanu tiešsaistē, COM(2018)640, 2018. gada 12. septembris.

[68] Eiropols, 2019. gada novembris.

[69] *A Europe that protects — EU Crisis Protocol: responding to terrorist content online* ("Eiropa, kas aizsargā: ES Krīžu protokols — reaģēšana uz teroristisku saturu tiešsaistē"), (2019. gada oktobris)

[70] Saistīta ar Radikalizācijas izpratnes programmas darbu, skatīt IV iedaļas 3. punktu.

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] ES stratēģija seksuālas vardarbības pret bērniem efektīvākai apkarošanai, COM(2020) 607.

[73] Teroristi arvien vairāk izmanto spēļu platformu ziņojumapmaiņas sistēmu apmaiņai, un jaunie teroristi videospēlēs arī atkārtoti izspēlē vardarbīgus uzbrukumus.

Hibrīddraudi

Hibrīddraudu mērogs un daudzveidība patlaban ir nepieredzēti. To vēl vairāk pierādīja Covid-19 krīze, jo vairāki valsts un nevalstiskie dalībnieki centās instrumentalizēt pandēmiju, jo īpaši, manipulējot ar informācijas vidi un radot problēmas galvenajām infrastruktūrām. Tas var vājināt sociālo kohēziju un iedragāt uzticēšanos ES iestādēm un dalībvalstu valdībām.

ES pieeja hibrīddraudiem ir izklāstīta 2016. gada kopīgajā regulējumā[74] un 2018. gada kopīgajā paziņojumā par noturības palielināšanu pret hibrīddraudiem[75]. ES līmeņa rīcības pamatā ir apjomīgs instrumentu kopums, kas aptver iekšējo un ārējo saikni un kura pamatā ir visas sabiedrības pieeja un cieša sadarbība ar stratēģiskajiem partneriem, jo īpaši NATO un G7. Kopā ar šo stratēģiju ir publicēts ziņojums par to, kā tiek īstenota ES pieeja hibrīddraudiem[76]. Pamatojoties uz kartēšanu[77], ar kuru nākts klajā līdztekus šai stratēģijai, Komisijas dienesti un Eiropas Ārējās darbības dienests izveidos **ierobežotas pieejamības tiešsaistes platformu**, kurā dalībvalstis varēs izmantot hibrīddraudu novēršanas rīkus un pasākumus ES līmenī.

Tā kā būtisko saikņu ar valsts drošības un aizsardzības politiku dēļ par hibrīddraudu apkarošanu galvenokārt ir atbildīgas dalībvalstis, dažas ievainojamības ir kopīgas visām dalībvalstīm un daži apdraudējumi sniedzas pāri robežām, piemēram, vēršas pret pārrobežu tīkliem vai infrastruktūru. Komisija un Augstais pārstāvis izstrādās ES pieeju hibrīddraudiem, integrējot ārējo un iekšējo dimensiju vienotā plūsmā un apvienojot valstu un ES mēroga apsvērumus. Tam jāaptver viss darbību spektrs – sākot ar agrīnu atklāšanu, analīzi, informētību, izturētspējas veidošanu un profilaksi un beidzot ar reaģēšanu uz krīzēm un to seku pārvarēšanu.

Papildus pastiprinātai īstenošanai, hibrīddraudiem pastāvīgi attīstoties, īpaša uzmanība tiks pievērsta **hibrīddraudu apsvērumu integrēšanai politikas veidošanā,** lai neatpaliktu no dinamiskās attīstības un nodrošinātu, ka neviena potenciāli nozīmīga iniciatīva netiek atstāta novārtā. Ietekme, ko rada jaunas iniciatīvas, tiks novērtēta arī, ņemot vērā hibrīddraudu aspektus, ieskaitot iniciatīvas jomās, kas līdz šim nav bijušas hibrīddraudu novēršanas regulējuma darbības jomā, piemēram, izglītībā, tehnoloģijās un pētniecībā. Šādai pieejai par labu nāktu darbs, kas paveikts hibrīddraudu konceptualizācijas jomā, kas sniedz visaptverošu pārskatu par dažādajiem instrumentiem, kurus var izmantot pretinieki[78]. Mērķim vajadzētu būt nodrošināt, ka lēmumu pieņemšanas procesa pamatā ir regulāri, visaptveroši, uz izlūkdatiem balstīti ziņojumi par hibrīddraudu attīstību. Tas ļoti lielā mērā būs balstīts uz dalībvalstu izlūkdatiem un izlūkošanas sadarbības turpmāku uzlabošanu ar dalībvalstu kompetentajiem dienestiem, izmantojot ES *INTCEN*.

Lai uzlabotu **situācijas apzināšanos**, Komisijas dienesti un Eiropas Ārējās darbības dienests izskatīs iespējas racionalizēt informācijas plūsmas no dažādiem avotiem, tostarp dalībvalstīm, kā arī ES aģentūrām, piemēram, *ENISA*, Eiropola un *Frontex*. ES Hibrīddraudu analīzes vienība arī turpmāk būs ES galvenā struktūra hibrīddraudu novērtēšanai. **Izturētspējas veidošanai** ir centrāla nozīme hibrīddraudu novēršanā un

[74] Kopīgs regulējums hibrīddraudu apkarošanai — Eiropas Savienības reakcija, JOIN (2016) 18.

[75] Noturības un spēju palielināšana cīņā ar hibrīddraudiem, JOIN (2018) 16.

[76] Ziņojums par 2016. gada kopīgā regulējuma hibrīddraudu apkarošanai un 2018. gada kopīgā paziņojuma par noturības un spēju palielināšanu cīņā ar hibrīddraudiem īstenošanu, SWD(2020) 153.

[77] Ar izturētspējas uzlabošanu un hibrīddraudu apkarošanu saistīto pasākumu kartēšana, SWD(2020) 152.

[78] Hibrīddraudu aina: konceptuālais modelis, JRC117280, ko kopīgi izstrādājis Kopīgais pētniecības centrs un Izcilības centrs hibrīddraudu novēršanai.

aizsardzībā pret tiem. Tādēļ ir izšķiroši svarīgi sistemātiski sekot līdzi progresam šajā jomā un objektīvi novērtēt to. Pirmais solis būs noteikt hibrīddraudu izturētspējas pamatlīmeni nozarēs gan dalībvalstīm, gan ES iestādēm un struktūrām. Visbeidzot, lai uzlabotu **gatavību reaģēt uz hibrīddraudu krīzēm**, spēkā esošais protokols būtu jāpārskata, kā noteikts 2016. gada ES operatīvajā protokolā[79], atspoguļojot pašlaik izskatāmās ES krīzes reaģēšanas sistēmas plašāku pārskatīšanu un stiprināšanu[80]. Mērķis ir maksimāli palielināt ES rīcības efektivitāti, ātri apvienojot nozaru atbildes pasākumus un nodrošinot netraucētu sadarbību ar mūsu partneriem, pirmkārt, NATO.

Galvenās darbības
• Nodrošināt, ka tiesību akti kibernoziedzības jomā tiek īstenoti un atbilst paredzētajam mērķim • Stratēģija efektīvākai cīņai pret seksuālu vardarbību pret bērniem • Priekšlikumi par tādu materiālu atklāšanu un izņemšanu, kas satur seksuālu vardarbību pret bērniem • ES pieeja hibrīddraudu apkarošanai • ES operatīvā protokola hibrīddraudu apkarošanai (*EU Playbook*) pārskatīšana • Novērtējums, kā uzlabot tiesībaizsardzības iestāžu spējas digitālās izmeklēšanas jomā

3. Eiropas iedzīvotāju aizsardzība pret terorismu un organizēto noziedzību

Terorisms un radikalizācija

ES joprojām ir augsts terorisma draudu līmenis. Neraugoties uz uzbrukumu skaita samazināšanos kopumā, tiem joprojām var būt postoša ietekme. Radikalizācija var arī plašāk polarizēt un destabilizēt sociālo kohēziju. Cīņā pret terorismu un radikalizāciju galvenā atbildība gulstas uz dalībvalstīm. Tomēr draudu arvien pieaugošā pārrobežu/starpnozaru dimensija nozīmē, ka ir vajadzīgi papildu pasākumi ES sadarbības un koordinācijas līmenī. Prioritāte ir efektīvi īstenot ES terorisma apkarošanas tiesību aktus, tostarp ierobežojošos pasākumus[81]. Mērķis joprojām ir paplašināt Eiropas Prokuratūras pilnvaras, attiecinot tās arī uz pārrobežu teroristu noziegumiem.

Terorisma apkarošana sākas ar tā pamatcēloņu novēršanu. Sabiedrības polarizācija, reāla vai šķietama diskriminācija un citi psiholoģiski un socioloģiski faktori var pastiprināt cilvēku neaizsargātību pret radikāliem izteikumiem. Šajā kontekstā **radikalizācijas** apkarošana ir cieši saistīta ar sociālās kohēzijas veicināšanu vietējā, valsts un Eiropas līmenī. Pēdējā desmitgadē ir izstrādātas vairākas ietekmīgas iniciatīvas un rīcībpolitikas, jo īpaši ar Radikalizācijas izpratnes tīkla un ES iniciatīvas "Pilsētas pret radikalizāciju"[82] starpniecību. Tagad ir pienācis laiks apsvērt darbības, lai racionalizētu ES politiku, iniciatīvas un līdzekļus radikalizācijas apkarošanai. Šādas darbības var atbalstīt spēju un prasmju attīstību,

[79] ES operatīvais protokols hibrīddraudu apkarošanai (*EU Playbook*), SWD(2016) 227.

[80] Pēc videokonferences, kas notika 2020. gada 26. martā, Eiropadomes locekļi pieņēma paziņojumu par ES rīcību, reaģējot uz Covid-19 uzliesmojumu, aicinot Komisiju nākt klajā ar priekšlikumiem par vērienīgāku un plašāku krīzes pārvarēšanas sistēmu Eiropas Savienībā.

[81] Padome pieņēma ierobežojošus pasākumus attiecībā uz *ISIL* (*Da'esh*) un *Al-Qaida*, kā arī īpašus ierobežojošus pasākumus, kas terorisma apkarošanas nolūkā vērsti pret konkrētām personām un organizācijām. Pārskatu par visiem ierobežojošajiem pasākumiem skatīt ES sankciju kartē (https://www.sanctionsmap.eu/#/main).

[82] Izmēģinājuma iniciatīvai "ES pilsētas pret radikalizāciju" ir divkāršs mērķis: veicināt pieredzes apmaiņu starp ES pilsētām un apkopot atsauksmes par to, kā vislabāk atbalstīt vietējās kopienas ES līmenī.

uzlabot sadarbību, stiprināt pierādījumu bāzi un palīdzēt novērtēt progresu, iesaistot visas attiecīgās ieinteresētās personas, tostarp pirmās līnijas speciālistus, politikas veidotājus un akadēmiskās aprindas[83]. "Maigā politika", piemēram, izglītības, kultūras, jaunatnes un sporta jomā, varētu veicināt radikalizācijas novēršanu, sniedzot iespējas riskam pakļautajiem jauniešiem un veicinot kohēziju Eiropas Savienībā[84]. Prioritārās jomas ietver darbu pie agrīnas atklāšanas un riska pārvaldības, izturētspējas veidošanas un distancēšanās, kā arī rehabilitācijas un reintegrācijas sabiedrībā.

Teroristi ir centušies iegūt un pielāgot militārām vajadzībām **ķīmiskos, bioloģiskos, radioloģiskos un kodolmateriālus** (*CBRN*)[85], kā arī attīstīt zināšanas un spēju tos izmantot[86]. Potenciāls, kāds būtu uzbrukumiem ar *CBRN* vielām, ieņem svarīgu vietu teroristu propagandā. Tā kā iespējamais kaitējums ir ārkārtīgi liels, ir jāpievērš īpaša uzmanība. Pamatojoties uz pieeju, ko izmanto, lai regulētu piekļuvi sprāgstvielu prekursoriem, Komisija izskatīs iespēju ierobežot piekļuvi dažām bīstamām ķīmiskām vielām, ko varētu izmantot uzbrukumu veikšanai. Būtiska nozīme būs arī ES civilās aizsardzības reaģēšanas spēju (*rescEU*) attīstīšanai *CBRN* jomā. Sadarbība ar trešām valstīm ir svarīga arī, lai stiprinātu kopēju *CBRN* drošuma un drošības kultūru, pilnībā izmantojot ES globālos *CBRN* izcilības centrus. Šī sadarbība ietvers valstu nepilnību un riska novērtējumus, atbalstu valstu un reģionāliem *CBRN* rīcības plāniem, labas prakses apmaiņu un *CBRN* spēju veidošanas pasākumus.

ES ir izstrādājusi visprogresīvākos tiesību aktus pasaulē, lai ierobežotu piekļuvi **sprāgstvielu prekursoriem**[87] un atklātu aizdomīgus darījumus, kuru mērķis ir izgatavot improvizētas sprāgstierīces. Tomēr apdraudējums, ko rada paštaisītas sprāgstvielas, joprojām ir liels, un tās izmanto daudzos uzbrukumos visā ES[88]. Pirmkārt, ir jāīsteno noteikumi, kā arī jānodrošina, ka tiešsaistes vide nedod iespēju apiet kontroli.

Terorisma apkarošanas politikas svarīgs elements ir arī efektīva kriminālvajāšana pret tiem, kas ir izdarījuši teroristu noziegumus, tostarp pret **ārvalstu kaujiniekiem teroristiem**, kas pašlaik atrodas Sīrijā un Irākā. Lai gan šos jautājumus galvenokārt risina dalībvalstis, ES koordinācija un atbalsts var palīdzēt dalībvalstīm risināt kopīgas problēmas. Svarīgs solis būs pasākumi, kas tiek veikti, lai pilnībā īstenotu robežu drošības tiesību aktus[89] un pilnībā izmantotu visas attiecīgās ES datubāzes nolūkā apmainīties ar informāciju par zināmajiem aizdomās turētajiem. Ir vajadzīga ne tikai augsta riska personu identificēšana, bet arī reintegrācijas un rehabilitācijas politika. Starpnozaru sadarbība, tostarp ar cietumu un probācijas darbiniekiem, stiprinās tiesu iestāžu izpratni par radikalizācijas un vardarbīga ekstrēmisma procesiem un tiesu sektora pieeju soda piespriešanai un aizturēšanas alternatīvām.

Ārvalstu kaujinieku teroristu problēma skaidri parāda saikni starp iekšējo un **ārējo drošību**. Sadarbība terorisma apkarošanā un radikalizācijas un vardarbīga ekstrēmisma novēršanā un

---

[83] Piemēram, finansējums no Eiropas Drošības fonda un Pilsonības programmas.

[84] ES pasākumi, piemēram, "*Erasmus*+ virtuālā apmaiņa", e-mērķsadarbība.

[85] Pēdējo divu gadu laikā gan Eiropā (Francijā, Vācijā, Itālijā), gan ārpus tās (Tunisijā, Indonēzijā) ir bijuši vairāki incidenti, kas saistīti ar bioloģiskajiem aģentiem (parasti augu izcelsmes toksīniem).

[86] Padome pieņēma ierobežojošus pasākumus pret ķīmisko ieroču izplatīšanu un izmantošanu.

[87] Ķīmiskas vielas, ko varētu ļaunprātīgi izmantot pašdarinātu sprāgstvielu izgatavošanai. Tās ir reglamentētas Regulā (ES) 2019/1148 par sprāgstvielu prekursoru tirdzniecību un lietošanu.

[88] Daži šādu postošu uzbrukumu piemēri ir uzbrukumi Oslo (2011. gadā), Parīzē (2015. gadā), Briselē (2016. gadā) un Mančestrā (2017. gadā). Uzbrukumā ar pašdarinātu sprāgstvielu Lionā (2019. gadā) tika ievainoti 13 cilvēki.

[89] Tostarp Eiropas Robežu un krasta apsardzes aģentūras (*Frontex*) jaunās pilnvaras.

apkarošanā ir būtiska drošībai Eiropas Savienībā[90]. Ir vajadzīgi turpmāki pasākumi, lai attīstītu terorisma apkarošanas partnerības un sadarbību ar kaimiņvalstīm un citām valstīm, izmantojot ES terorisma apkarošanas/drošības ekspertu tīkla pieredzi. Kopīgais terorisma apkarošanas rīcības plāns Rietumbalkāniem ir labs atskaites punkts šādai mērķtiecīgai sadarbībai. Jo īpaši būtu jāpieliek pūles, lai atbalstītu partnervalstu spējas identificēt un atrast ārvalstu kaujiniekus teroristus. ES arī turpinās veicināt daudzpusēju sadarbību, sadarbojoties ar vadošajiem globālajiem dalībniekiem šajā jomā, piemēram, Apvienoto Nāciju Organizāciju, NATO, Eiropas Padomi, Interpolu un EDSO. Tā arī sadarbosies ar Globālo terorisma apkarošanas forumu un Globālo koalīciju pret *Da'esh*, kā arī ar attiecīgajiem pilsoniskās sabiedrības dalībniekiem. Savienības ārpolitikas instrumentiem, tostarp attīstībai un sadarbībai, ir svarīga nozīme arī sadarbībā ar trešām valstīm, lai novērstu terorismu un pirātismu. Starptautiskā sadarbība ir būtiska arī, lai likvidētu visus **terorisma finansēšanas** avotus, piemēram, ar Finanšu darījumu darba grupas starpniecību.

Organizētā noziedzība

Organizētā noziedzība rada milzīgas ekonomiskas un personiskas izmaksas. Tiek lēsts, ka organizētās noziedzības un korupcijas radītie ekonomiskie zaudējumi sasniedz no 218 līdz 282 miljardiem EUR gadā[91]. Eiropā 2017. gadā tika izmeklēta vairāk nekā 5000 organizētās noziedzības grupējumu darbība, kas ir par 50 % vairāk nekā 2013. gadā[92]. Organizētā noziedzība arvien vairāk darbojas pāri robežām, tai skaitā no ES tuvākajām kaimiņvalstīm, un tādēļ ir nepieciešama pastiprināta operatīvā sadarbība un informācijas apmaiņa ar partneriem kaimiņvalstīs.

Rodas jaunas problēmas, kas padara noziedzību klātesošu arī tiešsaistē: līdz ar Covid-19 pandēmiju bija vērojams milzīgs tiešsaistes krāpniecības gadījumu skaita pieaugums attiecībā uz neaizsargātām grupām, kā arī attiecībā uz veselības un higiēnas precēm, kuras bija zādzību un ielaušanās gadījumu mērķis[93]. ES ir jāpastiprina darbs cīņā pret organizēto noziedzību, tai skaitā starptautiskā līmenī, izmantojot vairāk instrumentu, lai izjauktu organizētās noziedzības uzņēmējdarbības modeli. Organizētās noziedzības apkarošanai ir vajadzīga arī cieša sadarbība ar vietējām un reģionālajām pārvaldes iestādēm, kā arī ar pilsonisko sabiedrību, kas ir galvenie partneri noziedzības novēršanā, kā arī palīdzības un atbalsta sniegšanā cietušajiem, un īpaša uzmanība jāvelta pārvaldes iestādēm pierobežas reģionos. Šis darbs tiks apkopots **programmā organizētās noziedzības apkarošanai**.

Vairāk nekā trešdaļa organizētās noziedzības grupējumu, kas darbojas ES, ir iesaistītas narkotiku ražošanā, tirdzniecībā vai izplatīšanā. 2019. gadā Eiropas Savienībā narkotiku atkarība bija iemesls vairāk nekā astoņiem tūkstošiem nāves gadījumu, kurus izraisīja narkotiku pārdozēšana. Lielākā daļa **narkotiku tirdzniecības** notiek pāri robežām, un daudzi ienākumi tiek iefiltrēti likumīgajā ekonomikā[94]. Jauna ES Narkomānijas apkarošanas programma[95] stiprinās ES un dalībvalstu centienus narkotiku pieprasījuma un piedāvājuma

[90] Padomes 2020. gada 16. jūnija secinājumos ir uzsvērta vajadzība aizsargāt ES iedzīvotājus pret terorismu un vardarbīgu ekstrēmismu visās to formās un neatkarīgi no to izcelsmes un turpināt stiprināt ES ārējo iesaisti un rīcību terorisma apkarošanas jomā noteiktās prioritārās ģeogrāfiskās un tematiskās jomās.

[91] Iekšzemes kopprodukta (IKP) izteiksmē; Eiropola ziņojums: "Does crime still pay?" – *Criminal asset recovery in the EU*, 2016. gads.

[92] Eiropols, *Serious and Organised Crime Threat Assessments* (Smagās un organizētās noziedzības draudu novērtējumi) (*SOCTA*), 2013. un 2017. gads.

[93] Eiropols, 2020. gads.

[94] *EMCDDA* un Eiropols, *EU Drug Markets Report 2019* (2019. gada ziņojums par ES narkotiku tirgiem), (2019. gada novembris).

[95] ES programma narkomānijas apkarošanai un narkomānijas apkarošanas rīcības plāns 2021.–2025. gadam, COM(2020) 606.

samazināšanas jomā, nosakot kopīgas darbības kopīgās problēmas risināšanai un stiprinot dialogu un sadarbību starp ES un ārējiem partneriem narkotiku apkarošanas jautājumos. Pēc tam, kad būs veikts Eiropas Narkotiku un narkomānijas uzraudzības centra izvērtējums, Komisija lems, vai centra pilnvaras ir jāatjaunina, lai tas varētu risināt jaunus uzdevumus.

Organizētās noziedzības grupējumi un teroristi ir arī galvenie **nelikumīgo šaujamieroču** tirdzniecības dalībnieki. Laikposmā no 2009. līdz 2018. gadam Eiropā notika 23 masu apšaudes incidenti, kuros gāja bojā vairāk nekā 340 cilvēki[96]. Šaujamieročus bieži nelikumīgi ieved Eiropas Savienībā caur tās tuvākajām kaimiņvalstīm[97]. Tas norāda uz nepieciešamību pastiprināt koordināciju un sadarbību gan ES iekšienē, gan ar starptautiskajiem partneriem, jo īpaši ar Interpolu, lai saskaņotu informācijas vākšanu un ziņošanu par šaujamieroču konfiskācijas gadījumiem. Ir arī būtiski uzlabot ieroču izsekojamību, tai skaitā internetā, un nodrošināt informācijas apmaiņu starp licencēšanas un tiesībaizsardzības iestādēm. Komisija nāk klajā ar jaunu **ES rīcības plānu cīņai pret šaujamieroču nelikumīgu tirdzniecību**[98] un izvērtēs arī, vai noteikumi par šaujamieroču eksporta atļaujām un importa un tranzīta pasākumiem joprojām atbilst paredzētajam mērķim[99].

Noziedzīgās organizācijas migrantus un cilvēkus, kam nepieciešama starptautiskā aizsardzība, uzskata par preci. 90 % no neatbilstīgiem migrantiem, kuri ierodas ES, šeit ierodas ar noziedzīgu tīklu starpniecību[100]. Migrantu kontrabanda bieži ir saistīta arī ar citiem organizētās noziedzības veidiem, jo īpaši cilvēku tirdzniecību[101]. Eiropols lēš, ka, neraugoties uz cilvēku tirdzniecības milzīgajām cilvēciskajām izmaksām, gada peļņa par visu veidu ekspluatāciju no cilvēku tirdzniecības ir 29,4 miljardi EUR. Tas ir noziegums, kurš pārsniedz valstu robežas un kura pamatā ir nelikumīgs pieprasījums gan ES, gan ārpus tās, un kurš ietekmē visas ES dalībvalstis. Nepietiekamie panākumi šo noziegumu identificēšanā, kriminālvajāšanā un notiesāšanā par tiem prasa jaunu pieeju rīcības pastiprināšanai. Jauna **visaptveroša pieeja cilvēku tirdzniecības apkarošanai** apkopos dažādos darbības virzienus. Turklāt Komisija nāks klajā ar **jaunu ES Rīcības plānu cīņai pret migrantu kontrabandu** 2021.–2025. gadam. Abos pasākumos galvenā uzmanība tiks pievērsta noziedzīgo tīklu apkarošanai, sadarbības veicināšanai un tiesībaizsardzības darba atbalstam.

Organizētās noziedzības grupējumi, kā arī teroristi, arī meklē iespējas citās jomās, jo īpaši tajās, kuras rada lielu peļņu un kurās ir zems atklāšanas risks, piemēram, **noziegumi pret vidi**. Savvaļas dzīvnieku un augu nelikumīgas medības un tirdzniecība, nelikumīga kalnrūpniecība, mežizstrāde un nelikumīga atkritumu apglabāšana un sūtījumi ir kļuvuši par ceturto lielāko noziedzīgo darbību pasaulē[102]. Ir notikusi arī emisijas kvotu tirdzniecības shēmu un energosertifikātu sistēmu noziedzīga izmantošana, kā arī vides izturētspējai un

[96] Flandrijas Miera institūts, *Armed to kill* (“Bruņojies, lai nogalinātu”), (2019. gada oktobris).

[97] Kopš 2002. gada ES ir finansējusi cīņu pret kājnieku ieroču un vieglo ieroču izplatīšanu un tirdzniecību reģionā; to galvenokārt finansē Dienvidaustrumeiropas šaujamieroču ekspertu tīkls (*SEEFEN*). Kopš 2019. gada Rietumbalkānu partneri ir pilnībā iesaistīti Eiropas daudznozaru platformas pret noziedzības draudiem (*EMPACT*) prioritātē “Šaujamieroči”.

[98] COM(2020) 608.

[99] Regula (ES) Nr. 258/2012, ar kuru īsteno 10. pantu Apvienoto Nāciju Organizācijas Protokolā par šaujamieroču nelikumīgu ražošanu un tirdzniecību.

[100] Avots: Eiropols.

[101] Eiropols, *EMSC*, 4. gada pārskats.

[102] ANO Vides programmas un Interpola ātrās reaģēšanas novērtējums: *The Rise of Environmental Crime* (“Noziegumi pret vidi pieņemas spēkā”), 2016. gada jūnijs.

ilgtspējīgai attīstībai piešķirtā finansējuma ļaunprātīga izmantošana. Komisija ne tikai veicina ES, dalībvalstu un starptautiskās sabiedrības rīcību, lai pastiprinātu centienus apkarot noziegumus pret vidi[103], bet arī izvērtē, vai Direktīva par noziegumiem pret vidi[104] joprojām atbilst paredzētajam mērķim. **Arī kultūras priekšmetu tirdzniecība** ir kļuvusi par vienu no ienesīgākajām noziedzīgajām darbībām, par finansējuma avotu teroristiem, kā arī organizētajai noziedzībai, un tā kļūst arvien izplatītāka. Būtu jāapzina pasākumi, kā uzlabot kultūras priekšmetu izsekojamību tiešsaistē un bezsaistē iekšējā tirgū un sadarbību ar trešām valstīm, kurās tiek izlaupīti kultūras priekšmeti, kā arī jāsniedz aktīvs atbalsts tiesībaizsardzības un akadēmiskajām kopienām.

Ekonomiskie un finanšu noziegumi ir ļoti sarežģīti, taču ik gadu tie skar miljoniem ES iedzīvotāju un tūkstošiem uzņēmumu. Krāpšanas apkarošanai ir izšķiroša nozīme, un ir nepieciešama ES līmeņa rīcība. Eiropols kopā ar *Eurojust*, Eiropas Prokuratūru un Eiropas Biroju krāpšanas apkarošanai atbalsta dalībvalstis un ES ekonomikas un finanšu tirgu un ES nodokļu maksātāju naudas aizsardzībā. Eiropas Prokuratūra pilnībā sāks darboties 2020. gada beigās un izmeklēs noziegumus, kas vērsti pret ES budžetu, piemēram, krāpšanu, korupciju un nelikumīgi iegūtu līdzekļu legalizāciju, veiks kriminālvajāšanu, kā arī sauks pie atbildības par tiem. Tā arī novērsīs pārrobežu krāpšanu PVN jomā, kas nodokļu maksātājiem katru gadu izmaksā vismaz 50 miljardus EUR.

Komisija arī atbalstīs speciālo zināšanu un tiesiskā regulējuma attīstību attiecībā uz jauniem riskiem, piemēram, kriptoaktīviem un jaunām maksājumu sistēmām. Jo īpaši Komisija izskatīs reakciju uz kriptovalūtas, piemēram, bitmonētas, parādīšanos un šo jauno tehnoloģiju ietekmi uz to, kā tiek emitēti, mainīti, koplietoti finanšu aktīvi un kā tiem piekļūst.

Eiropas Savienībā jāvalda absolūtai neiecietībai pret nelikumīgi iegūtu naudu. Trīsdesmit gadu laikā ES ir izstrādājusi stabilu tiesisko regulējumu **nelikumīgi iegūtu līdzekļu legalizēšanas** un teroristu finansēšanas novēršanai un apkarošanai, pilnībā ievērojot vajadzību aizsargāt personas datus. Tomēr arvien pieaug vienprātība par to, ka ir būtiski jāuzlabo pašreizējā regulējuma īstenošana. Ir jānovērš būtiskas atšķirības tā piemērošanā un nopietnas nepilnības noteikumu izpildē. Kā sīki izklāstīts 2020. gada maija rīcības plānā[105], pašlaik tiek izvērtētas iespējas uzlabot ES regulējumu nelikumīgi iegūtu līdzekļu legalizācijas un teroristu finansēšanas apkarošanai. Pētāmās jomas ietver valstu centralizēto bankas kontu reģistru savstarpēju savienošanu, kas varētu ievērojami paātrināt finanšu izlūkošanas vienību un kompetento iestāžu piekļuvi finanšu informācijai.

Tiek lēsts, ka **organizētās noziedzības grupējumu peļņa** ES ir 110 miljardi EUR gadā. Pašreizējā reakcija ietver saskaņotus tiesību aktus par konfiskāciju un līdzekļu atgūšanu[106] ar mērķi uzlabot noziedzīgi iegūtu līdzekļu iesaldēšanu un konfiskāciju ES un veicināt savstarpēju uzticēšanos un efektīvu pārrobežu sadarbību starp dalībvalstīm. Tomēr tikai aptuveni 1 % no šīs peļņas tiek konfiscēts[107], kas ļauj organizētās noziedzības grupējumiem ieguldīt savu noziedzīgo darbību paplašināšanā un iefiltrēties likumīgajā ekonomikā, un galvenais mērķis nelikumīgi iegūtu līdzekļu legalizēšanai ir jo īpaši mazie un vidējie

[103] Sk. "Eiropas zaļais kurss", COM(2019)640 final.
[104] Direktīva 2008/99/EK par vides krimināltiesisko aizsardzību.
[105] Rīcības plāns nelikumīgi iegūtu līdzekļu legalizācijas un teroristu finansēšanas novēršanai, COM(2020) 2800.
[106] ES tiesību akti paredz, ka līdzekļu atguves dienestiem jābūt izveidotiem visās dalībvalstīs.
[107] Ziņojums par līdzekļu atgūšanu un konfiskāciju: "Noziedzības nedrīkst "atmaksāties"", COM(2020) 217 final.

uzņēmumi, kuriem ir grūtības saņemt kredītu. Komisija analizēs tiesību aktu īstenošanu[108] un iespējamo vajadzību pēc turpmākiem kopīgiem noteikumiem, tostarp attiecībā uz konfiskāciju bez notiesājoša sprieduma. Lai uzlabotu konfiskācijas rādītājus, līdzekļu atguves dienestus[109], kas ir galvenie līdzekļu atguves procesa dalībnieki, varētu aprīkot arī ar labākiem instrumentiem līdzekļu ātrākai identificēšanai un izsekošanai visā ES.

Pastāv cieša saikne starp organizēto noziedzību un **korupciju.** Ir aplēsts, ka korupcija vien ES ekonomikai izmaksā 120 miljardus EUR gadā[110]. Korupcijas novēršana un apkarošana arī turpmāk tiks regulāri uzraudzīta saskaņā ar tiesiskuma mehānismu, kā arī Eiropas pusgadu. Eiropas pusgadā ir novērtē, kādas problēmas cīņā pret korupciju ir vērojamas, piemēram, publiskā iepirkuma jomā, valsts pārvaldē, uzņēmējdarbības vidē vai veselības aprūpē. Komisijas jaunais ikgadējais ziņojums par tiesiskumu būs veltīts cīņai pret korupciju un ļaus veidot preventīvu dialogu ar valstu iestādēm un ieinteresētajām personām ES un valstu līmenī. Pilsoniskās sabiedrības organizācijām var būt svarīga loma arī valsts iestāžu darbības stimulēšanā organizētās noziedzības un korupcijas novēršanā un apkarošanā, un būtu lietderīgi šīs grupas apvienot kopīgā forumā. Ņemot vērā organizētās noziedzības un korupcijas pārrobežu raksturu, vēl viena svarīga dimensija to apkarošanas jomā ir sadarbība ar ES kaimiņreģioniem un palīdzība tiem.

Galvenie pasākumi
• ES terorisma apkarošanas programma, tai skaitā atjauninātas radikalizācijas apkarošanas darbības ES • Jauna sadarbība ar svarīgām trešām valstīm un starptautiskām organizācijām cīņā pret terorismu • Organizētās noziedzības, tai skaitā cilvēku tirdzniecības, apkarošanas programma • ES programma un rīcības plāns narkomānijas apkarošanai 2021.–2025. gadam • Eiropas Narkotiku un narkomānijas uzraudzības centra novērtējums • ES rīcības plāns attiecībā uz šaujamieroču nelikumīgu tirdzniecību 2020.–2025. gadam • Tiesību aktu par iesaldēšanu un konfiskāciju un par līdzekļu atguves dienestiem pārskatīšana • Direktīvas par noziegumiem pret vidi novērtējums • ES rīcības plāns cīņai pret migrantu kontrabandu (2021.–2025. gadam)

4. Spēcīga Eiropas drošības ekosistēma

Lai panāktu patiesu un efektīvu drošības savienību, vajadzīgi visu sabiedrības daļu kopīgi centieni. Lai uzlabotu sagatavotību un izturētspēju visiem, jo īpaši visneaizsargātākajiem, cietušajiem un lieciniekiem, jāiesaistās gan valdībām, tiesībaizsardzības iestādēm, privātajam sektoram, izglītības nozarei, gan pašiem iedzīvotājiem, tiem jābūt aprīkotiem un pienācīgi saistītiem.

Visās rīcībpolitikās ir jāiekļauj drošības dimensija, un ES var sniegt ieguldījumu visos līmeņos. Mājās vardarbība ģimenē ir viens no nopietnākajiem drošības riskiem. ES 22 %

[108] Direktīva 2014/42/ES par nozieguma rīku un noziedzīgi iegūtu līdzekļu iesaldēšanu un konfiskāciju.

[109] Padomes Lēmums 2007/845/TI attiecībā uz sadarbību starp dalībvalstu līdzekļu atguves dienestiem noziedzīgi iegūtu līdzekļu vai citu īpašumu meklēšanas un identificēšanas jomā.

[110] Ir grūti aplēst korupcijas kopējās ekonomiskās izmaksas, lai gan to ir mēģinājušas darīt tādas struktūras kā, piemēram, Starptautiskā Tirdzniecības palāta, *Transparency International*, ANO Globālais līgums un Pasaules Ekonomikas forums, un saskaņā ar šīm aplēsēm korupcija veido 5 % no pasaules IKP.

sieviešu ir saskārušās ar vardarbību ģimenē[111]. Viena no galvenajām prioritātēm joprojām ir ES pievienošanās Stambulas konvencijai par vardarbības pret sievietēm un vardarbības ģimenē novēršanu un apkarošanu. Ja sarunas joprojām nevirzīsies uz priekšu, Komisija veiks citus pasākumus, lai sasniegtu tos pašus mērķus, kādi paredzēti Konvencijā, tostarp ierosinās iekļaut vardarbību pret sievietēm Līgumā noteikto ES noziegumu sarakstā.

Sadarbība un informācijas apmaiņa

Viens no būtiskākajiem ieguldījumiem, ko ES var sniegt iedzīvotāju aizsardzībā, ir palīdzēt efektīvi sadarboties tiem, kas atbildīgi par drošību. Sadarbība un informācijas apmaiņa ir visspēcīgākie instrumenti noziedzības un terorisma apkarošanai un tiesiskuma panākšanai. Lai tā būtu efektīva, tai jābūt mērķtiecīgai un savlaicīgai. Lai tā būtu uzticama, tajā jāizmanto kopīgi aizsardzības pasākumi un kontrole.

Lai turpinātu pilnveidot **operatīvo sadarbību tiesībaizsardzības jomā** starp dalībvalstīm, ir izveidoti vairāki ES instrumenti un konkrētām nozarēm paredzētas stratēģijas[112]. Viens no galvenajiem ES instrumentiem, kas atbalsta tiesībaizsardzības iestāžu sadarbību starp dalībvalstīm, ir Šengenas Informācijas sistēma, ko izmanto, lai reāllaikā apmainītos ar datiem par meklētām un pazudušām personām un priekšmetiem. Rezultāti ir acīmredzami: tiek apcietināti noziedznieki, konfiscētas narkotikas un glābti potenciālie upuri[113]. Tomēr sadarbības līmeni joprojām varētu uzlabot, racionalizējot un modernizējot pieejamos instrumentus. Lielākā daļa ES tiesiskā regulējuma, kas ir pamatā operatīvajai sadarbībai tiesībaizsardzības jomā, tika izstrādāta pirms 30 gadiem. Sadrumstalotības risku rada arī sarežģīts dalībvalstu divpusējo nolīgumu tīkls, no kuriem daudzi ir novecojuši vai nepietiekami izmantoti. Mazākās valstīs vai valstīs, kurām ir tikai sauszemes robežas, tiesībaizsardzības amatpersonām, kas strādā pāri robežām, ir jāveic operatīvas darbības, dažos gadījumos ievērojot līdz pat septiņus dažādus noteikumu kopumus: rezultātā dažas operācijas, piemēram, aizdomās turēto tūlītēja vajāšana pāri iekšējām robežām, vienkārši netiek veikta. Pašreizējā ES regulējumā nav ietverta arī operatīvā sadarbība jaunu tehnoloģiju, piemēram, dronu, jomā.

Operatīvo efektivitāti var atbalstīt, nodrošinot īpašu tiesībaizsardzības iestāžu sadarbību, kas var arī palīdzēt sniegt būtisku atbalstu citiem politikas mērķiem, piemēram, sniegt drošības ieguldījumu ārvalstu tiešo investīciju jaunā novērtējumā. Komisija izskatīs, kā Policijas sadarbības kodekss varētu atbalstīt šos mērķus. Dalībvalstu tiesībaizsardzības iestādes arvien vairāk ir izmantojušas atbalstu un speciālās zināšanas ES līmenī, savukārt ES *INTCEN* ir bijusi nozīmīga loma stratēģisko izlūkdatu apmaiņas veicināšanā starp dalībvalstu izlūkdienestiem un drošības dienestiem, nodrošinot izlūkošanas situācijas apzināšanos ES iestādēm[114]. **Eiropolam** var būt būtiska nozīme, arī paplašinot sadarbību ar trešām valstīm, lai apkarotu noziedzību un terorismu saskaņā ar citām ES ārējām rīcībpolitikām un instrumentiem. Tomēr Eiropols pašlaik saskaras ar vairākiem nopietniem ierobežojumiem, jo īpaši attiecībā uz tiešu personas datu apmaiņu ar privātām struktūrām, kas tam traucē efektīvi atbalstīt dalībvalstis cīņā pret terorismu un noziedzību. Pašlaik tiek novērtētas Eiropola pilnvaras nolūkā noteikt, kā tās būtu jāuzlabo, lai nodrošinātu, ka aģentūra var pilnībā pildīt savus uzdevumus. Šajā saistībā arī attiecīgajām ES līmeņa iestādēm

[111] Savienība, kurā valda līdztiesība: dzimumu līdztiesības stratēģija 2020.–2025. gadam, COM(2020) 152.

[112] Piemēram, ES Jūras drošības stratēģijas rīcības plāns, kas ļāva gūt nozīmīgus panākumus, attiecīgajām ES aģentūrām sadarbojoties krasta apsardzes funkciju jomā.

[113] ES cīņa pret organizēto noziedzību 2019. gadā (Padome, 2020. gads).

[114] ES *INTCEN* ir vienīgā iespēja dalībvalstu izlūkdienestiem un drošības dienestiem nodrošināt uz izlūkdatiem balstītu situācijas apzināšanos ES.

(piemēram, *OLAF*, Eiropolam, *Eurojust* un Eiropas Prokuratūrai) būtu ciešāk jāsadarbojas un jāuzlabo informācijas apmaiņa.

Vēl viena svarīga saikne ir ***Eurojust*** turpmākā attīstība, lai maksimāli palielinātu sinerģiju starp tiesībaizsardzības iestāžu sadarbību un tiesu iestāžu sadarbību. ES gūtu labumu arī no labākas stratēģiskās saskaņotības: ***EMPACT***[115] – ES politikas cikls organizētas un smagas starptautiskas noziedzības jomā – sniedz iestādēm uz kriminālizlūkošanu balstītu metodoloģiju, lai kopīgi novērstu svarīgākos noziedzības draudus, kas skar ES. Pēdējo desmit gadu laikā tas ir devis nozīmīgus darbības rezultātus[116]. Pamatojoties uz praktiķu pieredzi, esošais mehānisms būtu jāracionalizē un jāvienkāršo, lai jaunajā politikas ciklā 2022.–2025. gadam efektīvāk risinātu vissteidzamākos un mainīgos noziedzības draudus.

Ikdienas darbā, kas saistīts ar noziedzības apkarošanu, būtiski ir iegūt savlaicīgu un atbilstošu **informāciju**. Neraugoties uz to, ka ir izstrādātas jaunas ES līmeņa datubāzes drošības un robežu pārvaldības jomā, liela daļa informācijas joprojām atrodas valstu datubāzēs vai ar to apmaiņās, neizmantojot šos rīkus. Rezultātā rodas ievērojama papildu darba slodze, kavējumi un lielāks risks, ka būtiska informācija netiks sniegta. Labāki, ātrāki un vienkāršāki procesi, iesaistot visu drošības kopienu, palīdzētu gūt labākus rezultātus. Pareizie instrumenti ir būtiski, lai informācijas apmaiņa varētu sasniegt savu potenciālu efektīvā cīņā pret noziedzību; ir jāizmanto nepieciešamie aizsardzības pasākumi, lai datu apmaiņā tiktu ievēroti datu aizsardzības tiesību akti un pamattiesības. Ņemot vērā tehnoloģiju, tiesu ekspertīzes un datu aizsardzības attīstību un izmaiņas operatīvajās vajadzībās, ES varētu apsvērt, vai ir jāmodernizē tādi instrumenti kā **2008. gada Prīmes lēmumi**, ar ko izveido automatizētu apmaiņu ar DNS, pirkstu nospiedumu un transportlīdzekļu reģistrācijas datiem, lai nodrošinātu automatizētu apmaiņu ar papildu datu kategorijām, kas kriminālizmeklēšanas nolūkos jau ir pieejamas dalībvalstu krimināltiesību vai citās datubāzēs. Turklāt Komisija izskatīs iespēju apmainīties ar policijas datiem, lai palīdzētu noteikt, vai citā dalībvalstī ir ziņas par personas sodāmību, un, ievērojot visus vajadzīgos aizsardzības pasākumus, atvieglos piekļuvi šīm ziņām, tiklīdz tās būs identificētas.

Informācija par ceļotājiem ir palīdzējusi uzlabot robežkontroli, samazināt neatbilstīgo migrāciju un identificēt personas, kas rada drošības riskus. Iepriekšējas pasažieru informācijas dati ir biogrāfiskie dati par katru pasažieri, kurus gaisa pārvadātāji vāc reģistrācijas laikā un iepriekš nosūta robežkontroles iestādēm galamērķī. Tiesiskā regulējuma[117] pārskatīšana varētu ļaut efektīvāk izmantot šo informāciju, vienlaikus nodrošinot atbilstību datu aizsardzības tiesību aktiem un atvieglojot pasažieru plūsmu. Pasažieru datu reģistrs (PDR) ir dati, ko pasažieri sniedz, rezervējot lidojumus. PDR direktīvas[118] īstenošana ir ļoti svarīga, un Komisija turpinās to atbalstīt un īstenot. Turklāt kā vidēja termiņa darbību Komisija sāks pārskatīt pašreizējo pieeju **PDR datu nosūtīšanai uz trešām valstīm.**

Tiesu iestāžu sadarbība ir nepieciešams papildinājums policijas centieniem apkarot pārrobežu noziedzību. Pēdējo 20 gadu laikā tiesu iestāžu sadarbībā ir notikušas būtiskākas pārmaiņas. Tādām struktūrām kā **Eiropas Prokuratūra** un ***Eurojust*** ir jābūt pieejamiem līdzekļiem, lai nodrošinātu to pilnīgu funkcionēšanu vai darbības stiprināšanu. Varētu

[115] *EMPACT* – Eiropas daudznozaru platforma pret noziedzības draudiem.
[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.
[117] Padomes Direktīva 2004/82/EK par pārvadātāju pienākumu darīt zināmus datus par pasažieriem.
[118] Direktīva 2016/681 par pasažieru datu reģistra (PDR) datu izmantošanu teroristu nodarījumu un smagu noziegumu novēršanai, atklāšanai, izmeklēšanai un saukšanai pie atbildības par tiem.

uzlabot arī sadarbību starp praktizējošiem juristiem, veicot turpmākus pasākumus attiecībā uz tiesu nolēmumu savstarpēju atzīšanu, tiesisko apmācību un informācijas apmaiņu. Mērķim vajadzētu būt lielākai savstarpējai uzticībai starp tiesnešiem un prokuroriem, kam ir galvenā nozīme pārrobežu procedūru atvieglošanā. Arī **digitālo tehnoloģiju** izmantošana var uzlabot mūsu tiesu sistēmu efektivitāti. Ar *Eurojust* atbalstu tiek izveidota jauna digitāla apmaiņas sistēma, kas paredzēta Eiropas izmeklēšanas rīkojumu, savstarpējas tiesiskās palīdzības lūgumu un ar tiem saistītas saziņas pārsūtīšanai starp dalībvalstīm. Komisija sadarbosies ar dalībvalstīm, lai paātrinātu vajadzīgo IT sistēmu ieviešanu valsts līmenī.

Starptautiskā sadarbība ir būtiska arī efektīvai tiesībaizsardzībai un tiesu iestāžu sadarbībai. Divpusējiem nolīgumiem ar galvenajiem partneriem ir būtiska nozīme, lai nodrošinātu informāciju un pierādījumus no valstīm ārpus ES. Svarīga loma ir **Interpolam,** kas ir viena no lielākajām starpvaldību kriminālpolicijas organizācijām. Komisija izskatīs iespējamos veidus, kā pastiprināt sadarbību ar Interpolu, tostarp iespējamu piekļuvi Interpola datubāzēm un operatīvās un stratēģiskās sadarbības stiprināšanu. Noziedznieku un teroristu atklāšanā un to nodarījumu izmeklēšanā ES tiesībaizsardzības iestādes paļaujas arī uz galvenajām partnervalstīm. Lai uzlabotu sadarbību cīņā pret tādiem kopīgiem apdraudējumiem kā terorisms, organizētā noziedzība, kibernoziedzība, seksuāla vardarbība pret bērniem un cilvēku tirdzniecība, varētu pastiprināt **drošības partnerības starp ES un trešām valstīm.** Šāda pieeja balstītos uz kopīgām drošības interesēm, kā arī uz iedibinātu sadarbību un drošības dialogiem.

Ne tikai informācijai, bet arī speciālo zināšanu apmaiņai var būt īpaša nozīme, lai palielinātu tiesībaizsardzības iestāžu sagatavotību **netradicionāliem apdraudējumiem.** Komisija ne tikai veicinās paraugprakses apmaiņu, bet arī pētīs iespējamu **ES līmeņa koordinācijas mehānismu policijas spēku sadarbībai** nepārvaramas varas, piemēram, pandēmiju, gadījumos. Šī pandēmija ir arī pierādījusi, ka Digitālās kopienas policijas darbībai, ko papildina tiesiskais regulējums, lai atvieglotu policijas darbu tiešsaistē, būs būtiska nozīme cīņā pret noziedzību un terorismu. Policijas un kopienu partnerības gan tiešsaistē, gan bezsaistē var novērst noziedzību un mazināt organizētās noziedzības, radikalizācijas un teroristu aktivitāšu ietekmi. Saikne starp vietējiem un reģionāliem risinājumiem, kā arī valstu un ES policijas risinājumiem ir galvenais panākumu faktors ES drošības savienībai kopumā.

Ieguldījums spēcīgu ārējo robežu saglabāšanā

Moderna un efektīva ārējo robežu pārvaldība sniedz divējādu ieguvumu – saglabā Šengenas integritāti un garantē mūsu iedzīvotāju drošību. Visu attiecīgo dalībnieku iesaistīšanai, lai panāktu maksimālu drošību uz robežas, var būt reāla ietekme uz pārrobežu noziedzības un terorisma novēršanu. Nesen nostiprinātās Eiropas Robežu un krasta apsardzes kopīgās operatīvās darbības[119] palīdz novērst un atklāt pārrobežu noziedzību pie **ārējām robežām** un ārpus ES. Pārrobežu noziedzības un terorisma apkarošanā izšķirīga nozīme ir muitas darbībām, kuru mērķis ir atklāt drošuma un drošības riskus visās precēs, pirms tās nonāk ES, un kontrolēt preces, kad tās tiek ievestas. Gaidāmajā Muitas savienības rīcības plānā tiks izziņotas darbības, lai stiprinātu arī riska pārvaldību un uzlabotu iekšējo drošību, tostarp jo īpaši izvērtējot iespēju izveidot saikni starp attiecīgām informācijas sistēmām drošības riska analīzei.

[119] To veido Eiropas Robežu un krasta apsardzes aģentūra (*Frontex*) un dalībvalstu robežsardzes iestādes un krasta apsardzes iestādes.

Satvars **ES informācijas sistēmu sadarbspējai** tieslietu un iekšlietu jomā tika pieņemts 2019. gada maijā. Šīs jaunās struktūras mērķis ir uzlabot jauno vai modernizēto informācijas sistēmu efektivitāti un lietderību[120]. Tādējādi tiesībaizsardzības iestāžu darbiniekiem, robežsargiem un migrācijas jomā nodarbinātajām amatpersonām tiks sniegta ātrāka un sistemātiskāka informācija. Tas palīdzēs veikt pareizu identifikāciju, kā arī apkarot identitātes viltošanu. Lai to īstenotu, sadarbspējas īstenošanai vajadzētu būt prioritātei gan politiskā, gan tehniskā līmenī. Cieša sadarbība starp ES aģentūrām un visām dalībvalstīm būs ārkārtīgi svarīga, lai līdz 2023. gadam sasniegtu pilnīgas sadarbspējas mērķi.

Ceļošanas dokumentu viltošana tiek uzskatīta par vienu no visbiežāk izdarītajiem noziegumiem. Tā veicina noziedznieku un teroristu nelikumīgu pārvietošanos, un tai ir būtiska nozīme cilvēku un narkotiku tirdzniecībā[121]. Komisija izpētīs, kā paplašināt pašreizējo darbu pie ES uzturēšanās un ceļošanas dokumentu drošības standartiem, tai skaitā ar digitalizācijas starpniecību. No 2021. gada augusta dalībvalstis sāks izdot personas apliecības un uzturēšanās dokumentus atbilstīgi saskaņotiem drošības standartiem, kas ietvers mikroshēmu ar biometriskiem identifikatoriem, ko var pārbaudīt visas ES robežkontroles iestādes. Komisija uzraudzīs šo jauno noteikumu īstenošanu, kā arī pašlaik apritē esošo dokumentu pakāpenisku aizstāšanu.

Drošības pētniecības un inovāciju stiprināšana

Darbs, kura mērķis ir nodrošināt kiberdrošību un apkarot organizēto noziedzību, kibernoziedzību un terorismu, lielā mērā ir atkarīgs no instrumentu izstrādes, kuri palīdzēs radīt drošākas un aizsargātākas jaunās tehnoloģijas, risinās problēmas, ko rada tehnoloģijas, un atbalstīs tiesībaizsardzības iestāžu darbu. Tas savukārt ir atkarīgs no privātajiem partneriem un nozarēm.

Inovācija būtu jāuzskata par stratēģisku instrumentu pašreizējo apdraudējumu novēršanai un nākotnes risku un iespēju paredzēšanai. Inovatīvas tehnoloģijas var radīt jaunus instrumentus, kas palīdzētu tiesībaizsardzības un citiem drošības jomas dalībniekiem. Mākslīgajā intelektā un lielo datu analīzē varētu izmantot augstas veiktspējas datošanu, lai nodrošinātu labāku atklāšanu un ātru un visaptverošu analīzi[122]. Svarīgs priekšnoteikums uzticamu tehnoloģiju izstrādei ir augstas kvalitātes datu kopas, kas pieejamas kompetentajām iestādēm, lai apmācītu, pārbaudītu un apstiprinātu algoritmus[123]. Kopumā mūsdienās tehnoloģiskās atkarības risks ir liels – ES ir, piemēram, kiberdrošības produktu un pakalpojumu neto importētāja ar visām sekām, ko tas atstāj uz ekonomiku un kritisko infrastruktūru. Lai apgūtu tehnoloģijas un garantētu piegādes nepārtrauktību arī nelabvēlīgu notikumu un krīžu gadījumā, ir vajadzīga Eiropas klātbūtne un kapacitāte attiecīgo vērtību ķēžu kritiskajās daļās.

ES **pētniecība, inovācija un tehnoloģiju attīstība** sniedz iespēju ņemt vērā drošības dimensiju, izstrādājot šīs tehnoloģijas un to pielietojumu. Nākamās paaudzes ES

[120] Ieceļošanas/izceļošanas sistēma (IIS), Eiropas ceļošanas informācijas un atļauju sistēma (*ETIAS*), paplašinātā Eiropas Sodāmības reģistru informācijas sistēma (*ECRIS-TCN*), Šengenas informācijas sistēma, Vīzu informācijas sistēma un nākamais atjauninātais *Eurodac*.

[121] Saikne starp dokumentu viltošanu un cilvēku tirdzniecību ir izklāstīta Otrajā ziņojumā par progresu, kas panākts cīņā pret cilvēku tirdzniecību, COM(2018) 777 un tam pievienotajā SWD(2018) 473, un Eiropola 2016. gada operatīvajā ziņojumā "Cilvēku tirdzniecība ES"(*Situation Report — Trafficking in human beings in the EU*).

[122] Tam būtu jābalstās uz Komisijas stratēģiju mākslīgā intelekta jomā.

[123] "Eiropas datu stratēģija", COM(2020) 66 final.

finansējuma priekšlikumi var būt nozīmīgs stimuls[124]. Iniciatīvās par Eiropas datu telpām un mākoņdatošanas infrastruktūru jau no paša sākuma ir paredzēts drošības aspekts. Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centra un Nacionālo koordinācijas centru tīkla[125] mērķis ir izveidot efektīvu un lietderīgu struktūru kiberdrošības pētniecības spēju un rezultātu apkopošanai un apmaiņai. ES Kosmosa programma sniedz pakalpojumus, kas atbalsta ES, tās dalībvalstu un privātpersonu drošību[126].

ES finansēta drošības pētniecība (kopš 2007. gada ir sākti vairāk nekā 600 projekti, kuru kopējā vērtība ir gandrīz 3 miljardi EUR) ir svarīgs instruments, lai veicinātu tehnoloģijas un zināšanas drošības risinājumu atbalstam. Pārskatot Eiropola pilnvaras, Komisija izskatīs iespēju izveidot **Eiropas Inovācijas centru iekšējai drošībai**[127], kura mērķis būtu mēģināt rast kopīgus risinājumus kopīgām drošības problēmām un iespējām, ko dalībvalstis vienas pašas nevarētu izmantot. Sadarbība ir būtiska, lai ieguldījumus koncentrētu pēc iespējas efektīvāk un lai izstrādātu inovatīvas tehnoloģijas, kas sniedz gan drošību, gan ekonomisku labumu.

Prasmju un informētības uzlabošana

Lai veidotu izturētspējīgāku sabiedrību, labāk sagatavotus uzņēmumus, pārvaldes iestādes un privātpersonas, būtiska nozīme ir informētībai par drošības jautājumiem un prasmju apgūšanai, kas palīdzētu novērst iespējamos apdraudējumus. Problēmas, kas saistītas ar IT infrastruktūru un e-sistēmām, liecina, ka ir jāuzlabo cilvēku sagatavotības un reaģēšanas spēja kiberdrošības jomā. Šī pandēmija ir arī uzsvērusi digitalizācijas nozīmi visās ES ekonomikas un sabiedrības jomās.

Sabiedrības izturētspēju var reāli ietekmēt pat **pamatzināšanas par drošības apdraudējumiem** un par to apkarošanu. Kiberuzbrukumu apkarošanā kibernoziedzības riska apzināšanos un vajadzību aizsargāt sevi no tā var apvienot ar pakalpojumu sniedzēju sniegto aizsardzību. Informācija par narkotiku tirdzniecības briesmām un riskiem var mazināt noziedznieku panākumus. ES var veicināt paraugprakses izplatīšanu, piemēram, izmantojot drošāka interneta centru tīklu[128], un nodrošināt, ka šādi mērķi tiek ņemti vērā tās programmās.

Nākamajā Digitālās izglītības rīcības plānā būtu jāiekļauj mērķtiecīgi pasākumi, kuru mērķis ir veidot drošības IT prasmes visiem iedzīvotājiem. Nesen pieņemtā Prasmju programma[129] atbalsta prasmju veidošanu visa mūža garumā. Tā ietver īpašas darbības, kuru mērķis ir vairot absolventu skaitu zinātnē, tehnoloģijās, inženierzinātnēs, mākslā un matemātikā, kas nepieciešami tādās progresīvās jomās kā kiberdrošība. Papildu darbības, ko finansē no programmas "Digitālā Eiropa", ļaus profesionāļiem iet kopsolī ar izmaiņām drošības

[124] Komisijas priekšlikumi par pamatprogrammu "Apvārsnis Eiropa", Iekšējās drošības fondu, Integrētas robežu pārvaldības fondu, programmu *InvestEU*, Eiropas Reģionālās attīstības fondu un programmu "Digitālā Eiropa" atbalstīs inovatīvu drošības tehnoloģiju un risinājumu izstrādi un ieviešanu visā drošības vērtību ķēdē.

[125] Komisijas priekšlikums regulai (2018. gada 12. septembris), ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu, COM(2018) 630.

[126] Piemēram, *Copernicus* sniedz pakalpojumus, kas ļauj uzraudzīt ES ārējās robežas un jūras uzraudzību un kas palīdz apkarot pirātismu un kontrabandu, kā arī atbalsta kritisko infrastruktūru. Kad tas pilnībā sāks darboties, tas būs galvenais faktors, kas sekmēs civilās un militārās misijas un operācijas.

[127] Tas sadarbotos arī ar *EBCGA/Frontex*, *CEPOL*, *eu-LISA* un Kopīgo pētniecības centru.

[128] Sk. www.betterinternetforkids.eu: centrālo portālu un valstu drošāka interneta centrus pašlaik finansē no EISI/telekomunikāciju programmas, nākotnē to ierosināts finansēt programmas "Digitālā Eiropa" ietvaros.

[129] Eiropas Prasmju programma ilgtspējīgai konkurētspējai, sociālajam taisnīgumam un izturētspējai, COM(2020) 274 final

apdraudējumu jomā un vienlaikus novērst darbinieku trūkumu šajā jomā ES darba tirgū. Vispārējā ietekme būs tāda, ka privātpersonas varēs apgūt prasmes, kas vajadzīgas, lai novērstu apdraudējumus drošībai, un uzņēmumi varēs atrast šajā jomā nepieciešamos speciālistus. Gaidāmā Eiropas pētniecības telpa un Eiropas izglītības telpa arī veicinās karjeru zinātnē, tehnoloģijās, inženierzinātnēs, mākslā un matemātikā.

Būtiski ir arī, lai **cietušajiem** būtu iespēja izmantot savas tiesības; viņiem ir jāsaņem nepieciešamā palīdzība un atbalsts, ņemot vērā viņu īpašos apstākļus. Īpaši centieni ir vajadzīgi attiecībā uz minoritātēm un visneaizsargātākajiem cietušajiem, piemēram, bērniem vai sievietēm, kas tiek pārdoti seksuālai izmantošanai vai pakļauti vardarbībai ģimenē[130].

Īpaša nozīme ir **prasmju uzlabošanai tiesībaizsardzības jomā**. Pašreizējie un jaunie tehnoloģiskie apdraudējumi liek ieguldīt vairāk līdzekļu tiesībaizsardzības iestāžu darbinieku prasmju uzlabošanā viņu karjeras sākumposmā un tās gaitā. *CEPOL* ir būtisks partneris, kas palīdz dalībvalstīm veikt šo uzdevumu. Tiesībaizsardzības apmācībai saistībā ar rasismu un ksenofobiju, kā arī pilsoņu tiesībām kopumā ir jābūt būtiskai ES drošības kultūras sastāvdaļai. Valstu tiesu sistēmām un tieslietu speciālistiem arī jābūt sagatavotiem, lai pielāgotos nepieredzētām problēmām un reaģētu uz tām. Apmācība ir svarīga, lai operatīvā situācijā iestādes uz vietas varētu izmantot minētos instrumentus. Turklāt būtu jādara viss iespējamais, lai pastiprinātu integrētu pieeju dzimumu līdztiesībai un stiprinātu sieviešu līdzdalību tiesībaizsardzībā.

Galvenās darbības
• Eiropola pilnvaru stiprināšana • ES "Policijas sadarbības kodeksa" un policijas koordinācijas krīzes laikā izpēte • *Eurojust* stiprināšana nolūkā veidot saikni starp tiesu un tiesībaizsardzības iestādēm • Iepriekšējas pasažieru informācijas direktīvas pārskatīšana • Paziņojums par pasažieru datu reģistra ārējo dimensiju • ES un Interpola sadarbības stiprināšana • Satvars sarunām ar galvenajām trešām valstīm par informācijas apmaiņu • Labāki ceļošanas dokumentu drošības standarti • Eiropas Inovācijas centra iekšējai drošībai izpēte

V. Secinājumi

Kamēr situācija pasaulē kļūst arvien nestabilāka, Eiropas Savienība joprojām tiek plaši uzskatīta par vienu no drošākajām un aizsargātākajām vietām. Tomēr to nevar uzskatīt par pašsaprotamu.

Jaunā Drošības savienības stratēģija veido pamatu drošības ekosistēmai, kas aptver visu Eiropas sabiedrību. Tās pamatā ir apziņa, ka drošība ir kopīga atbildība. Drošība ir jautājums, kas skar ikvienu. Visām valdības struktūrām, uzņēmumiem, sociālajām organizācijām, iestādēm un iedzīvotājiem ir jāpilda savi pienākumi, lai mūsu sabiedrību padarītu drošāku.

Drošības jautājumi tagad jāskata daudz plašākā perspektīvā nekā iepriekš. Ir jāpārvar mākslīgais dalījums starp fizisko un digitālo. ES Drošības savienības stratēģija ietver visas drošības vajadzības un koncentrējas uz jomām, kas tuvākajos gados būs visbūtiskākās ES

[130] Sk. Dzimumu līdztiesības stratēģiju, COM(2020) 152; Stratēģiju par cietušo tiesībām, COM(2020) 258; un Eiropas stratēģiju "Bērniem labāks internets", COM(2012) 196.

drošībai. Tajā arī atzīts, ka drošības apdraudējumos netiek ievērotas ģeogrāfiskās robežas, kā arī pieaug saikne starp iekšējo un ārējo drošību[131]. Šajā saistībā ES būs svarīgi sadarboties ar starptautiskajiem partneriem, lai aizsargātu visus ES iedzīvotājus, un šīs stratēģijas īstenošanā saglabāt ciešu koordināciju ar ES ārējo darbību.

Mūsu drošība ir saistīta ar mūsu pamatvērtībām. Visas šajā stratēģijā ierosinātās darbības un iniciatīvas pilnībā ievēros pamattiesības un mūsu Eiropas vērtības. Tās ir mūsu Eiropas dzīvesveida pamats, un tām jāpaliek visa mūsu darba pamatā.

Visbeidzot, Komisija pilnībā apzinās, ka jebkura rīcībpolitika vai darbība ir tikai tik efektīva, cik efektīva ir tās īstenošana. Tādēļ ir neatlaidīgi jāuzsver, cik svarīga ir spēkā esošo un turpmāko tiesību aktu pareiza īstenošana un izpilde. To uzraudzīs ar regulāriem drošības savienības ziņojumiem, un Komisija pilnībā informēs Eiropas Parlamentu, Padomi un ieinteresētās personas un iesaistīsies visās attiecīgajās darbībās. Turklāt Komisija ir gatava piedalīties un organizēt kopīgas debates ar iestādēm par Drošības savienības stratēģiju, lai kopā izvērtētu gūtos panākumus, vienlaikus kopīgi izskatot turpmākās problēmas.

Komisija aicina Eiropas Parlamentu un Padomi apstiprināt šo Drošības savienības stratēģiju kā pamatu sadarbībai un vienotai rīcībai drošības jomā nākamajiem pieciem gadiem.

[131] Sk. ES globālo stratēģiju