



Eiropas Savienības
Padome

Briselē, 2022. gada 27. maijā
(OR. en)

9563/22

JAI 761	DROIPEN 69
COSI 149	COPEN 210
ENFOPOL 298	FREMP 110
ENFOCUSTOM 89	JAIEX 61
IXIM 145	CFSP/PESC 705
CT 99	COPS 238
CRIMORG 81	HYBRID 49
FRONT 218	DISINFO 47
ASIM 47	TELECOM 248
VISA 87	DIGIT 108
CYBER 191	COMPET 408
DATAPROTECT 175	RECH 307
CATS 30	

PAVADVĒSTULE

Sūtītājs: Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*

Saņemšanas datums: 2022. gada 25. maijs

Saņēmējs: Padomes Ģenerālsekretariāts

K-jas dok. Nr.: COM(2022) 252 final

Temats: KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI par ceturto progresu ziņojumu par ES Drošības savienības stratēģijas īstenošanu

Pielikumā ir pievienots dokuments COM(2022) 252 *final*.

Pielikumā: COM(2022) 252 *final*



Briselē, 25.5.2022.
COM(2022) 252 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI
par ceturto progresu ziņojumu par ES Drošības savienības stratēģijas īstenošanu

I. IEVADS

Pašlaik ES drošības darba kārtībā lielākā uzmanība tiek pievērsta Krievijas agresīvajam karam pret Ukrainu. Šis karš ne tikai apdraud Ukrainu — tā mērķis ir arī iedragāt stabilitāti un drošību pasaulē. Eiropas Savienībā tas dažādos veidos apdraud iedzīvotāju drošību. Ir radušās jaunas neskaidrības par enerģijas un citu izejmateriālu piegādēm, un pret kritisko infrastruktūru var tikt vērsti kiberuzbrukumi. ES iekšējo drošību apdraud iespējami uzbrukumi vai negadījumi, ko var radīt kara zonā izmantotās ķīmiskās, bioloģiskās vai radioloģiskās vielas. Miljoniem cilvēku, kas ir aizbēguši no kara, atrodas neaizsargātā situācijā, un organizētie noziedznieki šo neaizsargātību var nevilcinoties izmantot, padarot sievietes un bērnus — riskam īpaši pakļautās grupas — par cilvēku tirdzniecības upuriem.

ES uz šiem jaunajiem un iespējamajiem draudiem ir reaģējusi stingri un vienoti. Lai gan kara ietekme līdz šim lielākoties ir skārusi tikai Ukrainas teritoriju, ES ir pastiprinājusi *modrību un koordinēšanu* un šo centienu ietvaros intensīvāk monitorē drošības apdraudējumu ainu, kā arī ir strādājusi ar mērķi uzlabot noturību, lai nodrošinātu *gatavību*.

Eiropas valstu un valdību vadītāji 2022. gada 10. un 11. martā pieņemtajā Versaļas deklarācijā¹ uzsvēra vajadzību sagatavoties izaicinājumiem, kas rodas strauji, un to panākt, cita starpā “aizsargājoties pret arvien plašāko hibrīdkaru, stiprinot mūsu kiberneturību, aizsargājot mūsu infrastruktūru, jo īpaši mūsu kritisko infrastruktūru, un apkarojot dezinformāciju”.

Drošības savienības sistēmai ir ļoti liela nozīme drošības nodrošināšanā visā ES. Drošības savienības stratēģijā² izklāstītās četras stratēģiskās prioritātes joprojām pilnīgi atbilst šim uzdevumam arī pašreizējā ģeopolitiskajā situācijā, un tās ir šādas: i) nākotnes prasībām atbilstoša drošības vide, ii) vēršanās pret jauniem apdraudējumiem, iii) Eiropas iedzīvotāju aizsardzība pret terorismu un organizēto noziedzību un iv) spēcīga Eiropas drošības ekosistēma. Karš ir apliecinājis, ka ES un tās dalībvalstīm ir pilnvērtīgi jāizmanto leģislatīvie un politiskie instrumenti, kas jau ir pieejami saskaņā ar Drošības savienības stratēģiju un kas ir pamatā koordinētajam atbalstam, kuru ES sniedz dalībvalstīm tādos jautājumos kā organizētā noziedzība un terorisms un kiberdrošība un hibrīddraudi.

Arī Eiropas aģentūras, kas darbojas tieslietu un iekšlietu jomā, ir pastiprinājušas savus centienus, reaģējot uz karu Ukrainā, un ir ļoti palīdzējušas novērtēt draudus un atbalstīt operatīvos reaģēšanas pasākumus³. Vēl viens svarīgs uzdevums ir pastāvīgi stiprināt Šengenas zonas darbības principus un pārvaldību.

Šajā ceturtajā progresa ziņojumā par drošības savienību lielākā uzmanība ir pievērsta notikumiem, kas norisinājušies dažos pēdējos mēnešos kopš Krievijas agresīvā kara pret Ukrainu sākuma. Tajā ir sniegts pārskats par darbībām, kas veiktas visos drošības savienības darbības virzienos, un ir aplūkota vajadzība būt gataviem, ko rada iespējamie, no Ukrainā notiekošā kara izrietošie drošības apdraudējumi. Informācija par progresu saistībā ar citiem drošības savienības dokumentiem ir sniegta pielikumā.

¹ <https://www.consilium.europa.eu/media/54790/20220311-versailles-declaration-lv.pdf>

² COM(2020) 605.

³ [Joint Statement from EU Justice and Home Affairs Agencies on Ukraine | Eiropas Savienības Patvēruma aģentūra \(europa.eu\)](#)

II. KIBERDROŠĪBA UN KRITISKĀ INFRASTRUKTŪRA

Kopš kara sākuma privāti rīcībspēki un kriminālās aprindas ir publiski pauduši, ka veic kiberpasākumus vienas vai otras puses atbalstam. Haktīvisms⁴ rada apdraudējumu, jo pastāv risks, ka tam būs negatīva blakusietekme uz kritiskajiem pakalpojumiem Eiropas Savienībā, risks, ka tiks veikti uzbrukumi no oficiālajiem tīkliem, un ir iespējamās citas neparedzamas papildu sekas. Lai gan līdz šim karā lielākoties ir izmantoti tradicionāli līdzekļi, kas ir radījuši tikai nelielas papildu sekas, pastāv reāls eskalācijas risks šajā jomā.

Tāpēc ES ir uzlabojusi koordināciju un gatavību. Kara radītie apdraudējumi ir izgaismojuši vajadzību veidot tādu sadarbības kultūru starp ES, dalībvalstīm un visā kiberdrošības kopienā, kurai raksturīga dalīšanās ar informāciju un speciālajām zināšanām. Tas nozīmē arī veidot integrētu priekšstatu par situāciju — tādu, kas ir kopīgs ES iestādēm, struktūrām un aģentūrām un dalībvalstīm, īpaši attiecībā uz kritisko infrastruktūru, kas ir vajadzīga, lai iekšējais tirgus darbotos bez sarežģījumiem.

Pret Ukrainu vērsto kiberuzbrukumu vaininieku noteikšana

Kiberuzbrukumi Ukrainai sākās pirms Krievijas agresijas, un pirmajās kara dienās⁵ to mērķis bija apdraudēt Ukrainas militārpersonu lietotāju kontus un traucēt pamatpakalpojumu sniegšanu, ieskaitot robežkontroli un telesakarus.

2022. gada 14. janvārī Augstais pārstāvis Eiropas Savienības vārdā sniedza deklarāciju⁶, ar ko nosodīja kiberuzbrukumus pret Ukrainu un atkārtoti apliecināja ES nepārprotamo atbalstu Ukrainai.

10. maijā Eiropas Savienība un tās dalībvalstis kopā ar starptautiskajiem partneriem stingri nosodīja⁷ ļaunprātīgās kiberdarbības pret Ukrainu, kuras 24. februārī tika vērstas pret uzņēmumam “Viasat” piederošo *KA-SAT* satelītītīklu, un noteica, ka par uzbrukumu ir atbildīga tieši Krievijas Federācija. Šim kiberuzbrukumam bija smagas sekas, jo tas nešķirojot radīja sakaru pārrāvumus un traucējumus vairākām publiskā sektora iestādēm, uzņēmumiem un lietotājiem Ukrainā un skāra arī vairākas ES dalībvalstis.

Modrība un koordinācija

⁴ Nesens haktīvisma piemērs ir “protestprogrammatūras” izmantošana ar mērķi izplatīt ļaunprogrammatūru Krievijas IP adresēs. Šim mērķim izmantoja populāru atklātā pirmkoda pakotni, un tas varētu radīt riskus piegādes ķēdēm un pamudināt vairs neuzticēties atvērtā pirmkoda kopienai. Komisija ir skaidri norādījusi, ka (pat labu nodomu vadīti) kiberuzbrukumi Krievijai nav likumīgi.

⁵ *Microsoft* īpašais ziņojums [An overview of Russia's cyberattack activity in Ukraine; The hybrid war in Ukraine - Microsoft On the Issues](#)

⁶ <https://www.consilium.europa.eu/iv/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/>

⁷ [“Krievijas kiberdarbības pret Ukrainu: Eiropas Savienības vārdā sniegta Augstā pārstāvja deklarācija”](#)

Kopš Krievijas agresīvā kara pret Ukrainu sākuma ir pastiprinājusies kibernetikas drošības situācijas uzraudzība dalībvalstīs un ES iestādēs. Gan ES Kibernetikas drošības aģentūra (*ENISA*) un Eiropas Eiropas Kibernetikas drošības apkarotājs centrs, gan arī ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienība (*CERT-EU*) un ES Izlūkošanas un situāciju centrs (*EU INTCEN*) ir sniedzis ieguldījumu ES kopējā priekšstata par kibernetikas drošības situāciju veidošanā, tostarp tie ir regulāri uzraudzījuši aizdomīgas kibernetikas darbības, citu starpā īpaši pievērsoties tādām nozarēm kā enerģētika, transports un aviācija, un ir snieguši novērtējumus, kas kalpo par orientieriem preventīvas rīcības īstenošanā.

Ir arī notikusi pastiprināta koordinācija un informācijas apmaiņa ar kibernetikas drošības tīkliem, piemēram, Kiberkrīžu sadarbības organizāciju tīklu (*CyCLONe*), kurā ir iesaistītas valstu kibernetikas drošības aģentūras, Komisija un *ENISA*. Šī pieeja ir pārņemta arī ES iestāžu iekšienē, kur tiek izmantots koordinēšanas mehānisms — Kiberkrīžu darba grupa —, lai dalītos ar informāciju starp visiem attiecīgajiem dienestiem, struktūrām un aģentūrām, ieskaitot *ENISA*, Eiropas Eiropas Kibernetikas drošības apkarotājs centru un *CERT-EU*. Ir pastāvīgi jācenšas nodrošināt sakaru kanālus starp politisko, operatīvo un tehnisko līmeni, kā arī uzlabot rīcības saskaņošanu ar datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīklu.

Eiropols ir arī iedarbinājis ES Tiesībaizsardzības ārkārtas reaģēšanas protokolu, kas ļauj pastiprināti uzraudzīt kibernetikas draudus un dalīties ar informāciju starp daudzām dažādām ieinteresētajām personām, lai gūtu visaptverošu priekšstatu par situāciju, balstoties uz kibernetikas izlūkošanas datiem.

Līdztekus kibernetikas draudu uzraudzībai dalībvalstīs EĀDD un Komisijas dienesti ir arī pastiprinājuši modrību attiecībā uz kritiskās infrastruktūras pakļautību fiziskiem draudiem, kas nav kibernetikas draudi. Kritiskā infrastruktūra un subjekti, kas to ekspluatē, var būt pakļauti fiziskiem riskiem, piemēram, sabotāžai, kuru īsteno valsts vai valsts sponsorēti rīcībbspēki, kas tādējādi varētu mēģināt atbaidīt ES.

Gatavība

Gatavība kibernetikas drošības un kritiskās infrastruktūras drošības jomā ir svarīgāka nekā jebkad agrāk, ņemot vērā, ka Eiropa ir pastiprināti pakļauta virknei kara izraisītu apdraudējumu. Cenšoties uzlabot gatavību, ir veiktas vairākas tiešas darbības, arī tādas, kas bija iekļautas jau pirms Krievijas agresijas pret Ukrainu. To vidū bija mācības, norādījumu sniegšana, likumdošana, noturības palielināšana kritiskajās nozarēs un darbs ar partneriem.

Eiropas Savienības Padomes prezidentvalsts Francija kopā ar Eiropas Ārējās darbības dienestu (EĀDD) un Eiropas Savienības Kibernetikas drošības aģentūru (*ENISA*) 2022. gada sākumā organizēja uz scenārijiem balstītas mācības *EU CyCLES* (*Cyber Crisis Linking Exercise on Solidarity*), kuru mērķis bija vairost informētību politiskā līmenī un stiprināt sadarbību starp operatīvo un politisko līmeni gadījumam, ja notiktu liela mēroga kibernetikas drošības krīze.

ENISA un *CERT-EU* februārī publicēja **pamatnostādnes** par to, kā palielināt noturību un gatavību ES⁸. Pamatnostādnēs visas publiskā un privātā sektora organizācijas ES tiek mudinātas īstenot kibernetikas drošības paraugprakses minimumu, lai ievērojami uzlabotu kibernetikas drošības kultūru. Martā *CERT-EU* ar *ENISA* atbalstu publicēja papildu tehniskās

⁸ *Boosting your Organisation's Cyber Resilience*, kopīgā publikācija, 14.2.2022.

norādes⁹, kā arī drošības norādes, kuras palīdz uzlabot *Signal* lietotņu¹⁰ konfigurāciju un kurās sniegti vairāki praktiski ieteikumi organizācijām, kā uzlabot to kiberdrošības situāciju.

Likumdošanas iniciatīvas

Pašreizējā situācija liek skaidri saprast, ka ir steidzami **jāsteno pašlaik spēkā esošie tiesību akti** un jāpaātrina **ieplānoto iniciatīvu pieņemšana**.

Komisija palīdz dalībvalstīm īstenot **TID direktīvu**¹¹, kurā dalībvalstīm ir noteikta prasība pienācīgi sagatavoties, piemēram, nodrošināt datordrošības incidentu reaģēšanas vienību (*CSIRT*) un noteikt kompetentās iestādes. Tā nodrošina pamatu rezultatīvai dalībvalstu sadarbībai. Likumdevēju politiskā vienošanās par **TID 2 direktīvu**¹² ir vēl viens liels solis uz priekšu ceļā uz spēcīgu ES gatavības satvaru.

TID 2 — vēl lielākas gatavības nodrošināšana

- Ar jauno Tīklu un informācijas sistēmu drošības direktīvu tiks novērsti iepriekšējās TID direktīvas trūkumi, pielāgojot to pašreizējām vajadzībām un padarot atbilstošu nākotnes prasībām. Tajā ir izklāstīti tiesiskā regulējuma minimālie noteikumi un noteikti mehānismi, kas izmantojami efektīvai sadarbībai starp attiecīgajām iestādēm katrā dalībvalstī.
- Ar to tiek paplašināta noteikumu darbības joma, tajā iekļaujot vēl citas nozares, kas ir kritiski svarīgas ekonomikai un sabiedrībai (piemēram, farmācijas un medicīnisko ierīču nozare vai pārtikas ražošana). Direktīva attieksies uz visiem vidējiem un lielajiem uzņēmumiem, kas darbojas šajās nozarēs vai sniedz pakalpojumus, kuri ietilpst direktīvas darbības jomā. Direktīva attiecas arī uz centrālās valdības publiskās pārvaldes struktūrām (izņemot tiesu iestādes, parlamentus un centrālās bankas) un reģionālajām publiskās pārvaldes struktūrām. Papildus tam dalībvalstis var nolemt, ka direktīvu piemēro arī vietēja līmeņa publiskās pārvaldes struktūrām.
- Ar TID 2 tiks noteikts kiberdrošības riska pārvaldības pasākumu pamatscenārijs un tiek oficiāli izveidots Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*), kas palīdzēs koordinēti pārvaldīt liela mēroga kiberdrošības incidentus.
- Priekšlikumā ir arī iekļauti precīzāki noteikumi par incidentu paziņošanas procesu, ziņojumu saturu un grafiku un paredzēti tiesiskās aizsardzības līdzekļi un sankcijas, ar ko nodrošināt izpildi.
- Dalībvalstīm būs jāiekļauj šie noteikumi savos valsts tiesību aktos 21 mēneša laikā no direktīvas stāšanās spēkā.

Pēc panākumiem TID 2 jomā pēc iespējas drīz būtu jāpabeidz sarunas par ierosināto **Direktīvu par kritisko vienību noturību**¹³ (“KVN direktīva”), kam pēc tās pieņemšanas un īstenošanas vajadzētu palielināt kritisko vienību noturību pret dažādiem draudiem, ieskaitot teroristu uzbrukumus, iekšnieku draudus un sabotāžu. Ir arī būtiski, lai Direktīvas par kritisko

⁹ Drošības norādes 2022-01 *Cybersecurity mitigation measures against critical threats*.

¹⁰ *CERT-EU* drošības norādes 22-002 *Hardening Signal*.

¹¹ Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

¹² COM(2020) 823.

¹³ COM(2020) 829.

vienību noturību vēriens atbilstu Komisijas priekšlikuma vērienam un lai tiktu saglabāta saskaņa ar politisko kompromisu, kas tika panākts attiecībā uz TID 2. Kopā šie pasākumi uzlabos noturību un gatavību, radot saskaņotāku un spēcīgāku sistēmu, kuras viens no elementiem būs valstu plāni reaģēšanai uz incidentiem un krīzēm. Tie bija paredzēti arī Komisijas pagājušā gada Ieteikumā¹⁴ par **Kopējās kibervienības** izveidošanu, kurā bija izklāstīts, kā dažādiem kibersdrošības ekosistēmas dalībniekiem (diplomātiskajiem, policijas, civilajiem un attiecīgā gadījumā aizsardzības) jāsadarbojas operatīvajā līmenī. Pašreizējā drošības apdraudējumu ainā ir skaidri redzams, cik liela vērtība ir šādai rezultatīvai sadarbībai starp galvenajiem dalībniekiem.

Komisija turpina uzraudzīt **5G** kibersdrošības rīkkopas¹⁵ īstenošanu. Šajā saistībā TID sadarbības grupa 11. maijā pieņēma ziņojumu par *Open RAN* drošību¹⁶. Tā arī turpina kopā ar dalībvalstīm strādāt, lai padarītu Eiropas Kibersdrošības kompetenču centru pilnīgi darbīgu.

2022. gada 22. martā Komisija ierosināja **jaunus noteikumus, lai ieviestu kopīgus kibersdrošības un informācijas drošības pasākumus visās ES iestādēs, struktūrās un aģentūrās (ES ISA)**. Šie noteikumi uzlabos ES administrācijas noturību un spēju reaģēt uz kibersdraudiem un incidentiem. Iekļaujot šīs darbības kopīgā satvarā, tiks stiprināta iestāžu sadarbība un mazināta pakļautība riskam. Saskaņā ar ierosināto **ES ISA kibersdrošības regulu**¹⁷ tiks paplašinātas *CERT-EU* pilnvaras un izveidota jauna iestāžu Kibersdrošības padome, un regula palielinās kibersdrošības spējas un veicinās regulāru gatavības novērtēšanu un kibersdrošības uzlabojumus. Ar ierosināto **Informācijas drošības regulu**¹⁸ tiks izveidots informācijas drošības noteikumu un standartu minimums drošai visu ES ISA informācijas apstrādei un apmaiņai, lai nodrošinātu pastiprinātu un konsekventu aizsardzību pret augošajiem draudiem to informācijai. Komisija aicina Eiropas Parlamentu un Padomi drīz pieņemt šos pasākumus.

Komisija nu ir pabeigusi savu sabiedrisko apspriešanu par pasākumiem, kuru mērķis ir uzlabot digitālo produktu **kibernoturību**, un tā gatavo priekšlikumu, ko paredzēts publicēt šoruden¹⁹. Tajā pievērsīsies digitālo produktu un papildpakalpojumu neaizsargātībai; šie produkti un pakalpojumi sniedz iespējas ES ekonomikai un sabiedrībai, taču rada arī jaunas problēmas, ņemot vērā, ka, jo vairāk viss ir savā starpā savienots, jo vieglāk kādam kibersdrošības incidentam ietekmēt visu sistēmu un tādējādi pārraut ekonomiskās un sociālās norises.

2022. gada 9. martā ES ministri, kas atbildīgi par telesakariem, vienprātīgi pieņēma Nevēras Aicinājumu pastiprināt ES kibersdrošības spējas, kurā cita starpā bija paredzēts “īstenot jaunu Ārkārtas reaģēšanas fondu kibersdrošībai, kas jāievieš Komisijai”²⁰. Komisija pašlaik ir

¹⁴ [Ieteikums par Kopējās kibervienības izveidošanu | Eiropas digitālās nākotnes veidošana \(europa.eu\)](#).

¹⁵ <https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>

¹⁶ TID sadarbības grupa, *Report on the cybersecurity of Open RAN*, 2022. gada 11. maijs.

¹⁷ COM(2022) 122.

¹⁸ COM(2022) 119.

¹⁹ [Kibernoturības akts — jauni kibersdrošības noteikumi attiecībā uz digitālajiem produktiem un papildpakalpojumiem](#)

²⁰ [8.3.2022., Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique - Presse - Ministère des Finances \(economie.gouv.fr\)](#)

pārdomās par to, kā labāk izmantot pašreizējos fondus, lai atbalstītu preventīvus un reaģēšanas pasākumus.

Kritiskās nozares

ES **energoapgādes** drošība ir kritiski svarīga iedzīvotāju labklājībai un netraucētai mūsu ekonomikas darbībai, un pašreizējā situācija ir cēlusi gaismā vajadzību pēc skaidriem noteikumiem par kiberdrošību šajā nozarē. Komisija, kā prasīts Elektroenerģijas regulā²¹, gatavo tīkla kodeksu par pārrobežu elektroenerģijas plūsmu kiberdrošību, kurā paredzēs noteikumus par riska novērtējumiem, kopīgām minimālajām prasībām, plānošanu, uzraudzību, ziņošanu un krīzes pārvaldību. Kopš ir sācies Krievijas agresīvais karš pret Ukrainu, kiberdrošības tīkla kodeksam noteiktie mērķi ir ieguvuši vēl jo lielāku nozīmi. Komisija ir arī sākusi strukturālu sadarbību starp *ENISA*, *ENTSO-E*²², *ENTSO*²³ un Enerģētikas kopienu kiberdrošības situācijas regulārā uzraudzīšanā enerģētikas nozarē.

ES ir strādājusi, lai aizsargātu partneru drošību, neradot jaunus riskus sev pašai. 2022. gada martā pēc risku, īpaši kiberdrošības risku, mazināšanas pasākumu pieņemšanas notika Ukrainas un Moldovas elektrotīklu ārkārtas sinhronizēšana ar kontinentālās Eiropas tīklu.

Karš un sankcijas ir radījuši daudz problēmu arī ES **transporta** nozarei, sākot ar drošības riskiem, kas apdraud ES civilo aviāciju un kravas automobiļu vadītājus, kuri ir iestrēguši konflikta zonās, un beidzot ar Ukrainas transporta infrastruktūras iznīcināšanu, kā rezultātā tiek pārrautas piegādes ķēdes un apdraudēts pasaules pārtikas nodrošinājums. Eiropas Savienības Aviācijas drošības aģentūra ciešā sadarbībā ar Komisiju un Eiropas Aeronavigācijas drošības organizāciju Eirokontroli kopš kara sākuma ir ieteikusi operatoriem nedarboties Ukrainas gaisa telpā un neizmantot arī gaisa telpu 100 jūras jūdžu rādiusā no Baltkrievijas un Krievijas/Ukrainas robežas.

Komisija ir arī strādājusi, lai stiprinātu ES transporta nozares gatavību un noturību. Konkrētāk, 23. maijā tika pieņemts jauns Ārkārtas rīcības plāns transporta nozarei²⁴, kurā ir ņemtas vērā mācības, kas gūtas gan saistībā ar Covid-19 pandēmiju, gan saistībā ar Krievijas militāro agresiju pret Ukrainu. Tajā ir ierosināts 10 darbību instrumentu kopums, kas kalpos par orientieri ES un tās dalībvalstīm, kad tās ievieš ārkārtas pasākumus reaģēšanai uz krīzi, kuru vidū ir minimālās savienojamības nodrošināšana, noturības pret kiberdraudiem un hibrīddraudiem veidošana un sadarbības ar starptautiskajiem partneriem uzlabošana gatavības krīzēm un reaģēšanas uz krīzēm jomā. Tajā ir arī uzsvērts, cik svarīgi ir regulāri testēt noturību pret dažādām krīzēm, testēšanā iesaistot attiecīgās ES aģentūras vai citus dalībniekus un balstoties uz pastāvošajiem procesiem.

Saskaņā ar **ES Veselības drošības** satvaru informācijas apmaiņa, kas balstīta uz agrīnās brīdināšanas un reaģēšanas sistēmu, ieskaitot informācijas apmaiņu saistībā ar atbalstu medicīniskajai evakuācijai no Ukrainas, ir jāaizsargā pret kiberuzbrukumiem, tāpēc šīs sistēmas drošība tiek pastiprināta.

²¹ Eiropas Parlamenta un Padomes Regula (ES) 2019/943 (2019. gada 5. jūnijs) par elektroenerģijas iekšējo tirgu (OV L 158, 14.6.2019., 54. lpp.). Pašlaik Energoregulatoru sadarbības aģentūra pārskata priekšlikumu.

²² Elektroenerģijas pārvades sistēmu operatoru Eiropas tīkls.

²³ Gāzes pārvades sistēmu operatoru Eiropas tīkls.

²⁴ COM(2022) 211.

Sadarbība ar partneriem

ES turpina sadarboties ar starptautiskajiem partneriem, lai novērstu ļaunprātīgu rīcību kibertelpā, mazinātu motivāciju šādi rīkoties, atturētu no šādas rīcības un reaģētu uz to. Krievijas agresīvais karš pret Ukrainu ir padarījis sadarbību šajā jomā svarīgāku nekā jebkad agrāk. Šajā saistībā EĀDD ir strādājis, lai apmainītos ar informāciju par situāciju un koordinētu reaģēšanu uz ļaunprātīgām kiberdarbībām, kas vērstas pret Ukrainu, kā arī veicis darbu ar mērķi atbalstīt Ukrainu un citus tai pašā reģionā esošos un šajā jautājumā sadarbojies ar tādiem partneriem kā ASV un NATO, lai nodrošinātu papildināmību un izvairītos no darbību pārklāšanās.

Ciešā sadarbība ar ASV ir pastiprinājusies arī ES un ASV Tirdzniecības un tehnoloģiju padomē (*TTC*). Kopīgajā paziņojumā²⁵, kas tika izdots pēc maijā Parīzē notikušās ministru sanāksmes, tika uzsvērts, cik liela nozīme atjaunotās transatlantiskās partnerības kontekstā ir *TTC*, kas palīdz koordinēt ES un ASV kopīgos pasākumus, kuri saistīti ar Krievijas agresiju pret Ukrainu. Abas puses piekrita, ka pašlaik vairāk nekā jebkad agrāk ir svarīgi cieši sadarboties, lai vairotu piegādes ķēžu noturību. Papildus tam tika izveidota īpaša darba grupa jautājumos par publisko finansējumu drošai un noturīgai digitālajai infrastruktūrai trešās valstīs, lai bruģētu ceļu kopīgam ASV un ES publiskajam finansējumam digitālajiem projektiem trešās valstīs, pamatojoties uz kopīgu vispārēju principu kopumu.

2022. gada martā pieņemtais Stratēģiskais kompass (sk. VII iedaļu) papildus nostiprinās ES kiberdiplomātijas rīkkopu un attīstīs ES kiberaizsardzības politiku, lai labāk sagatavotos kiberuzbrukumiem un varētu labāk reaģēt uz tiem, un šie pasākumi ir daļa no plašākas stratēģijas, kā mērķis ir stiprināt ES spējas rīkoties krīžu gadījumā un aizstāvēt savas intereses.

Ar kiberdrošību saistīts atbalsts Ukrainai un kaimiņvalstīm

ES veicināja Ukrainas kiberneturību jau pirms kara. Jau 2021. gada jūnijā ES un Ukraina sarīkoja pirmo dialogu par kiberjautājumiem, un ES sniedza atbalstu kiberdrošībai un pret riskiem noturīgai digitālajai pārveidei, izmantojot 25 miljonus EUR vērtu iniciatīvas *EU4Digital* Ukrainas programmu. Papildus tam ir vēl arī 1,5 miljonu EUR vērtā mērķsadarbības programma, kuras mērķis ir palīdzēt Ukrainas kiberdrošības iestādēm pielāgoties ES standartiem.

Pēc kara sākuma ES veicina sadarbību starp ES un Ukrainas kiberdrošības ekspertiem un koordinē tehniskās palīdzības, aprīkojuma, programmatūras un attiecīgu pakalpojumu nodrošināšanu, lai stiprinātu Ukrainas kiberneturību un kiberaizsardzību.

ES arī strādā, lai novērtētu iespējamo vidēja termiņa atbalstu Moldovai, Gruzijai un Rietumbalkāniem. 2022. gada 3. un 4. martā Moldovā notika kopīga kiberdrošības vajadzību novērtēšanas misija, un pēc tam tika pieņemts īpašs pasākums reaģēšanai uz krīzi, lai strauji palielinātu kiberdrošību valstī. Līdzīgs ātrās reaģēšanas atbalsts tiek gatavots arī vairākām Rietumbalkāņu valstīm, kuras ir uzskatāmas par īpaši pakļautām riskam, jo atbalsta ES sankcijas. Tiek izvērtēta arī iespēja sniegt papildu palīdzību Moldovai, izmantojot Eiropas Miera mehānismu.

²⁵ https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_3108

III. ORGANIZĒTĀ NOZIEDZĪBA UN TERORISMS

Krievijas agresīvais karš pret Ukrainu ir licis miljoniem cilvēku pamest mājas, tādējādi ievērojami pastiprinot kustību pāri ES ārējām robežām. Līdz 18. maijam ES bija ieradušies gandrīz 6 miljoni cilvēku no Ukrainas un Moldovas, un līdz šim 2,8 miljoni ir reģistrējušies pagaidu aizsardzībai ES. ES ir centusies nodrošināt cik vien iespējams ātru un elastīgu uzņemšanu no kara bēgošajiem, neapdraudot drošību pie ES ārējās robežas. ES ir īstenojusi vēl nepieredzētus pasākumus, lai piedāvātu no kara bēgošajiem pagaidu aizsardzību, un ir apņēmusies pievērsties visiem jauniebraucējiem bez jebkādas diskriminācijas. Tai pašā laikā nevar neņemt vērā riskus, ko var radīt tik daudzu cilvēku pārvietošanās, un ES ar spēcīgu atbalstu no attiecīgajām ES aģentūrām saglabā modrību, lai nepalaistu garām jaunas norises organizētajā noziedzībā un terorismā.

Spēcīga Šengenas zona palielinātu draudu laikā

Augsta līmeņa drošības garantēšana **Šengenas** zonā un ES nekad nav bijusi tik svarīga kā laikā, kad ir pastiprinājušies draudi, ko rada turpat pie ES ārējās robežas notiekošais karš.

Komisija maijā pieņēma pirmo ziņojumu par stāvokli Šengenas zonā²⁶, kurā ziņoja par panākumiem 2021. gada jūnija stratēģijā izklāstītās vērienīgās Šengenas zonas programmas īstenošanā. Ikgadējais Šengenas cikls paredz jaunu Šengenas zonas pārvaldības modeli, kas ietver regulāru Šengenas zonas stāvokļa veselīguma pārbaudi. Tas palīdzēs ātri atklāt trūkumus un īstenot efektīvas turpmākas procedūras, lai padarītu Šengenas zonu stiprāku un noturīgāku.

Minētajā pirmajā ziņojumā ir atzīta vajadzība pastiprināt centienus īstenot galvenās ES līmeņa iniciatīvas, ieskaitot sistemātiskas visu ceļotāju pārbaudes pie ārējām robežām, pilnvērtīgi izmantojot *Frontex* un Eiropola pilnvaras, kā arī ierosinātos un jau pieejamos policijas pārrobežu sadarbības instrumentus.

Konkrētāk, iekšējās drošības un robežu pārvaldības uzlabošanas centienu stūrakmens ir jaunā robežu, migrācijas un drošības ES informācijas sistēmu arhitektūra un šo sistēmu sadarbība. Būs ļoti svarīgi rezultatīvi ieviest visus sadarbības sistēmas elementus, ievērojot noteiktos termiņus.

Modrība un koordinācija

Spēcīgāka tiesībsardzības iestāžu sadarbība starp dalībvalstīm un ar trešām valstīm ir ļoti svarīga, lai varētu apzināties jaunus noziedznieku un teroristu draudus un vērsties pret noziedznieku tīkliem un personām, kas var censties izmantot karu pret Ukrainu savā labā. Dalībvalstis un operatīvie partneri aktīvi dalās būtiskā pieejamā informācijā un kriminālizlūkošanas datus ar Eiropolu, kas pārbauda un analizē informāciju un pārvērš to praktiski izmantojamās operatīvās izlūkošanas paziņojumos, piemēram, agrīnās brīdināšanas paziņojumos un draudu novērtējumos, kuri tiek nodoti partneriem.

²⁶ COM(2022) 301.

Organizētā noziedzība

Organizētie noziedznieki jau ir raduši veidus, kā savā labā izmantot pašreizējo situāciju. Sākotnējā izlūkdatu analizē atklājās noziedzīgās darbības modeļi vairākās jomās, ieskaitot cilvēku tirdzniecību, nepatiesas deklarācijas par importētajām un eksportētajām precēm, krāpšanu tiešsaistē, kibernetizāciju un šaujamo ierociņu nelikumīgu tirdzniecību. Ir arī pierādījumi tam, ka kibernetizācija izliekas par līdzekļu vācējiem Ukrainai, lai nozagtu naudu un kriptovalūtas²⁷. Noziedzīgās organizācijas no Ukrainas pašreizējās situācijas dēļ var centties pārcelties uz citu vietu un turpināt savas darbības ES.

Komisija un Padomes prezidentvalsts Francija sadarbojās savā starpā, kā arī ar ES tieslietu un iekšlietu aģentūrām, īpaši Eiropolu, lai mobilizētu Eiropas daudzdisciplīnu platformu pret noziedzības draudiem (*EMPACT*) nolūkā novērtēt, paredzēt, novērst un apkarot pastāvošus un jaunus nopietnas un organizētas noziedzības draudus. 2022. gada 7. aprīlī Eiropols sarīkoja *EMPACT* sanāksmi, kurā pulcējās pārstāvji un eksperti no ES dalībvalstīm un ES drošības kopienas, lai pievērstos problēmām saistībā ar nopietnas un organizētas noziedzības draudiem, kas radušies Ukrainā notiekošā kara dēļ. Tika apspriesti tādi konkrēti soļi kā plašāku izlūkdatu apkopošana, ārkārtas operatīvo darbību īstenošana un pašreizējo operatīvo darbību mērķa maiņa, kā arī *ad hoc* kopīgas rīcības dienas.

Austrumu un dienvidaustrumu sauszemes robežas muitas ekspertu grupa (*CELBET*) — sadarbības projekts, ko finansē Eiropas Komisija, — seko līdzi notikumiem pie robežas, tādējādi pildot savu uzdevumu sniegt operatīvo atbalstu un norādījumus muitas amatpersonām, un uzrauga muitas veikto konfiskāciju robežšķērsošanas vietās, kas atrodas uz ES robežas ar Ukrainu (Polijā, Slovākijā, Ungārijā un Rumānijā).

Noziedzīgas un teroristiskas darbības

Lai gan Eiropas Savienībā saistībā ar Krievijas iebrukumu Ukrainā vēl nav radušies tieši terorisma draudi, ir skaidrs, ka jābūt modriem.

Paaugstinātais noziedzīgu un teroristisku darbību risks skaidri parāda, cik svarīgi ir, lai dalībvalstis izmantotu attiecīgās ES datubāzes, piemēram, Šengenas Informācijas sistēmu, nepieciešamības gadījumā ievadītu tajās datus un ieskatītos tajās, pārbaudot personas, kas ierodas ES. Tas palīdzēs nodrošināt, ka personas, kas apdraud ES iekšējo drošību, tiek atklātas pie ārējām robežām. Eiropas Savienības Aģentūra lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*) turpina nodrošināt, ka ES robežu pārvaldības sistēmas ir pilnīgi pieejamas un efektīvi darbojas. Norādījumos²⁸ dalībvalstīm ir paskaidrots, kā rast līdzsvaru starp vajadzību raiti tikt galā ar cilvēku ierašanos pie ārējās robežas un vajadzīgo drošības pārbaužu veikšanu.

Gatavība

²⁷ Google Draudu analīzes grupa novēroja, ka ir pieaudzis to apdraudētāju skaits, kas karu Ukrainā izmanto par ēsmu pikšķerēšanas un ļaunprogrammatūras kampaņās. Interneta drošības uzņēmuma *Cyren* pētnieki ziņo, ka ir pieaudzis tādu ar kriptovalūtām saistītas krāpniecības gadījumu skaits, kuros šo konfliktu izmanto, lai aicinātu ziedot neīstās ziedojumu vākšanas tīmekļa vietnēs.

²⁸ Komisijas paziņojums “Operatīvās vadlīnijas ārējo robežu pārvaldībai ar mērķi atvieglināt robežšķērsošanu pie ES un Ukrainas robežām”, 2022/C 104 I/01.

ES gatavība ir stiprināta ne vien ar norādījumiem un koordināciju, bet arī izvietojot ES aģentūru darbiniekus.

Eiropols ir izvietojis operatīvās grupas ES dalībvalstīs, kas atrodas blakus Ukrainai. Šīs grupas sastāv no Eiropola pieaicinātajām amatpersonām no dalībvalstīm un Eiropola ekspertiem un atrodas Ungārijā, Lietuvā, Polijā, Rumānijā, Slovākijā un Moldovā²⁹. Eiropola pieaicinātās amatpersonas palīdz valstu iestādēm veikt drošības pārbaudes otrajā līnijā pie ES ārējām robežām. Eiropola eksperti sniedz atbalstu, vācot un izvērtējot informāciju, lai atklātu terorisma un noziedzības draudus, palīdzētu izmeklēšanā un atklātu personas, kas, cenšoties iekļūt ES, rada risku. Šīs operatīvās grupas vāc informāciju, kas tiek izmantota noziedzības draudu novērtējumos, kuri ir pieejami dalībvalstīm. Šī izlūkdatu vākšana dod iespēju Eiropolam prognozēt notikumu attīstību un saskaņot operatīvās darbības ar ES dalībvalstīm, lai reaģētu uz darbībām, ko veic noziedznieku grupas, kuras vēlas gūt labumu no kara Ukrainā, un papildināt Eiropola aktīvo sadarbību ar Ukrainas tiesībsardzības iestādēm, kas norit ar Eiropola galvenajā mītnē Nīderlandē esošā Ukrainas sadarbības koordinatora starpniecību.

Dalībvalstīs un ES kaimiņvalstīs atrodas arī **Eiropas Robežu un krasta apsardzes aģentūra (Frontex)**, lai atbalstītu robežkontroles darbības, — pašlaik visā ES, Rietumbalkānos un Moldovā kopā ir izvietots vairāk nekā 2100 robežsargu. **Eiropas Savienības Patvēruma aģentūra (EUAA)** ir izvietojusi gandrīz 750 darbinieku ES dienvidu dalībvalstīs un Lietuvā, lai atbalstītu operatīvās darbības, palielinātu uzņemšanas spējas un palīdzētu īstenot patvēruma procedūras.

Pamatojoties uz pašlaik spēkā esošo **Prīmes lēmumu**³⁰, kas dalībvalstīm nodrošina satvaru tiesībsardzības amatpersonu nosūtīšanai uz kopīgām operācijām, piemēram, kopīgām patruļām, Komisija un Eiropas Savienības Padomes prezidentvalsts Francija nosūtīja kopīgu vēstuli visām dalībvalstīm, lai apzinātu vajadzības un lūgtu nosūtīt policistus, kas nepieciešams, lai varētu sākt kopīgas patruļas ES priekšposteņa dalībvalstīs, ko kara izraisītā robežu masveida šķērsošana skar visvairāk. Komisija finansēs šo amatpersonu izvietojumu no fonda "Iekšējās drošības fonds — policija".

Vēršanās pret cilvēku tirdzniecību

Kopš kara pirmajām dienām ES īpaši lielu vērību pievērš riskiem, ko rada viena konkrēta noziedzības joma, kas varētu gūt labumu no tā, ka cilvēki masveidā dodas meklēt drošību ES. Ļoti svarīgs uzdevums ir bijis nepieļaut, ka cilvēku tirgotāji ar, piemēram, nepatiesiem transporta vai izmitināšanas piedāvājumiem ievilina briesmās neaizsargātus cilvēkus, kas atrodas ceļā un lielākoties ir **sievietes un bērni**.

Martā Eiropols un *Eurojust* attiecīgajām valstu iestādēm izdeva agrīnās brīdināšanas paziņojumus par iespējamu cilvēku tirdzniecību un no Ukrainas ierodošos cietušo izmantošanu. *Eurojust* palīdz uzlabot informācijas apmaiņu un paātrināt tiesu iestāžu

²⁹ Saskaņā ar 3. maija datiem Eiropols ir izvietojis vienu Eiropola darbinieku un trīs pieaicinātās amatpersonas Slovākijā, vienu Eiropola amatpersonu Polijā, vienu Eiropola amatpersonu un četras pieaicinātās amatpersonas Rumānijā un divas pieaicinātās amatpersonas Ungārijā. Viens Eiropola darbinieks un divas pieaicinātās amatpersonas ir izvietotas Moldovā.

³⁰ 2008/615/TI, 2008/616/TI.

sadarbību, arī ar Ukrainu, un aģentūrai ir uzdots koordinēt cilvēku tirdzniecības gadījumu izmeklēšanu.

ES koordinators cilvēku tirdzniecības apkarošanas jomā ir rīkojis sanāksmes ar ES valstu ziņotāju un līdzvērtīgu mehānismu tīklu, tieslietu un iekšlietu aģentūrām un ES Pilsoniskās sabiedrības platformu cīņai pret cilvēku tirdzniecību, lai pārrunātu darbības, kas jāveic, lai novērstu un apkarotu ļaunprātīgu izmantošanu un aizsargātu cietušos. Vairākās dalībvalstīs ir sākta izmeklēšana par iespējamiem šādiem gadījumiem.

ES ir ātri un aktīvi nodrošinājusi koordinētu reakciju uz šo reālo draudu cilvēkiem, kam nepieciešama ES palīdzība. Dalībvalstīm, kas īsteno Pagaidu aizsardzības direktīvu, lai palīdzētu tiem, kuri bēg no kara Ukrainā, tika ātri piedāvātas operatīvās vadlīnijas³¹, arī par cilvēku tirdzniecības problēmu. Saskaņā ar 10 punktu plānu, kā stiprināt koordinēšanu no kara Ukrainā bēgošo cilvēku sagaidīšanā Eiropā³², ar ko nāca klajā 2022. gada 28. martā Tieslietu un iekšlietu padomē, ES koordinators cilvēku tirdzniecības apkarošanas jomā sadarbībā ar ES aģentūrām un dalībvalstīm ir izstrādājis Kopīgu cilvēku tirdzniecības apkarošanas plānu³³, kā novērst cilvēku tirdzniecību un palīdzēt cietušajiem. Īpaša liela uzmanība ir pievērsta to struktūru un personu (arī brīvprātīgo) reģistrēšanai, kuri ir iecerējuši nodrošināt izmitināšanu, transportu un citu veidu palīdzību, kā arī iepriekšējās darbības pārbaužu veikšanai. Komisija ir arī sadarbojusies ar *EUAA*, lai palīdzētu atklāt cilvēku tirdzniecībā cietušos, kad uzņemšanas centros tiek veikta veselības stāvokļa novērtēšana. Nepavadīti un no vecākiem nošķirti bērni ir īpaši pakļauti vardarbības, seksuālas izmantošanas un piespiedu noziedzības riskam. Iepriekš minētajās operatīvajās vadlīnijās ir sniegti arī tādi norādījumi, kas palīdz dalībvalstīm tikt galā ar bērnu, jo īpaši nepavadītu nepilngadīgo, ierašanos, uzņemšanu un atbalstīšanu. Lai vairotu riskam pakļauto personu informētību, Komisija ir arī izveidojusi īpašu tīmekļa vietni, kurā vienā no sadaļām ir sniegti praktiski padomi par to, kā izvairīties no cilvēku tirgotājiem.

Daļa gatavības palielināšanas darbību ir veiktas, reaģējot tieši uz jaunajiem kara radītajiem apstākļiem, taču citi svarīgi pasākumi izriet no **likumdošanas iniciatīvām**, kas jau bija iepļānotas pirms Krievijas agresīvā kara pret Ukrainu.

Komisija pauž atzinību par 2022. gada februārī panākto vienošanos par pārskatītajām **Eiropola** pilnvarām³⁴, kas, līdzko būs ieviestas, dos iespēju Eiropalam labāk atbalstīt dalībvalstis cīņā pret organizēto noziedzību un terorismu. Tad aģentūrai būs vajadzīgie rīki un aizsardzības pasākumi, lai palīdzētu policijai analizēt lielos datus noziegumu izmeklēšanas nolūkā un izstrādāt jaunas metodes kibernetiskās noziedzības apkarošanai. Šīs izmaiņas papildina pastiprināts datu aizsardzības satvars, stingrāka parlamentārā pārraudzība un lielāka pārskatatbildība.

³¹ C/2022/1806, EUR-Lex — 52022XC0321(03) — LV — EUR-Lex (europa.eu).

³² https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en

³³ https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en

³⁴ COM(2020) 796.

Tiesību aktu kopums **policijas sadarbības** jomā, ar kuru Komisija nāca klajā 2021. gada 8. decembrī³⁵ un par kuru pašlaik notiek sarunas, pastiprinās sadarbību starp dažādu dalībvalstu tiesībsardzības amatpersonām, padarot datu apmaiņu ātrāku, vieglāku un drošāku un pastiprinot un padarot efektīvāku operatīvo policijas sadarbību uz vietas. Komisija aicina Eiropas Parlamentu un Padomi ātri pieņemt šo tiesību aktu kopumu.

Kad šie tiesību aktu priekšlikumi būs pieņemti un īstenoti, tie atbalstīs tiesībsardzības iestāžu cīņu pret organizēto pārobežu noziedzību. Tam būs īpaši liela nozīme apstākļos, kad noziedzīgās organizācijas no Ukrainas pašreizējās situācijas dēļ var censties pārcelties uz citu vietu un turpināt savas darbības ES.

ES padomdevēja misija Ukrainā ir atbalstījusi tiesībsardzības un tiesiskuma iestāžu reformu valstī kopš 2014. gada. 2022. gada martā misijas pilnvaras tika pārskatītas, dodot iespēju sniegt atbalstu robežšķērsošanas vietās uz Ukrainas robežas ar Poliju, Rumāniju un Slovēniju, palīdzot labāk apzināties situāciju noziedzīgu pārobežu darbību, tostarp cilvēku tirdzniecības, jomā un veicinot humāno preču ieviešanu Ukrainā.

IV. IEROČI, BĪSTAMI MATERIĀLI UN KRITISKI INCIDENTI

Karš ir ārkārtīgi palielinājis šaujamieroču un citu ieroču apriti pašā Ukrainā, kas rada jaunus riskus ES un citām Ukrainas kaimiņvalstīm.

Modrība un koordinācija

Martā izdotajās operatīvajās vadlīnijās dalībvalstīm bija sniegti padomi par to, kā tikt galā ar problēmu, ka ir palielinājusies šaujamieroču aprite, laikā, kad pie ES ārējās robežas masveidā ierodas cilvēki³⁶. Šajās vadlīnijās ir uzsvērts, ka būtu pastāvīgi jāpārbauda ieroču klātbūtne un nevienu, kuram nav atļaujas, nedrīkstētu ielaist ES ar šaujamieroci. Ja Ukrainas iestādes par kādu no šiem šaujamieročiem ir ziņojušas kā par pazudušu, dalībvalstīm par attiecīgajiem šaujamieročiem būtu jāziņo Šengenas Informācijas sistēmā.

Ir ārkārtīgi svarīgi, lai visi šaujamieroču sūtījumi uz Ukrainu tiktu pienācīgi reģistrēti, norādot visu attiecīgo informāciju (ieskaitot tipu, ražošanas valsti un gadu, zīmolu, marķu, kalibru, sērijas numuru), lai šos šaujamieročus būtu vieglāk izsekot gan Ukrainā, gan ES.

ES ir publiski paudusi nožēlu par Krievijas neapdomīgajiem militārajiem uzbrukumiem Ukrainā esošiem civiliem kodolobjektiem, bioloģiskajiem un ķīmiskajiem objektiem un to tuvākajai apkārtnē un par visām darbībām, kas apdraud šo objektu drošību. Komisija novēro situāciju Ukrainā, īpašu uzmanību pievēršot radioloģiskajiem draudiem, kas rada ļoti lielas bažas no ES iekšējās drošības viedokļa³⁷. Komisija monitorē arī iespējamās ķīmiskos draudus un ir izveidojusi iekšējās koordinācijas mehānismu gadījumam, ja būtu vajadzīga ātra riska novērtēšana.

Gatavība

³⁵ COM(2021) 780, COM(2021) 782, COM(2021) 784.

³⁶ Komisijas paziņojums "Operatīvās vadlīnijas ārējo robežu pārvaldībai ar mērķi atvieglināt robežšķērsošanu pie ES un Ukrainas robežām", 2022/C 104 I/01.

³⁷ Komisija sadarbībā ar partneriem no ASV organizēs darbsemināru par riskiem, kas saistīti ar tajās slimmīcās esošiem radioloģiskiem materiāliem, pār kurām tiek zaudēta regulatīvā kontrole.

Ukraina jau ir viena no valstīm, kas ES 2020.–2025. gada rīcības plānā attiecībā uz šaujamo nelikumīgu tirdzniecību ir atzītas par ļoti svarīgām, ņemot vērā konkrētas ārējas darbības. Papildus tam reģionā, kur atrodas arī Ukraina, tiek veikts īpašs operatīvais pasākums kā daļa no *EMPACT* rīcības šaujamo jomā. Taču, ņemot vērā šaujamo novirzīšanas risku, būs vajadzīgi īpaši ES finansēti projekti, kā arī operatīvā sadarbība ar Eiropu, *Frontex* un *EMPACT* šaujamo sadaļu. Komisija drīz iesniegs priekšlikumu pārskatīt Šaujamo regulu³⁸ par civilo šaujamo eksportu, importu un tranzītu, un šis priekšlikums būs daļa no vispārējās juridiskās un operatīvās sistēmas, kuras mērķis ir novērst, atklāt un izmeklēt šaujamo nelikumīgu tirdzniecību un veikt kriminālvajāšanu par to.

Lai uzlabotu ES gatavību sabiedrības veselības riskiem, piemēram, ķīmiskiem, bioloģiskiem, radioloģiskiem un nukleāriem (*CBRN*) draudiem, un reaģēšanu uz tiem, Komisija palielina reaģēšanas spēju stratēģiskās rezerves, izmantojot ES civilās aizsardzības mehānismu (*UCPM*), ko finansē Veselības ārkārtas situāciju gatavības un reaģēšanas iestāde (*HERA*)³⁹. Komisijas dienesti strādā kopā, lai izveidotu 540,5 miljonu EUR *rescEU* stratēģiskos krājumus. Šajos krājumos ietilps aprīkojums un zāles, vakcīnas un citi terapijas līdzekļi, ar ko ārstēt pacientus, kuri ārkārtas situācijās nonākuši saskarē ar *CBRN* vielām, kā arī *rescEU* dekontaminācijas rezerve, kas nodrošinās dekontaminācijas aprīkojumu un ekspertu reaģēšanas vienības. Pirmais steidzamais solis, ko ES ir spērusi, ir *rescEU* medicīniskās rezerves mobilizēšana, lai iegādātos kālija jodīda tabletes, kuras var izmantot cilvēku pasargāšanai no kaitīgajām radiācijas sekām, kā arī citas Ukrainai nekavējoties nepieciešamas preces. Uz Ukrainu ar *UCPM* starpniecību un Francijas un Spānijas palīdzību jau ir nogādāti gandrīz trīs miljoni jodīda tablešu.

V. KOORDINĒTA RĪCĪBA AR MĒRĶI SAUKT KRIEVIJU PIE ATBILDĪBAS PAR AGRESIJU

ES ir izšķirīga loma starptautiskās sabiedrības darbībās, kuru mērķis ir izdarīt spiedienu uz Krieviju, lai tā izbeigtu nepieņemamo un starptautiskajām tiesībām neatbilstošu agresiju pret Ukrainas valsti un civiliedzīvotājiem, kas ierauti konfliktā. Spiedienu cita starpā izdara ar pasākumiem, ar kuriem parāda, kādas sekas gaida agresorus, ieskaitot bargas sankcijas, kā arī pasākumiem, kuru mērķis ir apzināt kara noziegumus un atvieglot kriminālvajāšanu par tiem.

Ierobežojoši pasākumi un konfiskācija

Kopš 2022. gada 21. februāra, kad Krievija atzina valdības nekontrolētos Ukrainas apgabalus Donecku un Luhansku, un 2022. gada 24. februāra, kad sākās iebrukums Ukrainā, ES ir piemērojusi Krievijai vēl nepieredzēti daudz ierobežojošu pasākumu. Līdz šim ir pieņemtas piecas sankciju paketes. Šie pasākumi koncentrējas uz svarīgākajām nozarēm, ieskaitot finanses, tirdzniecību, transportu, aizsardzību un plašsaziņas līdzekļus, un ir vērsti pret politisko un militāro eliti, kā arī ievērojamiem Krievijas un Baltkrievijas oligarhiem. Sarakstos jau iekļauts vairāk nekā 1000 personu un 80 struktūru. Padomē pašlaik tiek apspriesta sestā sankciju pakete.

³⁸ Eiropas Parlamenta un Padomes Regula (ES) Nr. 258/2012 (2012. gada 14. marts), ar kuru īsteno 10. pantu Apvienoto Nāciju Organizācijas Protokolā par šaujamo, to detaļu, sastāvdaļu un munīcijas nelikumīgu ražošanu un tirdzniecību, kas pievienots Konvencijai pret transnacionālo organizēto noziedzību (ANO Šaujamo protokols), un ievieš eksporta atļauju, kā arī importa un tranzīta pasākumus šaujamo ierociem, to detaļām, sastāvdaļām un munīcijai.

³⁹ [HERA Work Plan 2022 \(europa.eu\)](https://ec.europa.eu/external-action/operation-hera/)

Tas, cik liela ietekme būs šiem un iepriekšējiem ierobežojošajiem pasākumiem, kas vērsti pret personām un uzņēmumiem no Krievijas un Baltkrievijas, būs atkarīgs no to izpildes. ES koordinācija var ļoti palīdzēt novērst iespējamās sankciju nepilnības, un Komisija ieinteresētajām personām ir sniegusi lielu atbalstu ar rakstveida norādījumiem, ieinteresēto personu sanāksmēm un īpašu ekspertu grupu, kā arī sniegusi dažādus resursus, kas var atvieglot atbilstības nodrošināšanu.

Papildus tam Komisija ir izveidojusi darba grupu “Freeze and Seize”, kurā apvienojušies Komisijas dienesti, dalībvalstis, *Eurojust* un Eiropols. Līdz šim dalībvalstis ir ziņojušas, ka ir iesaldējušas aktīvus 9,89 miljardu EUR vērtībā⁴⁰. 11. aprīlī Eiropols kopā ar dalībvalstīm, *Eurojust* un *Frontex* sāka operāciju “Oscar”, lai atbalstītu finanšu izmeklēšanu un kriminālizmeklēšanu, kas vērsta pret noziedzīgi iegūtiem līdzekļiem, kuri pieder fiziskām un juridiskām personām, uz ko attiecas ar Krievijas karu pret Ukrainu saistītas ES sankcijas. ES darba grupa “Freeze and Seize” darbojas cieši līdzās G7 valstu (Apvienotās Karalistes, ASV, Francijas, Itālijas, Japānas, Kanādas un Vācijas) un līdzīgi domājošu partneru, tādu kā Austrālijas, izveidotajai darba grupai “Krievijas elites, tās aģentu un oligarhu jautājumu darba grupa” (*REPO*), kā arī ASV darba grupai *KleptoCapture* un Ukrainas darba grupai.

Darba grupa “Freeze and Seize” ir platforma informācijas un pieredzes apmaiņas koordinēšanai un atvieglošanai starp dalībvalstīm un norādījumu sniegšanai par sankciju īstenošanu, kā arī kriminālizmeklēšanas un konfiscēšanas paraugprakses apmaiņas atvieglošanai. Ir jo īpaši svarīgi, lai tiesībaizsardzības iestādes būtu modras un proaktīvas attiecībā uz noziegumiem, ko varētu izdarīt sankcijām pakļautās personas un struktūras. Darba grupas mērķis ir arī rosināt diskusijas par iespējām izmantot konfiscētos līdzekļus, piemēram, kā ieguldījumu Ukrainas atjaunošanā.

Komisija šodien pieņem **aktīvu atgūšanas un konfiscēšanas** tiesību aktu kopumu⁴¹, kurā ir ņemtas vērā mācības, kas gūtas, īstenojot Savienības ierobežojošos pasākumus pret personām un struktūrām no Krievijas un Baltkrievijas. Tas palīdzēs vieglāk efektīvi īstenot ES ierobežojošos pasākumus Savienībā, dodot iespēju ātri izsekot un identificēt īpašumu, kas pieder šādiem pasākumiem pakļautām personām vai struktūrām vai ko kontrolē šādas personas vai struktūras. Uzlabotais aktīvu atgūšanas un konfiscēšanas satvars tiks piemērots arī ierobežojošo pasākumu pārkāpumiem, un tādējādi varēs rezultatīvi izsekot, iesaldēt, pārvaldīt un konfiscēt līdzekļus, kas iegūti, pārkāpjot ierobežojošos pasākumus. Lai nodrošinātu, ka var faktiski konfiscēt līdzekļus no personām un struktūrām, kas pārkāpušas ierobežojošos pasākumus, Komisija šodien arī pieņem priekšlikumus par Padomes lēmumu, ar ko sankciju pārkāpšanu pievieno ES noziegumu sarakstam, kurš izveidots saskaņā ar LESD 83. panta 1. punktu⁴², un to papildina paziņojums⁴³, kā mērķis ir ierosināt direktīvu, ar ko tuvinātu noziedzīgu nodarījumu un par ierobežojošu pasākumu pārkāpumiem piemērojamo sodu definīcijas.

Skatoties plašāk, ar šo tiesību aktu kopumu tiek sperts liels solis uz priekšu cīņā pret organizēto noziedzību. Ar to tiek īstenota Komisijas apņemšanās, ko tā paudusi Drošības savienības stratēģijā un Organizētās noziedzības novēršanas stratēģijā 2021.–2025. gadam⁴⁴. Ar to tiek pārskatīta 2014. gada Konfiskācijas direktīva, Padomes 2007. gada Lēmums par

⁴⁰ Ir bloķēti arī Krievijas Centrālās bankas aktīvi aptuveni 23 miljardu EUR apmērā.

⁴¹ COM(2022) 245.

⁴² COM(2022) 247.

⁴³ COM(2022) 249.

⁴⁴ COM(2021) 170.

līdzekļu atguves dienestiem (LAD) un 2005. gada Pamatlēmums par noziedzīgi iegūtu līdzekļu, nozieguma rīku un īpašuma konfiscāciju, lai pastiprinātu spējas izsekot, identificēt un galu galā konfiscēt nelikumīgi iegūtus līdzekļus un tādējādi risinātu problēmu, ka Eiropas Savienībā tiek konfiscēta tikai ļoti maza šo līdzekļu daļa⁴⁵. Ar šo tiesību aktu kopumu tiek paplašināts aptverto noziedzīgo nodarījumu loks un pastiprināti noteikumi par konfiscēšanu gadījumos, kad notiesājošs spriedums krimināllietā par konkrētu noziegumu nav iespējams, bet konkrētie aktīvi nepārprotami ir iegūti noziedzīgās darbībās. Ar šo pārskatīšanu tiek arī vēl vairāk uzlabota iesaldēto un konfiscēto aktīvu pārvaldības efektivitāte un palielinātas LAD spējas izsekot un identificēt nelikumīgi iegūtus aktīvus. Jaunais ES aktīvu atgūšanas satvars ir veidots tā, lai aptvertu sarežģīto darbības veidu, kas raksturīgs noziedzīgajām organizācijām, kuras bieži vien darbojas pāri robežām un izmanto dažādus paņēmienus, lai slēptu savus aktīvus, tostarp izmanto kriptoaaktīvus.

Koordinēta tiesu iestāžu reakcija

ES līmenī tiek arī veikts darbs, lai nodrošinātu koordinētu tiesu iestāžu reakciju uz Ukrainā, iespējams, izdarītajiem **starptautiskajiem noziegumiem**, lai vainīgos varētu saukt pie atbildības.

Divas dalībvalstis kopā ar Ukrainu izveidoja kopēju izmeklēšanas grupu (KIG), lai izmeklētu kara noziegumus, noziegumus pret cilvēci un citus starptautiskus noziegumus, kas, iespējams, izdarīti Ukrainas teritorijā. *Eurojust* sniedz juridisku, analītisku, finansiālu un loģistikas atbalstu šai KIG. 2022. gada 25. aprīlī par šīs KIG dalībnieci kļuva arī Starptautiskās Krimināltiesas Prokuratūra (*OTP-ICC*)⁴⁶, un paredzams, ka drīz tai pievienosies vēl citi dalībnieki.

2022. gada 25. aprīlī Komisija nāca klajā ar priekšlikumu grozīt *Eurojust* regulu⁴⁷, lai *Eurojust* varētu saglabāt, analizēt un glabāt galveno starptautisko noziegumu pierādījumus. *Eurojust* un Eiropols turpinās cieši sadarboties visu šā procesa laiku. Liela nozīme tiesu iestāžu reaģēšanas koordinēšanā ir arī Genocīda apkarošanas tīklam, kuram *Eurojust* nodrošina sekretariātu; šis tīkls ir sagatavojis to NVO atlantu, kuras pašlaik darbojas Ukrainā, un palīdz praktiķiem no dalībvalstīm un Ukrainas tikt galā ar izskatīšanas procesā esošām lietām, kas saistītas ar karu.

2022. gada aprīlī Padome vēlreiz pārskatīja **ES padomdevējas misijas Ukrainā** pilnvaras, kā rezultātā misija varēs sniegt atbalstu Ukrainas iestādēm Krievijas militārās agresijas kontekstā izdarītu starptautisku noziegumu izmeklēšanā un kriminālvajāšanā par tiem. Misija sniegs Ukrainas iestādēm stratēģiskas konsultācijas par starptautisko noziegumu izmeklēšanu un kriminālvajāšanu par tiem, nepieciešamajiem Ukrainas tiesību aktu grozījumiem un komunikācijas stratēģiju, kā arī nodrošinās apmācību par saistītiem jautājumiem. Misija ir viena no vairākām koordinācijas iniciatīvām, kas tiek īstenotas šajā saistībā, un kopā ar ES delegāciju ietilpst ASV un ES Ukrainas padomdevējā grupā nežēlīgu noziegumu jomā.

VI. ĀRVALSTU MANIPULĀCIJA AR INFORMĀCIJU UN IEJAUKŠANĀS

⁴⁵ Eiropols lēš, ka 2019. gadā tikai 2 % (2,4 miljardi EUR) noziedzīgi iegūto aktīvu bija iesaldēti un 1 % konfiscēti (1,2 miljardi EUR), lai gan noziedzīgās darbībās gūtā peļņa galvenajos noziedzīgajos tirgos ES bija 139 miljardi EUR (1 % no ES IKP).

⁴⁶ <https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine>

⁴⁷ COM(2022) 187 final.

Pašreizējie ģeopolitiskie notikumi ir izgaismojuši ārvalstu iejaukšanās risku. Krievijas militārā agresija pret Ukrainu ir gājusi roku rokā ar informācijas **manipulēšanas un iejaukšanās** darbībām. Lai attaisnotu brutālos uzbrukumus Ukrainai, Ukrainas valdība ir nepatiesi apsūdzēta “nacismā” un “genocīdā”, ir veiktas operācijas “zem sveša karoga” un izteiktas nepamatotas apsūdzības NATO un Rietumiem, bet Krievijā ir apspiesta vārda brīvība un neatkarīgā žurnālistika. Nepārtraukti pastāv risks, ka Krievija var censties izmantot sagrozītus audiovizuālos materiālus un dezinformāciju, lai ar tiem pamatotu militārus papildu uzbrukumus, vājinātu Ukrainas apņēmīgo pretestību, šķeltu starptautisko sabiedrību tās nostājā pret karu vai sētu šaubas par to, vai Krievija ir pārkāpusi starptautiskās tiesības. Eiropas Savienība Stratēģiskajā kompasā ir apņēmusies stingri reaģēt uz ārvalstu manipulāciju ar informāciju un iejaukšanos un palielināt savu noturību un spējas vērsties pret šādiem draudiem⁴⁸. Manipulācija ar demokrātiskajām diskusijām Eiropas Savienībā ir galvenais temats Eiropas Demokrātijas rīcības plānā — Komisijas koordinētajā plānā, kura mērķis ir novērst dezinformāciju un stiprināt demokrātijas noturību⁴⁹.

Modrība un koordinācija

Eiropas Savienība izlēmīgi un koordinēti reaģēja uz Krievijas dezinformācijas kampaņu, kas bija saistīta ar militāro agresiju pret Ukrainu. ES ir cieši sadarbojusies ar savām dalībvalstīm, izmantojot Ātrās brīdināšanas sistēmu, un ar starptautiskajiem partneriem, piemēram, NATO, ASV, Kanādu un G7 Ātrās reaģēšanas mehānismu, lai dalītos informācijā par manipulācijas tendencēm un taktiku, ko izmanto Krievija. Krievijas manipulāciju atmakošanas darbs ir pastiprinājies, un šim nolūkam jo īpaši tiek izmantota tīmekļa vietne *EUvsDisinfo*, kurā angļu, krievu, ukraiņu un citās valodās tiek sniegti fakti ES, Ukrainā un tās reģionā, kā arī Krievijā. ES pieņemto ierobežojošos pasākumu dēļ kopš 2. marta ir apturēta Krievijas valsts plašsaziņas līdzekļu *RT* un *Sputnik* kanālu pārraide un apraide Eiropas Savienībā un uz to. Tiešsaistes platformas, lielākie sociālie tīkli, reklāmas devēji un reklāmas nozares pārstāvji, kas parakstījuši Prakses kodeksu dezinformācijas jomā⁵⁰, steidzami rīkojas, lai ierobežotu dezinformāciju, kas saistīta ar Krievijas agresiju pret Ukrainu. Komisija un EĀDD uzrauga šos centienus. Sniegtā informācija liecina, ka platformas ir uzlabojušas savus uzraudzības un intervences instrumentus attiecībā uz šo karu.

Papildus tam tiek strauji izvērstas darbības, kuru mērķis ir atbalstīt Centrālāzijas un Rietumbalkānu valstis, lai uzlabotu informācijas noturību un apkarotu ārvalstu manipulāciju ar informāciju un dezinformāciju.

Gatavība

Ārvalstu manipulēšanas ar informāciju un iejaukšanās (ĀMII), arī dezinformācijas, neslēpta izmantošana par vienu no hibrīddraudu instrumentiem ir radījusi īpaši lielu nepieciešamību ātri pildīt Eiropas Demokrātijas rīcības plānu. Pēdējos mēnešos ES iestādes ir palīdzējušas dalībvalstīm apkarot ĀMII, īpaši Ātrās brīdināšanas sistēmas ietvaros, daloties informācijā par taktiku, ko izmanto ĀMII veicēji, un par reaģēšanas stratēģijām. Turpinās diskusijas par ES kopējās reakcijas uz ĀMII papildu pastiprināšanu, pamatojoties uz EĀDD iesniegto koncepcijas dokumentu par īpašas **rīkkopas** izstrādi šo draudu apkarošanai. Tā apvienotu pastāvošos iekšējos pasākumus ar jauniem ES instrumentiem, kas izstrādāti kopējās ārlietu un

⁴⁸ <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/lv/pdf>.

⁴⁹ COM(2020) 790.

⁵⁰ <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.

drošības politikas ietvaros. To veicinās arī pastiprināta Eiropas Ārējās darbības dienesta nodaļas *Stratcom*⁵¹ un Komisijas rīcība.

Eiropas Digitālo mediju observatorija (*EDMO*) pēc kara sākuma Ukrainā izveidoja darba grupu dezinformācijas jomā un koordinē tās tīklā iesaistīto faktu pārbaudītāju un pētnieku darbības. Tā ir analizējusi, kā Covid-19 sazvērestības teoriju piekritēji ir ātri pārgājuši uz maldinošas, Krieviju atbalstošas informācijas izplatīšanu; šāda pārmaiņa ir novērojama vairākās dalībvalstīs⁵².

Digitālo pakalpojumu akta priekšlikuma mērķis ir pielāgoties strauji mainīgajām digitālajām tehnoloģijām un problēmām, ko šāda strauja attīstība rada tehnoloģiju un demokrātijas jomā, ieskaitot naida runu, dezinformāciju internetā un destabilizācijas stratēģijas. Pateicoties Eiropas Parlamenta un Padomes sarunās panāktajam lielajam progresam, šo tiesību aktu kopumu vajadzētu varēt drīz pieņemt.

VII. GATAVĪBA PLAŠĀKĀ NOZĪMĒ

Laikā, kad Eiropā ir atgriezies karš, kā arī notiek lielas ģeopolitiskas pārmaiņas, drošības koordinācija ES ir pastiprinājusies, balstoties uz iniciatīvām, kas bija ieplānotas jau pirms Krievijas agresīvā kara pret Ukrainu. Iniciatīvas, kas vērstas galvenokārt uz ES ārējo drošību, spēcīgi ietekmē drošības savienības iekšējo programmu.

2022. gada 15. februārī Komisija nāca klajā ar **Aizsardzības tiesību aktu kopumu**⁵³, kurā ir ietvertas vairākas iniciatīvas jomās, kas ir kritiski svarīgas aizsardzībai un drošībai Eiropas Savienībā. Šis Komisijas ieguldījums Eiropas aizsardzībā un drošībā aptver visu problēmu loku. Tajā ir ierosinātas konkrētas darbības, kas palīdzēs radīt vairāk integrētu un konkurētspējīgāku Eiropas aizsardzības tirgu, jo īpaši tāpēc, ka uzlabos sadarbību ES un panāks apjomradītus ietaupījumus. Tajā ir arī paredzēts drošībai un aizsardzībai kritiski svarīgo tehnoloģiju ceļvedis, kā mērķis ir veicināt pētniecību, tehnoloģiju izstrādi un inovāciju šajās nozarēs un samazināt atkarību kritisko tehnoloģiju jomā un vērtības ķēdēs. Tiesību aktu kopuma mērķis ir arī pastiprināt kosmosa aizsardzību ES līmenī. Papildus tam tajā ir arī aplūkots, kā Komisija varētu pastiprināt savu rīcību pret hibrīddraudiem, arī kibernetikas jomā, uzlabot militāro mobilitāti Eiropā un ārpus tās un turpināt risināt klimata pārmaiņu radītās problēmas, kas saistītas ar aizsardzību. Papildinot šo darbu, 18. maija kopīgajā paziņojumā **par aizsardzības investīciju nepietiekamības analīzi un turpmāko virzību**⁵⁴ ir aplūkotas spēju un rūpniecības nepilnības, kas jānovērš, lai atbalstītu visvairāk apdraudētās ES dalībvalstis, un noteikti pasākumi, ar ko mazināt atklātos trūkumus.

Lai ES būtu noturīga pret šiem draudiem, ir arī jāizmanto uz spējām balstītas pieejas visos drošības sektoros, kā to mudināts darīt Komisijas Rīcības plānā par sinerģijām starp civilo,

⁵¹ Eiropas Ārējās darbības dienesta Stratēģiskās komunikācijas, darba grupu un informācijas analīzes nodaļa sniedz ar stratēģisko komunikāciju saistītu atbalstu ES ārlietu un drošības politikas īstenošanā attiecīgajos prioritārajos reģionos (dienvidu un austrumu kaimiņreģionā, Rietumbalkānos), izstrādājot un īstenojot īpašus stratēģiskās komunikācijas pasākumus, kas vērsti uz ES politikas, vērtību, mērķu un interešu veicināšanu.

⁵² <https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/>

⁵³ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en.

⁵⁴ JOIN(2022) 24.

aizsardzības un kosmosa rūpniecību⁵⁵. Tiek veikts darbs, lai veicinātu uz spējām balstītas pieejas iekšējās drošības un tiesībaizsardzības jomā.

2022. gada 21. martā Padome pieņēma **Stratēģisko kompasu drošībai un aizsardzībai**⁵⁶, ko neilgi pēc tam apstiprināja Eiropadome. Kompasā ir izklāstīts vērienīgs rīcības plāns, kā līdz 2030. gadam nostiprināt ES drošības un aizsardzības politiku. Mērķis ir padarīt ES par spēcīgāku un spējīgāku drošības devēju, kas aizsargā savus iedzīvotājus un veicina mieru un drošību pasaulē. Tas satur konkrētus priekšlikumus, kā uzlabot ES spēju krīzēs rīkoties izlēmīgi, un ļoti precīzu to īstenošanas grafiku.

Kā viens no Stratēģiskā kompasa nodevumiem ir jāizstrādā **ES hibrīddraudu novēršanas rīkkopa**, kas satur gan iekšējus, gan ārējus pasākumus un kam būtu jānodrošina satvars koordinētai reaģēšanai uz hibrīdkampaņām, kuras ietekmē ES un tās dalībvalstis. 2022. gada sākumā tika noteikti nozaru noturības atsaucēs līmeņi⁵⁷, un tagad jāpabeidz nepilnību un vajadzību analīze. ES saskaņā ar šo satvaru turpinās stiprināt gatavību draudiem, ko rada Krievijas agresija un jebkādi citi mēģinājumi destabilizēt demokrātiju un uz noteikumiem balstītu daudzpusēju kārtību, un noturību pret šādiem draudiem un reaģēšanu uz tiem.

VIII. SKATS NĀKOTNĒ

Nākotnē ES būs jāturpina īpaši modri vērot draudu attīstību un jāstiprina **gatavība visiem iespējamajiem gadījumiem un noturība pret tiem**. Kara negatīvās sekas var izpausties dažādos veidos, un ne visus no tiem jau ir iespējams novērtēt.

Vēl nav zināms, cik liela daļa no Ukrainas noziedzīgajiem tīkliem ir pārceļta uz citām vietām. *Eurojust* agrākais lietu izskatīšanas darbs liecina, ka pastāv tendence no Afganistānas caur Ukrainu uz ES nelegāli pārdot heroīnu, un šo tendenci apstiprina arī Eiropas Narkotiku un narkomānijas uzraudzības centrs (*EMCDDA*)⁵⁸. Nestabilitāte var apgrūtināt vēšanos pret heroīna tirdzniecību šajā maršrutā, kā rezultātā var palielināties narkotiku plūsma uz ES.

Daži riski Eiropas Savienībai drīzāk palielināsies pēc kauju beigām vai kauju pārtraukumos, ja tādi būs. Īpaša uzmanība tiks pievērsta šaujamo ierociņu aprītei, kuras risks palielināsies, kad kaujas Ukrainā aprims. Pieredze arī liecina par risku, ka pēc tam, kad būs atgriezušies ārvalstu kaujinieki, kas būs guvuši pieredzi kaujas laukā un, iespējams, būs saskārušies ar ekstrēmistu grupām, ES var piedzīvot teroristiskas darbības. Šī iespējamā parādība būtu cieši jāuzrauga, un Komisija jau veicina dalībvalstu diskusijas par problēmām, ko rada tādu ārvalstu brīvprātīgo atgriešanās, kuri pagātnē bijuši iesaistīti vardarbīgā ekstrēmismā.

Nemot vērā šos iespējamus draudus, ir svarīgi, lai turpinātos Drošības savienības stratēģijas īstenošana, tostarp tiktu īstenotas svarīgākās stratēģijas, tādas kā ES kiberdrošības stratēģija,

⁵⁵ COM(2021) 70.

⁵⁶ Stratēģiskais kompass drošībai un aizsardzībai — Eiropas Savienībai, kas aizsargā savus pilsoņus, vērtības un intereses un veicina starptautisko mieru un drošību: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/lv/pdf>.

⁵⁷ SWD(2022) 21 final.

⁵⁸ *Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data)*, EMCDDA, *Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery*, 2021/00446, Eurojust, 2020. gada maijs.

Organizētās noziedzības novēršanas stratēģija (2021.–2025. gadam), ES Terorisma apkarošanas programma (2020.–2025. gadam), ES rīcības plāns attiecībā uz šaujamo nelikumīgu tirdzniecību (2020.–2025. gadam), ES stratēģija cilvēku tirdzniecības apkarošanai (2021.–2025. gadam) un ES stratēģija narkotiku jomā (2021.–2025. gadam).

Turpināsies centieni nodrošināt Eiropas Savienībai nepieciešamo tiesisko regulējumu. Piemēram, Komisija gatavo ietekmes novērtējumu par priekšlikumu, ar ko reglamentē liela riska ķīmikāliju tirdzniecību un izmantošanu.

IX. SECINĀJUMS

Drošības savienība turpina ieņemt nozīmīgu vietu ES un tās dalībvalstu sagatavošanā pastāvošo un iespējamo draudu apkarošanai. Krievijas agresīvais karš pret Ukrainu ir parādījis, cik ātri teorētiski draudi var kļūt par realitāti, un ļauj skaidri ieraudzīt, cik liela nozīme ir modrībai, koordinēšanai un gatavībai.

Šis ceturtais progresa ziņojums par Drošības savienības stratēģiju parāda, ka ES spēj pielāgoties, pat tad, ja tai nākas saskarties ar ārkārtīgiem un negaidītiem draudiem, piemēram, tiem, ko rada Krievijas agresīvais karš pret Ukrainu. Apņēmīgi īstenot Drošības savienības stratēģiju pašlaik ir tik svarīgi kā nekad iepriekš.