



Svet
Evropske unije

Bruselj, 27. maj 2022
(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	

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	25. maj 2022
Prejemnik:	Generalni sekretariat Sveta

Št. dok. Kom.:	COM(2022) 252 final
Zadeva:	SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU Četrto poročilo o napredku pri izvajanju strategije EU za varnostno unijo

Delegacije prejmejo priloženi dokument COM(2022) 252 final.

Priloga: COM(2022) 252 final



Bruselj, 25.5.2022
COM(2022) 252 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

Četrto poročilo o napredku pri izvajanju strategije EU za varnostno unijo

I. UVOD

Na varnostnem dnevnem redu EU je trenutno v središču ruska vojna agresija proti Ukrajini. Ta vojna ne ogroža le Ukrajine, temveč škoduje svetovni stabilnosti in varnosti. V EU prinaša številna tveganja za varnost državljanov in državljanek. Pojavljajo se nove negotovosti glede oskrbe z energijo in drugimi surovinami, kritična infrastruktura pa je lahko tarča kibernetičnih napadov. Notranjo varnost in zaščito EU ogrožajo morebitni napadi ali nesreče, ki so posledica uporabe kemičnih, bioloških ali radioloških agensov na vojnem območju. Organizirane kriminalne združbe lahko s tihotapljenjem žensk in otrok, ki so še posebej ogroženi, hitro izkoristijo ranljivost milijonov ljudi, ki so zbežali pred vojno.

EU je ob teh novih in morebitnih grožnjah ostala odločna in enotna. Čeprav je bil vpliv vojne doslej večinoma omejen na ozemlje Ukrajine, je EU okrepila *pozornost in usklajevanje* z intenzivnejšim spremljanjem groženj ter si je prizadevala za krepitev odpornosti, da bi zagotovila *pripravljenost*.

Evropski voditelji in voditeljice so v Izjavi iz Versaillesa z dne 10. in 11. marca 2022¹ poudarili, da se je treba pripraviti na hitro nastajajoče izzive, vključno „z zaščito pred vse pogostejšim hibridnim vojskovanjem, krepitvijo naše kibernetične odpornosti, zaščito naše infrastrukture, zlasti kritične infrastrukture, in bojem proti dezinformacijam“.

Okvir varnostne unije ima osrednjo vlogo pri zagotavljanju varnosti po vsej EU. V strategiji EU za varnostno unijo² so opredeljene štiri strateške prednostne naloge, ki ostajajo neposredno povezane s to nalogo v sedanjem geopolitičnem okviru: (i) varnostno okolje, primerno za prihodnost, (ii) obravnavanje spreminjajočih se groženj, (iii) zaščita Evropejcev in Evropejk pred terorizmom in organiziranim kriminalom ter (iv) trden evropski varnostni ekosistem. Vojna je ponovno pokazala, da morajo EU in njene države članice v celoti izkoristiti zakonodajne instrumente in instrumente politike, ki so že na voljo v okviru strategije EU za varnostno unijo in so podlaga za usklajeno podporo EU državam članicam v zvezi z vprašanji, ki segajo vse od organiziranega kriminala in terorizma do kibernetične varnosti in hibridnih groženj.

Svoja prizadevanja so v odziv na vojno v Ukrajini povečale tudi evropske agencije s področja pravosodja in notranjih zadev, ki imajo ključno vlogo pri ocenjevanju groženj in podpiranju operativnih odzivov³. Še en pomemben dejavnik je stalna krepitev operativne prakse in upravljanja schengenskega območja.

To četrto poročilo o napredku pri varnostni uniji se osredotoča na razvoj dogodkov v zadnjih nekaj mesecih od ruske vojne agresije proti Ukrajini. Vsebuje pregled ukrepov, sprejetih na vseh področjih varnostne unije, in proučitev potreb po pripravljenosti, ki izhajajo iz morebitnih varnostnih groženj zaradi vojne v Ukrajini. Napredek v zvezi z drugimi dokumenti s področja varnostne unije je naveden v prilogi.

¹ <https://www.consilium.europa.eu/media/54783/20220311-versailles-declaration-sl.pdf>

² COM(2020) 605.

³ [Skupna izjava agencij EU s področja pravosodja in notranjih zadev o Ukrajini | Agencija Evropske unije za azil \(europa.eu\)](#).

II. KIBERNETSKA VARNOST IN KRITIČNA INFRASTRUKTRUA

Zasebni akterji in storilci kriminalnih dejavnosti od izbruha vojne naznanjajo, da s kibernetскими dejavnostmi podpirajo eno ali drugo stran. Hekerski aktivizem⁴ pomeni grožnjo zaradi tveganja učinka prelivanja na kritične storitve EU, tveganja napadov, ki prihajajo iz uradnih mrež, ali drugih nepredvidenih učinkov prelivanja. Čeprav se v vojni doslej večinoma bojujejo s konvencionalnimi sredstvi, ki imajo le omejene učinke prelivanja, obstaja na tem območju resnično tveganje zaostrovanja.

EU je zato okrepila usklajevanje in pripravljenost. Zaradi groženj, ki so posledica vojne, je treba vzpostaviti kulturo izmenjave informacij ter strokovnega znanja in izkušenj med EU, državami članicami in skupnostmi za kibernetško varnost. To zajema oblikovanje skupnega celovitega situacijskega zavedanja institucij, organov in agencij EU ter držav članic, zlasti v zvezi s kritično infrastrukturo, od katere je odvisno nemoteno delovanje notranjega trga.

Pripisovanje odgovornosti za kibernetške napade na Ukrajino

Kibernetški napadi na Ukrajino so se začeli že pred rusko agresijo in se nadaljevali v prvih dneh vojne⁵, njihov namen pa je bil kompromitirati uporabniške račune ukrajinskega vojaškega osebja ter povzročiti motnje v bistvenih storitvah, tudi nadzoru meje in telekomunikacijah.

Visoki predstavnik je 14. januarja 2022 v imenu Evropske unije podal izjavo⁶, v kateri je obsodil kibernetške napade na Ukrajino in vnovič potrdil odločno podporo EU Ukrajini.

Evropska unija in njene države članice so 10. maja skupaj z mednarodnimi partnerji odločno obsodile⁷ zlonamerno kibernetško dejavnost proti Ukrajini z dne 24. februarja, ki je bila uperjena proti satelitskemu omrežju KA-SAT, ki ga upravlja Viasat, in so napad neposredno pripisale Ruski federaciji. Ta kibernetški napad je imel znatne posledice in je povzročil vsesplošne izpade in motnje komunikacij, kar je občutilo več javnih organov, podjetij in uporabnikov v Ukrajini, prizadetih pa je bilo tudi več držav članic EU.

Pozornost in usklajevanje

Od začetka ruske vojne agresije proti Ukrajini se je okrepilo spremljanje stanja na področju kibernetške varnosti v državah članicah in institucijah EU. Agencija Evropske unije za kibernetško varnost (ENISA), Evropski center za boj proti kibernetški kriminaliteti pri

⁴ Nedavni primer hekerskega aktivizma je uporaba „protestne programske opreme,“ s katero se je na ruske IP-naslove prek priljubljenega odprtokodnega paketa širila zlonamerna programska oprema, kar bi lahko povzročilo tveganja v dobavni verigi in izgubo zaupanja v odprtokodno skupnost. Komisija je jasno poudarila, da so (celo dobronamerni) kibernetški napadi na Rusijo nezakoniti.

⁵ Posebno poročilo Microsofta: [An overview of Russia's cyberattack activity in Ukraine](#) (Pregled ruskih dejavnosti kibernetških napadov v Ukrajini); [The hybrid war in Ukraine – Microsoft On the Issues](#) (Hibridna vojna v Ukrajini – Microsoftova obravnava vprašanj).

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

⁷ [Ruske kibernetške operacije proti Ukrajini: izjava visokega predstavnika v imenu Evropske unije – Consilium \(europa.eu\).](#)

Europolu, skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU) ter Obveščevalni in situacijski center EU (EU INTCEN) so prispevali k skupnemu situacijskemu zavedanju EU, pri čemer so redno spremljali sumljive kibernetске dejavnosti, tudi v specifičnih sektorjih, kot so energetika, promet in letalstvo, ter pripravljali ocene za usmerjanje preventivnih ukrepov.

Potekala sta tudi okrepljeno usklajevanje in izmenjava informacij z mrežami za kibernetско varnost, kot je organizacijska mreža za povezovanje v kibernetски krizi (CyCLONe), v katero so vključene nacionalne agencije za kibernetско varnost, Komisija in ENISA. Da bi se ta pristop interno odražal v institucijah EU, usklajevalni mehanizem, imenovan projektna skupina za kibernetске krize, omogoča izmenjavo informacij med vsemi zadevnimi službami, organi in agencijami, vključno z agencijo ENISA, Evropskim centrom za boj proti kibernetски kriminaliteti pri Europolu in skupino CERT-EU. Potrebna so stalna prizadevanja za zagotovitev komunikacijskih kanalov med politično, operativno in tehnično ravno ter spodbujanje sodelovanja z mrežo skupin za odzivanje na incidente na področju računalniške varnosti.

Europol je prav tako sprožil protokol EU za odzivanje organov kazenskega pregona na izredne razmere, ki omogoča okrepljeno spremljanje kibernetских groženj in izmenjavo informacij med številnimi deležniki, da bi se oblikovala celovita slika obveščevalnih podatkov o kibernetских grožnjah.

Države članice, Evropska služba za zunanje delovanje (ESZD) in službe Komisije poleg ukrepanja proti kibernetским grožnjam bolj pozorno spremljajo izpostavljenost kritične infrastrukture nekibernetским, fizičnim grožnjam. Kritična infrastruktura in subjekti, ki jo upravljajo, so lahko izpostavljeni fizičnim tveganjem, kot so sabotaze, ki jih kot del morebitnih povračilnih ukrepov proti EU lahko izvajajo države ali akterji, ki jih podpirajo države.

Pripravljenost

Ob upoštevanju večje izpostavljenosti Evrope kopičenju groženj zaradi vojne je pripravljenost na področju kibernetске varnosti in varnosti kritične infrastrukture pomembnejša kot kdaj koli prej. Prizadevanja za povečanje pripravljenosti vključujejo številne neposredne ukrepe, med katerimi so bili nekateri predvideni že pred rusko agresijo proti Ukrajini. Ti vključujejo vaje, smernice, zakonodajne ukrepe, povečanje odpornosti v kritičnih sektorjih in sodelovanje s partnerji.

Francosko predsedstvo Sveta Evropske unije je skupaj z ESZD in ENISA v začetku leta 2022 organiziralo vajo na podlagi scenarijev, imenovano EU CyCLES (Cyber Crisis Linking Exercise on Solidarity – povezovalna vaja o solidarnosti na področju kibernetске varnosti), da bi se povečala ozaveščenost na politični ravni ter okrepilo sodelovanje med operativno in politično ravno v primeru kibernetских napadov velikih razsežnosti.

ENISA in CERT-EU sta februarja objavili **smernice** o tem, kako povečati odpornost in pripravljenost v EU⁸. Te smernice vse organizacije javnega in zasebnega sektorja v EU

⁸ Boosting your Organisation's Cyber Resilience - Joint Publication (Povečanje kibernetске odpornosti vaše organizacije – skupna publikacija) z dne 14. februarja 2022.

spodbujajo, naj sprejmejo minimalni sklop najboljših praks na področju kibernetike varnosti, da bi se znatno izboljšala kultura kibernetike varnosti. CERT-EU je s podporo agencije ENISA⁹ marca objavila nadaljnje tehnične smernice ter varnostne smernice za utrjevanje varnosti konfiguracije aplikacije Signal¹⁰ ter pri tem navedla številna praktična priporočila organizacijam za boljši položaj glede tveganja na področju kibernetike varnosti.

Zakonodajne pobude

V sedanjih razmerah je razvidna nujnost **izvajanja veljavne zakonodaje** in pospešitve **sprejetja še nesprejetih pobud**.

Komisija podpira države članice pri izvajanju **direktive o varnosti omrežij in informacij**¹¹, ki od držav članic zahteva, da imajo ustrezne zmogljivosti, na primer skupino za odzivanje na incidente na področju računalniške varnosti (CSIRT), in da določijo pristojne organe. Direktiva zagotavlja podlago za učinkovito sodelovanje med državami članicami. Politični dogovor, ki sta ga dosegla sozakonodajalca glede **revidirane direktive o varnosti omrežij in informacij**¹², je nadaljnji preboj pri zagotavljanju trdnega okvira pripravljenosti EU.

Revidirana direktiva o varnosti omrežij in informacij – nadaljnje povečanje pripravljenosti

- Nova direktiva o varnosti omrežij in informacij bo odpravila pomanjkljivosti prejšnje direktive o varnosti omrežij in informacij, da bi jo prilagodila trenutnim potrebam in zagotovila njeno primernost za prihodnost. Nova direktiva določa minimalna pravila za regulativni okvir in mehanizme za učinkovito sodelovanje med ustreznimi organi v posameznih državah članicah.
- Direktiva razširja področje uporabe pravil, tako da dodaja nove sektorje, ki so ključni za gospodarstvo in družbo (na primer sektorja farmacije in medicinskih pripomočkov ali sektor proizvodnje živil). Na področje uporabe direktive bodo spadala vsa srednja in velika podjetja, ki delujejo v zadevnih sektorjih ali zagotavljajo storitve, zajete v direktivi. Zajema tudi subjekte javne uprave enot centralne ravni držav (razen sodstva, parlamentov in centralnih bank) in tiste na regionalni ravni. Poleg tega se lahko države članice odločijo, da se uporablja za take subjekte na lokalni ravni.
- Revidirana direktiva bo določila izhodiščni okvir za ukrepe obvladovanja tveganj za kibernetiko varnost in uradno ustanovila Evropsko organizacijsko mrežo za povezovanje v kibernetiki krizi (EU-CyCLONe), ki bo podprla usklajeno upravljanje velikih kibernetičnih incidentov.
- Predlog tudi uvaja natančnejše določbe v zvezi s postopkom poročanja o incidentih, vsebino poročil in časovnicami ter določa pravna sredstva in sankcije za zagotovitev izvrševanja.
- Države članice bodo morale določbe direktive prenesti v nacionalno zakonodajo v

⁹ Security Guidance 2022-01 - Cybersecurity mitigation measures against critical threats (Varnostne smernice 2022-01 – ukrepi za zmanjšanje tveganja kritičnih groženj na področju kibernetike varnosti).

¹⁰ CERT-EU Security Guidance 22-002 - Hardening Signal (Varnostne smernice CERT-EU 22-002 – utrjevanje varnosti aplikacije Signal).

¹¹ Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

¹² COM(2020) 823.

21 mesecih po začetku njene veljavnosti.

Napredku v zvezi z revidirano direktivo o varnosti omrežij in informacij bi moral čim prej slediti zaključek pogajanj o predlogu **direktive o odpornosti kritičnih subjektov**¹³, ki naj bi po njenem sprejetju in začetku izvajanja povečala odpornost kritičnih subjektov proti številnim grožnjam, tudi terorističnim napadom, notranjim grožnjam ali sabotажam. Prav tako je bistveno, da sta ravni ambicij direktive o odpornosti kritičnih subjektov in predloga Komisije usklajeni ter da se ohrani doslednost s političnim kompromisom, doseženim o revidirani direktivi o varnosti omrežij in informacij. Ti ukrepi bodo skupaj povečali odpornost in pripravljenost z vzpostavitvijo skladnejšega in zanesljivejšega sistema, vključno z nacionalnimi načrti odzivanja na incidente in krize. Ti so bili vključeni tudi v lanskoletno priporočilo Komisije¹⁴ o vzpostavitvi **skupne kibernetске enote**, ki določa, kako bi morali različni akterji ekosistema kibernetске varnosti (diplomacija, policijski organi, civilna skupnost in po potrebi obrambni organi) sodelovati na operativni ravni. Trenutne grožnje razkrivajo pomen takega učinkovitega sodelovanja med ključnimi akterji.

Komisija še naprej spremlja izvajanje sklopa orodij EU za kibernetско varnost omrežij **5G**¹⁵. V tem okviru je Skupina za sodelovanje na področju varnosti omrežij in informacij 11. maja sprejela poročilo o varnosti arhitekture OpenRAN¹⁶. Z državami članicami prav tako še naprej sodeluje pri zagotavljanju popolnega delovanja evropskega kompetenčnega centra za kibernetско varnost.

Komisija je 22. marca 2022 predlagala **nova pravila za vzpostavitev skupnih ukrepov za kibernetско in informacijsko varnost v institucijah, organih in agencijah EU**. S temi pravili se bosta okrepili odpornost uprave EU ter njena sposobnost za odzivanje na kibernetске grožnje in incidente. Z umestitvijo teh dejavnosti v skupni okvir se bo okrepilo medinstitucionalno sodelovanje in zmanjšala izpostavljenost tveganju. Predlagana **uredba o kibernetски varnosti za institucije, organe in agencije EU**¹⁷ bo povečala pooblastila CERT-EU ter omogočila vzpostavitev Medinstitucionalnega odbora za kibernetско varnost, krepila zmogljivosti na področju kibernetске varnosti ter spodbujala redne ocene zrelosti in boljšo kibernetско higieno. Predlagana **uredba o informacijski varnosti**¹⁸ bo vzpostavila minimalni sklop pravil in standardov informacijske varnosti za varno izmenjavo informacij in ravnanje z njimi za vse institucije, organe, urade in agencije EU, da se zagotovi okrepljena in dosledna zaščita njihovih informacij pred spreminjajočimi se grožnjami. Komisija poziva Evropski parlament in Svet, naj ta predloga hitro sprejmeta.

Komisija je zdaj zaključila javno posvetovanje o ukrepih za povečanje **kibernetске odpornosti** digitalnih proizvodov ter pripravlja predlog, ki bo objavljen letošnje jesen¹⁹.

¹³ COM(2020) 829.

¹⁴ [Recommendation on building a Joint Cyber Unit | Shaping Europe's digital future \(europa.eu\)](#) (Priporočilo o vzpostavitvi skupne kibernetске enote | Oblikovanje digitalne prihodnosti Evrope (europa.eu)).

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

¹⁶ Skupina za sodelovanje na področju varnosti omrežij in informacij, Report on the cybersecurity of OpenRAN (Poročilo o kibernetски varnosti arhitekture OpenRAN) z dne 11. maja 2022.

¹⁷ COM(2022) 122.

¹⁸ COM(2022) 119.

¹⁹ [Akt o kibernetски odpornosti – nova pravila o kibernetски varnosti za digitalne proizvode in pomožne storitve \(europa.eu\)](#).

Tako se bodo obravnavale ranljivosti digitalnih proizvodov in pomožnih storitev, ki sicer ustvarjajo priložnosti za gospodarstva in družbe EU, vendar prinašajo tudi nove izzive. Čim bolj je vse povezano, tem lažje lahko namreč kibernetiski incident vpliva na celoten sistem ter tako povzroči motnje v gospodarskih in družbenih dejavnostih.

Ministri in ministrice EU, odgovorni za telekomunikacije, so 9. marca 2022 v Neversu soglasno sprejeli poziv za okrepitev zmogljivosti EU na področju kibernetске varnosti, v katerega je bilo zajeto „izvajanje novega sklada za nujno odzivanje na kibernetске grožnje, ki ga vzpostavi Komisija“²⁰. Komisija proučuje najboljše načine uporabe obstoječih sredstev za podpiranje preventivnega ukrepanja in odzivanja.

Kritični sektorji

Za dobrobit državljanov in državljanov ter nemoteno delovanje naših gospodarstev je bistvena zanesljiva oskrba EU z **energijo**, v sedanjih razmerah pa je očitna tudi potreba po jasnih pravilih o kibernetски varnosti v tem sektorju. Komisija pripravlja omrežni kodeks o kibernetски varnosti za čezmejne pretoke električne energije, kot se zahteva v uredbi o električni energiji²¹, da bi zagotovila pravila o ocenah tveganj, skupnih minimalnih zahtevah, načrtovanju, spremljanju, poročanju in kriznem upravljanju. Cilji, zastavljeni za omrežni kodeks o kibernetски varnosti, so od ruske vojne agresije proti Ukrajini postali še pomembnejši. Komisija je prav tako vzpostavila strukturno sodelovanje med agencijo ENISA, mrežama ENTSO-E²² in ENTSO-G²³ ter Energetsko skupnostjo pri rednem spremljanju stanja na področju kibernetске varnosti v energetiki.

EU si prizadeva zaščititi varnost partnerjev brez ustvarjanja novih tveganj zase. Marca 2022 je bila po sprejetju ukrepov za zmanjšanje tveganj, zlasti v smislu kibernetске varnosti, opravljena sinhronizacija v sili omrežij električne energije Ukrajine in Moldavije z omrežjem celinske Evrope.

Vojna in sankcije so prinesle tudi številne izzive za **promet** EU, od varnostnih tveganj za civilno letalstvo EU in voznike tovornjakov, ki so obtičali na konfliktnem območju, do uničenja ukrajinske prometne infrastrukture, kar je prekinilo dobavne verige in ogrozilo svetovno prehransko varnost. Agencija Evropske unije za varnost v letalstvu je v tesnem sodelovanju s Komisijo in Evropsko organizacijo za varnost zračne plovbe (Eurocontrol) letalskim prevoznikom od začetka vojne svetovala, naj ne letijo v zračnem prostoru Ukrajine ter naj se izogibajo uporabi zračnega prostora znotraj 100 navtičnih milj od beloruske in rusko-ukrajinske meje.

Komisija si prav tako prizadeva povečati pripravljenost in odpornost prometnega sektorja EU. Zlasti nov krizni načrt za promet²⁴, sprejet 23. maja, temelji na spoznanjih, pridobljenih

²⁰ [08/03/2022 - Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique - Presse - Ministère des Finances \(economie.gouv.fr\)](#) (Skupna izjava ministrov EU za digitalizacijo in elektronske komunikacije, naslovljena na digitalni sektor – tisk – ministrstvo za finance (economie.gouv.fr)).

²¹ Uredba (EU) 2019/943 Evropskega parlamenta in Sveta z dne 5. junija 2019 o notranjem trgu električne energije (UL L 158, 14.6.2019, str. 54). Predlog trenutno pregleduje Agencija za sodelovanje energetskih regulatorjev (ACER).

²² Evropska mreža operaterjev prenosnih sistemov za električno energijo.

²³ Evropska mreža sistemskih operaterjev prenosnih omrežij zemeljskega plina.

²⁴ COM(2022) 21.

med pandemijo COVID-19 in rusko vojaško agresijo proti Ukrajini. Načrt predlaga nabor desetih ukrepov, ki bodo EU in njene države članice usmerjali pri uvajanju nujnih ukrepov za odzivanje na krizo, vključno z zagotavljanjem minimalne povezljivosti, krepitvijo odpornosti proti kibernetičnim in hibridnim grožnjam ter boljšim sodelovanjem z mednarodnimi partnerji na področju pripravljenosti in odzivanja na krize. Poudarja tudi pomen rednega testiranja odpornosti proti različnim kriznim scenarijem, pri katerem bi se povezale ustrezne agencije EU ali drugi akterji in ki bi nadgrajevalo obstoječe postopke.

V okviru **EU za zdravstveno varnost** je treba pred kibernetičnimi napadi zaščititi izmenjavo informacij na podlagi sistema zgodnjega obveščanja in odzivanja, vključno s podporo pri medicinski evakuaciji iz Ukrajine, zato se trenutno krepi varnost sistema.

Sodelovanje s partnerji

Komisija še naprej sodeluje z mednarodnimi partnerji zaradi preprečevanja in preganjanja zlonamerne ravnanja v kibernetičnem prostoru, odvratanja od njega ter odzivanja nanj. Sodelovanje na tem področju je zaradi ruske vojne agresije proti Ukrajini pomembnejše kot kdaj koli prej. ESZD si je v zvezi s tem prizadevala za izmenjavo situacijskega zavedanja in usklajevanje odzivanja na zlonamerne kibernetične dejavnosti, usmerjene v Ukrajino, ter za podporo Ukrajini in drugim v regiji, tako da v sodelovanju s partnericami, vključno z ZDA in NATO, zagotavlja dopolnjevanje in preprečuje prekrivanja.

Tesno sodelovanje z ZDA se je okrepilo tudi v okviru Sveta za trgovino in tehnologijo med EU in ZDA. V skupni izjavi²⁵, podani po ministrskem srečanju maja v Parizu, se je poudarila osrednja vloga Sveta za trgovino in tehnologijo za prenovljeno čezatlantsko partnerstvo, ki usklajuje skupne ukrepe EU in ZDA v zvezi z rusko agresijo proti Ukrajini. Obe strani sta se strinjali, da je bolj kot kdaj koli prej pomembno tesno sodelovanje, da se poveča odpornost dobavnih verig. Poleg tega je bila vzpostavljena posebna delovna skupina za javno financiranje varne in odporne digitalne infrastrukture v tretjih državah, ki bo omogočila, da bodo EU in ZDA na podlagi sklopa skupnih krovnih načel skupaj javno financirale digitalne projekte v tretjih državah.

S strateškim kompasom, sprejetim marca 2022 (glej oddelek VII), se bo v okviru širše strategije za okrepitev zmožnosti EU za ukrepanje v krizah in zaščito njenih interesov nadalje izboljšala zbirka orodij EU za kibernetično diplomacijo in razvila politika EU za kibernetično obrambo, da bi bili boljše pripravljeni in se boljše odzivali na kibernetične napade.

Podpiranje kibernetične varnosti v Ukrajini in sosednjih državah

EU je kibernetično odpornost Ukrajine podpirala že pred vojno. Med EU in Ukrajino je že junija 2021 potekal prvi dialog o kibernetičnih vprašanjih, EU pa je s programom EU4Digital za Ukrajino v vrednosti 25 milijonov evrov podprla kibernetično varnost in odporno digitalno preobrazbo. Poleg tega je program tesnega medinstitucionalnega sodelovanja v vrednosti 1,5 milijona evrov zasnovan za pomoč ukrajinskim institucijam za kibernetično varnost pri usklajevanju s standardi EU.

EU po izbruhu vojne spodbuja sodelovanje med kibernetičnimi strokovnjaki iz EU in Ukrajine ter usklajuje zagotavljanje tehnične pomoči, opreme, programske opreme in ustreznih storitev, da bi se okrepili kibernetična odpornost in kibernetična obramba Ukrajine.

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

Poleg tega si EU prizadeva oceniti morebitno srednjeročno podporo Moldaviji, Gruziji in Zahodnemu Balkanu. Na podlagi skupne ocenjevalne misije potreb Moldavije po kibernetiski varnosti, izvedene 3. in 4. marca 2022, je bil sprejet poseben ukrep za odzivanje na krizo, da bi se v državi hitro povečala kibernetiska varnost. Podobna podpora za hiter odziv se pripravlja za nekatere države Zahodnega Balkana, ki se zaradi usklajevanja s sankcijami EU štejejo za posebej izpostavljene tveganju. Ocenjuje se tudi morebitna dodatna pomoč Moldaviji prek evropskega mirovnega instrumenta.

III. ORGANIZIRANI KRIMINAL IN TERORIZEM

Zaradi ruske vojne agresije proti Ukrajini so bili milijoni ljudi prisiljeni zapustiti svoje domove, zato se je močno povečalo gibanje prek zunanje meje EU. Do 18. maja je iz Ukrajine in Moldavije v EU prišlo skoraj 6 milijonov ljudi, doslej pa se jih je za začasno zaščito v EU registriralo 2,8 milijona. EU si prizadeva za čim hitrejši in čim prožnejši sprejem tistih, ki bežijo pred vojno, ne da bi ogrozila varnost na svojih zunanjih mejah. Sprejela je ukrepe brez primere, da je osebam, ki bežijo pred vojno, zagotovila začasno zaščito, in se zavezala, da bo vse nove prišleke obravnavala brez diskriminacije. Hkrati pa se ne smejo prezreti morebitna tveganja, ki se lahko pojavijo zaradi tako obsežnega gibanja oseb, zato EU ob močni podpori svojih ustreznih agencij ostaja pozorna na nov razvoj dogodkov na področju organiziranega kriminala in terorizma.

Močno schengensko območje v času povečanih groženj

Zagotavljanje visoke ravni varnosti v **schengenskem** območju in EU še nikoli ni bilo tako pomembno kot v razmerah povečanih groženj zaradi vojne tik za zunanjo mejo EU.

Komisija je za uresničevanje ambiciozne agende za schengensko območje, določene v strategiji iz junija 2021, maja letos sprejela prvo poročilo o stanju schengenske ureditve²⁶. Letni schengenski cikel zagotavlja nov model upravljanja schengenskega območja z rednim pregledom stanja schengenske ureditve. Tako se bodo lahko hitro opredelile pomanjkljivosti in učinkovit postopek nadaljnjega ukrepanja za okrepitev in večjo odpornost schengenskega območja.

V navedenem prvem poročilu je priznana potreba po večjih prizadevanjih za izvajanje ključnih pobud na ravni EU, vključno s sistematičnimi kontrolami vseh potnikov na zunanjih mejah ob polni uporabi pooblastil agencij Frontex in Europol ter predlaganih in razpoložljivih orodij za čezmejno policijsko sodelovanje.

Temelj prizadevanj za izboljšanje notranje varnosti in upravljanja meja sta zlasti nova arhitektura informacijskih sistemov EU za meje, migracije in varnost ter njihova interoperabilnost. Učinkovito izvajanje vseh elementov okvira interoperabilnosti v skladu z dogovorjenim časovnim razporedom bo pri tem odločilnega pomena.

²⁶ COM(2022) 301.

Pozornost in usklajevanje

Za ozaveščenost o novih grožnjah kriminala in terorističnih grožnjah je ključno tesnejše sodelovanje med državami članicami in s tretjimi državami na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter ukrepanje v zvezi s kriminalnimi mrežami in posamezniki, ki bi lahko poskušali izkoristiti vojno v Ukrajini. Države članice in operativni partnerji si z Europolom dejavno izmenjujejo ustrezne informacije in kriminalistične obveščevalne podatke, ki so na voljo, Europol pa informacije navzkrižno preverja, analizira in preoblikuje v uporabna operativna obveščevalna obvestila, kot so sporočila za zgodnje opozarjanje in ocene ogroženosti, ki jih deli s partnerji.

Organizirani kriminal

Organizirane kriminalne združbe že iščejo načine za izkoriščanje sedanjih razmer. V prvotni analizi obveščevalnih podatkov so se odkrili vzorci kaznivih dejanj na številnih področjih, vključno s trgovino z ljudmi, lažnimi deklaracijami blaga, ki se uvaža ali izvažata, spletnimi goljufijami, kibernetško kriminaliteto in nedovoljenim prometom z orožjem. Obstajajo tudi dokazi o storilcih kaznivih dejanj kibernetške kriminalitete, ki se izdajajo za zbiralce sredstev za Ukrajino ter kradejo denar in kriptovalute²⁷. Kriminalne organizacije iz Ukrajine se lahko poskušajo zaradi trenutnih razmer preseliti in nadaljevati svoje dejavnosti v EU.

Komisija in francosko predsedstvo Sveta sta sodelovala z agencijami EU s področja pravosodja in notranjih zadev, zlasti z Europolom, da bi mobilizirala Evropsko večdisciplinarno platformo proti grožnjam kriminala (**EMPACT**) za oceno, predvidevanje in preprečitev obstoječih ali novih groženj hudih kaznivih dejanj in organiziranega kriminala ter boj proti njim. Europol je 7. aprila 2022 gostil srečanje platforme EMPACT, na katerem so se zbrali predstavniki in strokovnjaki iz držav članic EU in evropske varnostne skupnosti, da bi obravnavali grožnje hudih kaznivih dejanj in organiziranega kriminala, ki so se pojavile zaradi vojne v Ukrajini. Konkretni ukrepi, o katerih so razpravljali, so zajemali zbiranje več obveščevalnih podatkov, izvajanje nujnih operativnih ukrepov in preusmeritev obstoječih ukrepov ter *ad hoc* dneve skupnega ukrepanja.

CELBET (skupina strokovnjakov za carino na vzhodni in jugovzhodni kopenski meji) – projekt sodelovanja, ki ga financira Evropska komisija, v okviru svoje naloge zagotavljanja operativne podpore in smernic carinskim uradnikom spremlja razvoj dogodkov na meji ter nadzoruje carinske zasege na mejnih prehodih na meji med EU (Poljsko, Slovaško, Madžarsko in Romunijo) in Ukrajino.

Kriminalna in teroristična dejavnost

V EU še ni neposredne teroristične grožnje, povezane z rusko invazijo na Ukrajino. Kljub temu je jasno, da moramo ostati pozorni.

²⁷ Googlova skupina za analizo groženj je opazila vse večje število akterjev groženj, ki vojno v Ukrajini uporabljajo kot vabo v kampanjah ribarjenja in zlonamerne programske opreme. Raziskovalci podjetja za varnost interneta, imenovanega Cyren, poročajo o povečanju števila prevar v zvezi s kriptosredstvi, ki izkoriščajo konflikt z uporabo lažnih donatorskih spletišč.

Zaradi povečanih tveganj za kriminalno in teroristično dejavnost je razvidno, kako pomembno je, da države članice uporabljajo ustrezne podatkovne zbirke EU, kot je Schengenski informacijski sistem, za vnašanje podatkov, ko je to potrebno, in opravljanje poizvedb v njih ob kontrolah oseb, ki vstopajo v EU. To bo prispevalo k prepoznavanju posameznikov, ki ogrožajo notranjo varnost EU, na zunanjih mejah. Agencija Evropske unije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (EU-LISA) še naprej zagotavlja popolno razpoložljivost in učinkovitost sistemov upravljanja meja EU. V smernicah²⁸ državam članicam je bilo pojasnjeno, kako uravnotežiti potrebo po zagotavljanju nemotene obravnave prišlekov na zunanjih mejah in hkrati še vedno izvajati potrebne varnostne kontrole.

Pripravljenost

Pripravljenost EU je bila poleg smernic in usklajevanja okrepljena z napotitvijo osebja agencij EU.

Europol je napotil operativne skupine v države članice EU, ki mejijo na Ukrajino. Te skupine sestavljajo gostujoči uradniki Europola iz držav članic ter strokovnjaki Europola na Madžarskem, v Litvi, na Poljskem, v Romuniji in na Slovaškem, pa tudi v Moldaviji²⁹. Gostujoči uradniki iz Europola podpirajo nacionalne organe z varnostnimi kontrolami v drugi vrsti na zunanjih mejah EU. Strokovnjaki Europola zagotavljajo podporo z zbiranjem in ocenjevanjem informacij, da bi odkrivali teroristične grožnje in grožnje kriminala, podpirali preiskave ter prepoznavali posameznike, ki pomenijo tveganje, ko poskušajo vstopiti v EU. Te operativne skupine zbirajo informacije, ki so podlaga za ocene ogroženosti zaradi kriminala, ki so na voljo državam članicam. Europolu taka dejavnost zbiranja obveščevalnih podatkov omogoča, da predvidi razvoj dogodkov in usklajuje operativne dejavnosti z državami članicami EU za odzivanje na dejavnosti kriminalnih združb, ki poskušajo izkoristiti vojno v Ukrajini, ter da nadgradi svoje dejavno sodelovanje z ukrajinskimi organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj prek ukrajinskega uradnika za zvezo na sedežu Europola na Nizozemskem.

V državah članicah in sosednjih državah EU je prisotna tudi **Evropska agencija za mejno in obalno stražo (Frontex)**, ki podpira operacije nadzora meje: po vsej EU, v države Zahodnega Balkana in v Moldavijo je trenutno napotenih več kot 2 100 pripadnikov mejne straže. **Evropski azilni podporni urad (EASO)** je v južne države članice EU in Litvo napotil skoraj 750 članov osebja za podporo operativnih dejavnosti, krepitev sprejemnih zmogljivosti in pomoč pri azilnih postopkih.

Komisija in francosko predsedstvo Sveta Evropske unije sta na podlagi veljavnega **Prümskega sklepa**³⁰, ki državam članicam zagotavlja okvir za napotitev uradnikov organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za skupne operacije, kot so skupne patrolje, poslala skupno pismo vsem državam članicam za opredelitev potreb ter pozvala k napotitvi policistov, da bi se v državah članicah EU na prvi črti, na katere najbolj

²⁸ Sporočilo Komisije – Operativne smernice za upravljanje zunanjih meja za poenostavitev prehajanja meja med EU in Ukrajino (2022/C 104 I/01).

²⁹ Europol je od 3. maja napotil enega svojega uslužbenca in tri gostujoče uradnike na Slovaško, enega svojega uradnika na Poljsko, enega svojega uradnika in štiri gostujoče uradnike v Romunijo ter dva gostujoča uradnika na Madžarsko. V Moldavijo sta napotena en uslužbenec Europola in dva gostujoča uradnika.

³⁰ 2008/615/PNZ, 2008/616/PNZ.

vplivajo množični prestopi meje kot posledica vojne, začele izvajati skupne patrolje. Komisija bo te napotitve financirala iz Sklada za notranjo varnost - policija.

Boj proti trgovini z ljudmi

EU je od prvih dni vojne pozorna na tveganja na posebnem področju kriminalne dejavnosti, na katerem bi se lahko izkoriščali veliki premiki ljudi, ki iščejo varnost v EU. Bistveno je, da se trgovcem z ljudmi, ki prežijo na ranljive osebe na begu, ki so večinoma **ženske in otroci**, prepreči na primer lažno ponujanje prevoza ali nastanitve.

Europol in Eurojust sta marca za ustrezne nacionalne organe izdala sporočila za zgodnje opozarjanje o morebitni trgovini z ljudmi in izkoriščanju žrtev, ki prihajajo iz Ukrajine. Eurojust pomaga okrepiti izmenjavo informacij in pospešiti pravosodno sodelovanje, tudi z Ukrajino, preiskave v zvezi s trgovino z ljudmi pa so bile posredovane tej agenciji zaradi usklajevanja.

Koordinatorica EU za boj proti trgovini z ljudmi se je sestala z mrežo nacionalnih poročevalcev ali enakovrednih mehanizmov EU, agencijami s področja pravosodja in notranjih zadev in platformo civilne družbe EU za boj proti trgovini z ljudmi, da so si izmenjali mnenja o ukrepih, potrebnih za preprečevanje zlorab in boj proti njim ter zaščito žrtev. V več državah članicah so bile sprožene preiskave morebitnih primerov.

EU je hitro in odločno poskrbela za usklajen odziv na to resnično grožnjo ljudem, ki potrebujejo pomoč EU. Državam članicam so bile hitro na voljo operativne smernice³¹, tudi v zvezi z izzivom trgovine z ljudmi, za izvajanje Direktive o začasni zaščiti v pomoč osebam, ki bežijo pred vojno v Ukrajini. Koordinatorica EU za boj proti trgovini z ljudmi je v sodelovanju z agencijami EU in državami članicami kot del načrta z desetimi točkami za močnejše evropsko usklajevanje pri sprejemanju oseb, ki bežijo pred vojno v Ukrajini³², predstavljenega 28. marca 2022 na zasedanju Sveta za pravosodje in notranje zadeve, razvila skupni načrt za boj proti trgovini z ljudmi in pomoč žrtvam³³. Poseben poudarek je namenjen evidentiranju subjektov in posameznikov (vključno s prostovoljci), ki nameravajo zagotavljati nastanitev, prevoz in druge vrste pomoči, ter varnostnemu preverjanju. Komisija se je povezala tudi z Agencijo EU za azil, da bi pri zdravstvenih pregledih v sprejemnih centrih podpirala odkrivanje žrtev trgovine z ljudmi. Tveganju zlorabe, spolnemu izkoriščanju ali prisilni kriminalni dejavnosti so še posebej izpostavljeni otroci brez spremstva ali ločeni otroci. V navedene operativne smernice so vključene tudi smernice za pomoč državam članicam, ki obravnavajo prihod in sprejem otrok, zlasti mladoletnikov brez spremstva, ter jim zagotavljajo podporo. Komisija je za ozaveščanje oseb, izpostavljenih tveganju, prav tako vzpostavila posebno spletišče z razdelkom, ki vključuje praktične nasvete o tem, kako se izogniti trgovcem z ljudmi.

³¹ C(2022) 1806, EUR-Lex - 52022XC0321(03) – SL – 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

Čeprav so bili posebej za odziv na nove razmere, ki so posledica vojne, sprejeti nekateri ukrepi za okrepitev pripravljenosti, drugi ključni ukrepi izhajajo iz **zakonodajnih pobud**, ki so bile v pripravi že pred rusko vojno agresijo proti Ukrajini.

Komisija pozdravlja dogovor o revidiranem mandatu **Europola**³⁴, dosežen februarja 2022, ki bo po začetku veljavnosti tej agenciji omogočal, da bolje podpre države članice v boju proti organiziranemu kriminalu in terorizmu. Agencija bo imela tedaj na voljo prava orodja in zaščitne ukrepe za podpiranje policijskih organov pri analizi masovnih podatkov za preiskovanje kaznivih dejanj in pri razvoju pionirskih metod za boj proti kibernetiski kriminaliteti. Te spremembe spremlja okrepljen okvir za varstvo podatkov ter večja parlamentarni nadzor in odgovornost.

S svežnjem o **policijskem sodelovanju**, ki ga je Komisija predstavila 8. decembra 2021³⁵ in o katerem trenutno potekajo pogajanja, se bo okrepilo sodelovanje med uradniki organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v državah članicah, tako da bo izmenjava podatkov potekala hitreje, lažje in varneje ter da se bo operativno policijsko sodelovanje na terenu izboljšalo in postalo učinkovitejše. Komisija poziva Evropski parlament in Svet, naj ta sveženj hitro sprejmeta.

Ko bodo ti zakonodajni predlogi sprejeti in se bodo začeli izvajati, bodo podprli preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v boju proti čezmejnemu organiziranemu kriminalu. To bo še zlasti pomembno v primerih, ko bi se lahko kriminalne združbe iz Ukrajine zaradi trenutnih razmer poskušale preseliti in nadaljevati svoje dejavnosti v EU.

Svetovalna misija EU v Ukrajini od leta 2014 podpira reformo preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter institucij pravne države. Marca 2022 je bil revidiran mandat misije, kar je omogočilo podporo na ukrajinskih mejnih prehodih s Poljsko, Romunijo in Slovaško, to pa je prispevalo k situacijskemu zavedanju o čezmejnih kriminalnih dejavnostih, vključno s trgovino z ljudmi, ter k pretoku humanitarnega blaga v Ukrajino.

IV. OROŽJE, NEVARNO BLAGO IN KRITIČNI INCIDENTI

Zaradi vojne se je v Ukrajini močno povečal promet s strelnim in drugim orožjem, kar pomeni nova tveganja za EU in druge države, ki mejijo na Ukrajino.

Pozornost in usklajevanje

Marca objavljene operativne smernice državam članicam zagotavljajo nasvete o tem, kako obravnavati izzive povečanega prometa s strelnim orožjem v času množičnih prihodov na zunanje meje EU³⁶. V teh smernicah je poudarjeno, da bi bilo treba stalno preverjati, ali oseba poseduje strelno orožje, in da osebam, ki za strelno orožje nimajo dovoljenja, vstop v EU s tem orožjem ne bi smel biti dovoljen. Če ukrajinski organi poročajo, da je katero od teh

³⁴ COM(2020) 796.

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

³⁶ Sporočilo Komisije – Operativne smernice za upravljanje zunanjih meja za poenostavitev prehajanja meja med EU in Ukrajino (2022/C 104 I/01).

strelnih orožij pogrešano, bi morale države članice to sporočiti v Schengenskem informacijskem sistemu.

Ključno je, da so vse pošiljke strelnega orožja v Ukrajino pravilno evidentirane z vsemi ustreznimi podatki (vključno s tipom/vrsto, državo in letom proizvodnje, znamko, modelom, kalibrom in serijsko številko) zaradi lažje sledljivosti tega orožja v Ukrajini in EU.

EU je javno obsodila nepremišljene vojaške napade Rusije na jedrske, biološke in kemijske civilne objekte in v njihovi neposredni bližini v Ukrajini ter dejanja, ki ogrožajo varnost teh objektov. Komisija spremlja razmere v Ukrajini, pri čemer posebno pozornost namenja radiološki grožnji, ki je z vidika notranje varnosti EU najbolj zaskrbljujoča³⁷. Spremlja tudi morebitne kemične grožnje; če bo potrebna hitra ocena tveganja, pa je vzpostavila mehanizem notranjega usklajevanja.

Pripravljenost

Ukrajina je v akcijskem načrtu EU glede trgovine s strelnim orožjem za obdobje 2020–2025 že opredeljena kot ena od ključnih držav za posebne ukrepe na zunanji ravni. V regiji, ki vključuje Ukrajino, poteka tudi posebni operativni ukrep v okviru platforme EMPACT za strelno orožje. Ker pa obstaja tveganje, da bo strelno orožje preusmerjeno, bodo potrebni posebni projekti, ki jih bo financirala EU, ter operativno sodelovanje z Europolom, Frontexom in sklopom platforme EMPACT za strelno orožje. Komisija bo kmalu predstavila predlog za revizijo uredbe o strelnem orožju,³⁸ ki obravnava izvoz, uvoz in tranzit strelnega orožja za civilno uporabo in je del splošnega pravnega in operativnega okvira, katerega namen je preprečevati, odkrivati, preiskovati in kazensko preganjati trgovino s strelnim orožjem.

Komisija za izboljšanje pripravljenosti in odzivanja EU na tveganja za javno zdravje, kot so kemične, biološke, radiološke in jedrske grožnje, oblikuje strateške rezerve zmogljivosti za odzivanje v okviru mehanizma Unije na področju civilne zaščite, ki ga financira organ EU za pripravljenost in odzivanje na izredne zdravstvene razmere (HERA)³⁹. Službe Komisije sodelujejo pri razvoju strateških zalog v okviru rescEU v vrednosti 540,5 milijona EUR. Zaloga bo sestavljena iz opreme in zdravil, cepiv in drugih terapevtikov za zdravljenje bolnikov, ki so bili izpostavljeni kemičnim, biološkim, radiološkim in jedrskim agensom, ter rezerve rescEU za dekontaminacijo, da se zagotovijo oprema za dekontaminacijo in strokovne skupine za odzivanje. EU je kot takojšen prvi ukrep mobilizirala svojo medicinsko rezervo v okviru rescEU za nabavo tablet kalijevega jodida, ki se lahko uporabijo za zaščito ljudi pred škodljivimi učinki ionizirajočega sevanja, ter drugega blaga, ki je v Ukrajini nujno potrebno. V Ukrajino je bilo prek mehanizma Unije na področju civilne zaščite s pomočjo Francije in Španije dostavljenih že skoraj tri milijone tablet jodida.

³⁷ Komisija bo v sodelovanju s partnerji iz ZDA organizirala delavnico o tveganjih, povezanih z radiološkimi materiali v bolnišnicah, ki niso pod regulativnim nadzorom.

³⁸ Uredba (EU) št. 258/2012 Evropskega parlamenta in Sveta z dne 14. marca 2012 o izvajanju člena 10 Protokola Združenih narodov o nedovoljeni proizvodnji strelnega orožja, njegovih sestavnih delov in streliva ter trgovini z njimi, ki dopolnjuje Konvencijo Združenih narodov proti mednarodnemu organiziranemu kriminalu (Protokol ZN o strelnem orožju), uvedbi izvoznih dovoljenj za strelno orožje, njegove sestavne dele in strelivo ter ukrepov glede njihovega uvoza in tranzita.

³⁹ [HERA Work Plan 2022 \(europa.eu\)](https://europa.eu/HERA-Work-Plan-2022) (Delovni načrt HERA za leto 2022 (europa.eu)).

V. USKLAJENO UKREPANJE, DA BI RUSIJA ODGOVARJALA ZA AGRESIJO

EU ima odločilno vlogo pri ukrepih na ravni mednarodne skupnosti, s katerimi se izvaja pritisk na Rusijo, naj konča agresijo proti Ukrajini in civilistom, ujetim v spopadih, ki je nesprejemljiva in v nasprotju z mednarodnim pravom. V ta pritisk so zajeti ukrepi z navedbo posledic za storilce kaznivih dejanj, vključno s hudimi sankcijami, ter ukrepi za opredelitev vojnih zločinov in olajšanje kazenskega pregona.

Omejevalni ukrepi in odvzem premoženja

Odkar je Rusija 21. februarja 2022 priznala območja ukrajinskih pokrajin Doneck in Lugansk, ki niso pod vladnim nadzorom, in 24. februarja 2022 začela invazijo na Ukrajino, je EU proti Rusiji uvedla najboljše omejevalne ukrepe doslej. Do danes je bilo sprejetih pet svežnjev omejevalnih ukrepov. Usmerjeni so v ključne sektorje, vključno s financami, trgovino, prometom, obrambo in mediji, ter v politično in vojaško elito in pomembne ruske in beloruske oligarhe. Na sezname je uvrščenih že več kot 1 000 posameznikov in 80 subjektov. Svet razpravlja o šestem svežnju omejevalnih ukrepov.

Učinek teh in prejšnjih omejevalnih ukrepov proti ruskim in beloruskim posameznikom ter podjetjem je odvisen od njihovega izvrševanja. Usklajevanje na ravni EU lahko pomembno prispeva k odpravi morebitnih vrzeli, Komisija pa je deležnikom zagotovila obsežno podporo s pisnimi smernicami, srečanji in posebno strokovno skupino ter naborom virov za olajšanje zagotavljanja skladnosti.

Poleg tega je Komisija vzpostavila projektno skupino „Freeze and Seize“, ki združuje službe Komisije, države članice, Europol in Eurojust. Države članice so poročale, da so doslej zamrzile sredstva v vrednosti 9,89 milijarde EUR⁴⁰. Europol je 11. aprila v sodelovanju z državami članicami, Eurojustom in Frontexom začel izvajati operacijo Oskar, s katero je podprl finančne in kazenske preiskave, usmerjene v sredstva, pridobljena s kaznivim dejanjem, ki so v lasti posameznikov in pravnih subjektov, za katere veljajo omejevalni ukrepi EU v zvezi z rusko vojno proti Ukrajini. Projektna skupina „Freeze and Seize“ EU tesno sodeluje s projektno skupino za ruske elite, posrednike in oligarhe, ki so jo vzpostavile države skupine G7 (Kanada, Francija, Nemčija, Italija, Japonska, Združeno kraljestvo in Združene države Amerike) ter podobno misleče partnerice, kot je Avstralija, ter z ameriško projektno skupino KleptoCapture in ukrajinsko projektno skupino.

Projektna skupina „Freeze and Seize“ se uporablja kot platforma za usklajevanje in olajšanje izmenjave informacij in izkušenj med državami članicami ter zagotavljanje smernic o izvajanju omejevalnih ukrepov, pa tudi za lažjo izmenjavo dobrih praks o kazenskih preiskavah in odvzemu. Pomembno je zlasti, da so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj pozorni in proaktivni v zvezi z morebitnimi kaznivimi dejanji posameznikov in pravnih subjektov, za katere veljajo omejevalni ukrepi. Projektna skupina si prav tako prizadeva za napredek pri razpravah o morebitni uporabi odvzetih sredstev, na primer kot prispevek k obnovi Ukrajine.

⁴⁰ Znesek zamrznjenih sredstev Ruske centralne banke znaša približno 23 milijard EUR.

Komisija danes sprejema sveženj o **povrnitvi in odvzemu sredstev**⁴¹, v katerem so bila upoštevana nova spoznanja, pridobljena pri izvajanju omejevalnih ukrepov Unije proti ruskim in beloruskim posameznikom in subjektom. Sveženj bo olajšal učinkovito izvajanje omejevalnih ukrepov EU po vsej Uniji, tako da bo omogočil hitro izsleditev in identifikacijo premoženja v lasti ali pod nadzorom oseb ali subjektov, za katere veljajo taki ukrepi. Okrepljen okvir za povrnitev in odvzem sredstev se bo uporabljal tudi pri kršitvah omejevalnih ukrepov ter bo tako zagotovil učinkovito izsleditev, zamrznitev, upravljanje in odvzem premoženjske koristi, pridobljene s kršitvijo omejevalnih ukrepov. Da bi Komisija zagotovila, da se sredstva posameznikov in subjektov, ki kršijo omejevalne ukrepe, dejansko lahko odvzamejo, danes sprejema tudi predlog sklepa Sveta o vključitvi kršitve omejevalnih ukrepov na seznam kaznivih dejanj EU iz člena 83(1) PDEU⁴² ter spremljajoče sporočilo⁴³ o prihodnjem predlogu direktive o približevanju opredelitve kaznivih dejanj in kazni za kršitve omejevalnih ukrepov.

Ta sveženj je splošneje ključen korak v boju proti organiziranemu kriminalu. Upošteva zaveze Komisije, sprejete v strategiji za varnostno unijo in strategiji za boj proti organiziranemu kriminalu za obdobje 2020–2025⁴⁴. Spreminja direktivo o odvzemu iz leta 2014, sklep Sveta o uradih za odvzem premoženjske koristi iz leta 2007 in okvirni sklep o zaplembi premoženjske koristi, pripomočkov in premoženja, ki so povezani s kaznivimi dejanji, iz leta 2005, da bi se okrepile zmogljivosti za izsleditev in identifikacijo ter nazadnje odvzem nezakonito pridobljene koristi, pri čemer obravnava zelo majhen delež odvzemov v EU⁴⁵. S svežnjem se povečuje obseg zajetih kaznivih dejanj in razširjajo pravila o odvzemu v primerih, v katerih kazenska obsodba za določeno kaznivo dejanje ni mogoča, sredstva pa jasno izhajajo iz kriminalne dejavnosti. Z revizijo se tudi izboljšuje učinkovito upravljanje zamrznjenih in odvzetih sredstev ter krepí zmogljivost uradov za odvzem premoženjske koristi za izsleditev in identifikacijo nezakonitih sredstev. Novi okvir EU za povrnitev sredstev je zasnovan tako, da obravnava kompleksen način delovanja kriminalnih organizacij, ki pogosto delujejo čezmejno in svoja sredstva prikrivajo z različnimi metodami, tudi s kriptosredstvi.

Usklajen pravosodni odziv

Na ravni EU je prav tako potekalo delo za zagotovitev usklajenega pravosodnega odziva na domnevno **mednarodno kriminaliteto** v Ukrajini, da bi lahko storilci kaznivih dejanj za svoja dejanja odgovarjali.

Dve državi članici in Ukrajina so vzpostavile skupno preiskovalno skupino za preiskovanje vojnih zločinov, kaznivih dejanj zoper človečnost in drugih oblik mednarodne kriminalitete, domnevno storjenih na ozemlju Ukrajine. Eurojust tej skupini zagotavlja pravno, analitično, finančno in logistično podporo. Tožilstvo Mednarodnega kazenskega sodišča (OTP-ICC) se

⁴¹ COM(2022) 245.

⁴² COM(2022) 247.

⁴³ COM(2022) 249.

⁴⁴ COM(2021) 170.

⁴⁵ Europol ocenjuje, da sta zamrznjena le 2 % sredstev, pridobljenih s kaznivim dejanjem (2,4 milijarde EUR), odvzet pa je le 1 % takih sredstev (1,2 milijarde EUR), medtem ko so prihodki od kaznivih dejanj na glavnih trgih kriminalnih dejavnosti EU leta 2019 znašali 139 milijard EUR (1 % BDP EU).

je skupni preiskovalni skupini 25. aprila 2022 pridružilo kot udeleženec⁴⁶ in pričakuje se, da se ji bodo kmalu pridružili še drugi.

Komisija je 25. aprila 2022 predstavila predlog za spremembo uredbe o Eurojustu⁴⁷, da bo lahko ta agencija zbirala, analizirala in shranjevala dokaze o osrednjih mednarodnih kaznivih dejanjih. Eurojust in Europol bosta v tem procesu še naprej tesno sodelovala. Ključno vlogo pri usklajevanju pravosodnega odziva bo imela tudi mreža za področje genocida, katere sekretariat gosti Eurojust, ki je pripravila atlas nevladnih organizacij, zdaj dejavnih v Ukrajini, ter ki podpira nacionalne pravosodne delavce iz držav članic in Ukrajine, ki obravnavajo odprte primere, povezane z vojno.

Svet je aprila 2022 nadalje revidiral **mandat svetovalne misije EU v Ukrajini**, s čimer je omogočil njeno podporo ukrajinskim organom pri preiskovanju in kazenskem pregonu vseh oblik mednarodne kriminalitete, storjenih v okviru ruske vojaške agresije. Misija bo ukrajinskim organom zagotavljala strateške nasvete o preiskavah in kazenskem pregonu mednarodne kriminalitete, potrebnih spremembah ukrajinske zakonodaje, komunikacijski strategiji ter usposabljanju o povezanih zadevah. Misija spada med številne pobude usklajevanja v tem okviru in je skupaj z delegacijo EU del svetovalne skupine ZDA-EU za Ukrajino za grozodejstva.

VI. TUJE MANIPULIRANJE Z INFORMACIJAMI IN VMEŠAVANJE

Sedanji geopolitični razvoj dogodkov je opozoril na tveganja tujega vmešavanja. Rusko vojaško agresijo proti Ukrajini so spremljale dejavnosti **manipuliranja** z informacijami in **vmešavanja**. Brutalni napadi na Ukrajino se upravičujejo z neosnovanimi očitki ukrajinski vladi glede „nacizma“ in „genocida“, operacijami pod lažno zastavo in neutemeljenimi obtožbami proti NATO in Zahodu, svoboda govora in neodvisno poročanje v Rusiji pa sta zatrta. Obstaja stalno tveganje manipuliranja z avdiovizualnim gradivom in dezinformiranja, ki bi ju Rusija lahko poskušala uporabiti kot izgovor za dodatne vojaške napade ter za oslabitev odločnosti ukrajinskega odpora, razdelitev mednarodne skupnosti v njenem nasprotovanju vojni ali sejanje dvoma o ruskih kršitvah mednarodnega prava. EU se je v strateškem kompasu zavezala k odločnemu odzivu na tuje manipuliranje z informacijami in vmešavanje ter krepitvi svoje odpornosti in zmogljivosti za boj proti takim grožnjam⁴⁸. Manipuliranje demokratične razprave v EU je vključeno v akcijski načrt za evropsko demokracijo, ki je usklajen načrt Komisije za obravnavanje dezinformacij in krepitev demokratične odpornosti⁴⁹.

Pozornost in usklajevanje

Evropska unija se je z odločnim in usklajenim ukrepanjem odzvala na rusko kampanjo dezinformiranja v okviru vojaške agresije proti Ukrajini. V tesnem sodelovanju z državami članicami prek sistema hitrega obveščanja in z mednarodnimi partnericami, kot so NATO, ZDA in Kanada, ter mehanizmom G7 za hitro odzivanje si izmenjuje spoznanja glede trendov in taktik manipuliranja, ki jih uporablja Kremelj. Okrepila so se prizadevanja za razkrivanje manipulacij Kremlja, zlasti prek spletišča EUvsDisinfo z vsebino v angleščini, ruščini,

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

⁴⁷ COM(2022) 187.

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

⁴⁹ COM(2020) 790.

ukrajinsčini in drugih jezikih, da bi se zagotovile na dejstvih temelječe informacije v EU, Ukrajini in regiji ter tudi v Rusiji. Prenos in oddajanje ruskih državnih medijskih kanalov RT in Sputnik v EU ali usmerjenih v EU sta bila od 2. marca začasno ustavljena, kar je posledica omejevalnih ukrepov, ki jih je sprejela EU. Spletne platforme, vodilna družbena omrežja, oglaševalci in podpisniki kodeksa ravnanja glede dezinformacij⁵⁰ iz oglaševalske industrije sprejemajo nujne ukrepe za omejitev dezinformacij v zvezi z rusko agresijo v Ukrajini. Njihova prizadevanja spremljata Komisija in ESZD. Informacije, ki jih objavljajo, kažejo, da so platforme okrepile orodja za spremljanje in ukrepanje, povezana z vojno.

Poleg tega se hitro uvajajo ukrepi v podporo državam v Srednji Aziji in na Zahodnem Balkanu, da bi se povečala informacijska odpornost ter preprečila tuje manipuliranje z informacijami in dezinformacije.

Pripravljenost

Zaradi odkritega tujega manipuliranja z informacijami in vmešavanja, vključno z dezinformacijami kot enim od orodij hibridnih groženj, se je izredno povečala nujnost nadgradnje akcijskega načrta za evropsko demokracijo. Institucije EU so v zadnjih mesecih podpirale države članice v boju proti tujemu manipuliranju z informacijami in vmešavanju, zlasti v okviru sistema hitrega obveščanja, z izmenjavo spoznanj o taktikah, ki jih uporabljajo akterji takega manipuliranja in vmešavanja, in o strategijah odzivanja. Potekajo razprave o nadaljnji okrepitvi splošnega odziva EU na tuje manipuliranje z informacijami in vmešavanje na podlagi dokumenta za razpravo, ki ga je predložila ESZD, o razvoju posebnega **nabora orodij** za obravnavanje te grožnje. Tako se bodo pod okriljem skupne zunanje in varnostne politike zbrali obstoječi ukrepi in nova orodja EU. Koristno bo tudi odločnejše ukrepanje projektne skupine Stratcom Evropske službe za zunanje delovanje⁵¹ in Komisije.

Evropska opazovalnica digitalnih medijev, ki je po izbruhu vojne v Ukrajini ustanovila projektno skupino za dezinformacije, usklajuje ukrepe s preverjevalci dejstev in raziskovalci v svoji mreži. Analizirala je, kako so se zagovorniki teorij zarot o COVID-19 hitro preusmerili v razširjanje proruskih prevar, kar je bilo mogoče opaziti v številnih državah članicah⁵².

Namen predloga akta o digitalnih storitvah je prilagoditi se na hitro razvijajoče se digitalne tehnologije in ugotoviti, kaj to pomeni za tehnološke in demokratične izzive, kot so sovražni govor, dezinformacije na spletu in strategije destabilizacije. Precejšen napredek pri pogajanjih med Evropskim parlamentom in Svetom bi moral omogočiti hitro sprejetje tega svežnja.

VII. ŠIRŠA PRIPRAVLJENOST

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

⁵¹ Oddelek za strateško komuniciranje, projektne skupine in analizo informacij Evropske službe za zunanje delovanje zagotavlja podporo na področju strateškega komuniciranja pri izvajanju skupne zunanje in varnostne politike EU v povezanih prednostnih regijah (južno in vzhodno sosedstvo, Zahodni Balkan), tako da razvija in izvaja posebne ukrepe strateškega komuniciranja, usmerjene v spodbujanje politik, vrednot, ciljev in interesov EU.

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

Usklajevanje na področju varnosti v EU se je v času, ko vojna znova poteka na evropskih tleh in se dogajajo veliki geopolitični premiki, okrepilo in temelji na pobudah, ki so bile v pripravi že pred rusko vojno agresijo proti Ukrajini. Pobude, usmerjene predvsem v zunanjo varnost EU, močno vplivajo na notranjo agendo varnostne unije.

Komisija je 15. februarja 2022 predstavila **obrambni sveženj**⁵³ s številnimi pobudami na področjih, ključnih za obrambo in varnost v EU. Ta prispevek Komisije k evropski obrambi in varnosti zajema celoten sklop izzivov. Predlaga konkretne ukrepe za bolj povezan in konkurenčnejši evropski obrambni trg, zlasti s krepitvijo sodelovanja v EU in ustvarjanjem ekonomije obsega. Vključuje tudi kažipot za tehnologije, kritične za varnost in obrambo, da bi se spodbudile raziskave, tehnološki razvoj in inovacije v teh sektorjih ter zmanjšale odvisnosti pri kritičnih tehnologijah in vrednostnih verigah. Namen svežnja je tudi krepitev obrambne razsežnosti vesolja na ravni EU. Poleg tega je proučeno, kako bi lahko Komisija okrepila svoja prizadevanja proti hibridnim grožnjam, tudi na kibernetnem področju, povečala vojaško mobilnost v Evropi in zunaj nje ter nadalje obravnavala izzive podnebnih sprememb, povezane z obrambo. Skupno sporočilo **o analizi vrzeli pri naložbah v obrambo in nadaljnjih korakih**⁵⁴ z dne 18. maja obravnava vrzeli v zmogljivostih in industriji, ki jih je treba odpraviti, da bi se podprle najbolj izpostavljene države članice EU in opredelili ukrepi za odpravo navedenih pomanjkljivosti.

Odpornost EU proti tem grožnjam pomeni tudi pristope, ki so usmerjeni v zmogljivosti v vseh varnostnih sektorjih, za kar se je Komisija zavzemala v akcijskem načrtu za sinergije med civilno, obrambno in vesoljsko industrijo⁵⁵. Potekajo prizadevanja za spodbujanje pristopov, ki so usmerjeni v zmogljivosti na področju notranje varnosti ter preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

Svet je 21. marca 2022 sprejel **Strateški kompas za varnost in obrambo**⁵⁶, ki ga je kmalu za tem podprl Evropski svet. Kompas določa ambiciozen akcijski načrt za okrepitev varnostne in obrambne politike EU do leta 2030. Njegov cilj je, da bi EU postala močnejša in zmogljivejša pri zagotavljanju varnosti, varovala svoje državljane in državljanke ter prispevala k mednarodnemu miru in varnosti. Vsebuje konkretne predloge z zelo natančnim časovnim razporedom izvajanja, da bi se izboljšala zmogljivost EU za odločno ukrepanje v kriznih razmerah.

Eden od rezultatov strateškega kompasa je razvoj **lastnega nabora orodij EU za odzivanje na hibridne grožnje**, ki naj bi zagotovil okvir za usklajen odziv na hibridne kampanje, ki vplivajo na EU in njene države članice, vključno z notranjimi in zunanjimi ukrepi. Po opredelitvi sektorskih izhodišč odpornosti v začetku leta 2022⁵⁷ bo dokončana analiza vrzeli in potreb. EU bo v tem okviru še naprej povečevala pripravljenost, odpornost in odzivanje na grožnje, ki so posledica ruske agresije ter vseh drugih poskusov destabilizacije demokracije in na pravilih temelječega večstranskega reda.

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

⁵⁴ JOIN(2022) 24.

⁵⁵ COM(2021) 70.

⁵⁶ Strateški kompas za varnost in obrambo – Za Evropsko unijo, ki varuje svoje državljane in državljanke, vrednote in interese ter prispeva k mednarodnemu miru in varnosti;
<https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/sl/pdf>.

⁵⁷ SWD(2022) 21.

VIII. OBETI ZA PRIHODNOST

EU bo morala v prihodnje ostati zelo pozorna na spreminjajoče se grožnje ter povečevati **pripravljenost in odpornost na vse možnosti**. Vojna ima lahko različne posledice, ki jih še ni mogoče vseh oceniti.

Ni še znano, kakšen je obseg razselitve ukrajinskih kriminalnih mrež. Iz pretekle Eurojustove obravnave primerov je razviden trend trgovanja s heroinom iz Afganistana v EU prek Ukrajine, kar je potrdil tudi Evropski center za spremljanje drog in zasvojenosti z drogami (EMCDDA)⁵⁸. Zaradi nestabilnosti bo morda težje ukrepati proti trgovini s heroinom prek te poti, zaradi česar obstaja tveganje morebitnega povečanja pretoka drog v EU.

Nekatera tveganja za EU se bodo verjetneje povečala ob koncu vojskovanja ali med morebitnimi premori. Posebna pozornost bo namenjena prometu s strelnim orožjem, pri čemer bo tveganje večje po prenehanju bojev v Ukrajini. Preteklo izkušnje kažejo tudi na tveganje, da lahko vračanje tujih bojnikov, ki so si pridobili bojne izkušnje in morda prišli v stik z ekstremističnimi skupinami, pomeni poznejše teroristične dejavnosti v EU. Možnosti za pojav teh dejavnosti je treba skrbno spremljati, Komisija pa že spodbuja razprave med državami članicami o izzivih, ki jih prinaša vračanje tujih prostovoljcev s preteklostjo nasilnega ekstremizma.

Ob upoštevanju teh morebitnih groženj je pomembno nadaljevati izvajanje strategije EU za varnostno unijo, pa tudi drugih ključnih strategij, kot so strategija EU za kibernetno varnost, strategija za boj proti organiziranemu kriminalu (2020–2025), agenda EU za boj proti terorizmu (2020–2025), akcijski načrt EU glede trgovine s strelnim orožjem (2020–2025), strategija EU za boj proti trgovini z ljudmi (2021–2025) in strategija EU na področju drog (2021–2025).

Prizadevanja za zagotovitev potrebnega zakonodajnega okvira EU se bodo nadaljevala. Komisija na primer pripravlja oceno učinka za predlog, ki ureja trženje in uporabo kemikalij z visokim tveganjem.

IX. SKLEP

Varnostna unija ima še naprej ključno vlogo pri pripravi EU in držav članic na boj proti obstoječim in morebitnim grožnjam. Ruska vojna agresija proti Ukrajini je pokazala, kako hitro se lahko teoretične grožnje udejanjijo, ter poudarila pomen pozornosti, usklajevanja in pripravljenosti.

Iz tega četrtega poročila o napredku pri izvajanju strategije za varnostno unijo je razvidno, da se lahko EU prilagodi, tudi v razmerah izrednih in nepričakovanih groženj, kot je ruska vojna agresija proti Ukrajini. Odločno izvajanje strategije za varnostno unijo je zdaj pomembnejše kot kdaj koli prej.

⁵⁸ Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data), OEDT, Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery (Poročilo o stanju na področju drog in alkohola v Ukrajini za leto 2020 (glede na podatke iz leta 2019), EMCDDA, Zaustavitev trgovanja z nadomestkom heroina v Franciji, na Poljskem in v Ukrajini, vključno z načrtovanjem in izvajanjem nadzorovanih pošiljk), 2021/00446, Eurojust, maj 2020.