Svet
Evropske unije

Bruselj, 18. oktober 2023
(OR. en)

14372/23

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

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	18. oktober 2023
Prejemnik:	Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije
Št. dok. Kom.:	COM(2023) 665 final
Zadeva:	SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU o šestem poročilu o napredku pri izvajanju strategije EU za varnostno unijo

Delegacije prejmejo priloženi dokument COM(2023) 665 final.

Priloga: COM(2023) 665 final

EVROPSKA
KOMISIJA

Bruselj, 18.10.2023
COM(2023) 665 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU IN SVETU

o šestem poročilu o napredku pri izvajanju strategije EU za varnostno unijo

I. Uvod

Komisija je pred tremi leti sprejela strategijo za varnostno unijo za obdobje 2020–2025[1], v kateri so opredeljene glavne prednostne naloge Unije na področju varnosti. Od takrat je bil dosežen velik napredek v okviru vseh štirih stebrov strategije, pri čemer se je zagotovila prelomna zakonodaja na vseh področjih od zaščite kritičnih subjektov do krepitve kibernetske odpornosti. Medtem pa se narava varnostnih groženj v Evropi in njenem sosedstvu še naprej spreminja. Teroristični napadi v eni od naših šol v Franciji in na ulicah Bruslja v zadnjih dneh so oster opomnik, da je nujno treba še naprej prilagajati in krepiti našo varnostno strukturo. Nevarnost, ki jo predstavljajo kibernetski napadi, se še naprej povečuje, podžigajo pa jih tudi zlonamerni akterji v sedanjih konfliktih. Hibridne grožnje, vključno z dezinformacijami, se še naprej povečujejo. Europol je rusko vojno agresijo proti Ukrajini opredelil kot vzrok za znatno povečanje kibernetskih napadov na tarče v EU, pri čemer so veliki napadi politično motivirani, usklajujejo pa jih proruske hekerske skupine[2]. To je bilo razvidno tudi pri blokiranju dostopa do interneta in prekinitvi ključnih storitev, kot so energetska omrežja[3].

Strategija za varnostno unijo je bila zasnovana tako, da bo lahko EU bolje vzdržala spreminjajočo se naravo groženj. Med spoprijemanjem s krizami, ki sta jih povzročili pandemija in vojna, so dogodki pokazali, kako pomemben je pristop iz strategije – naša odločenost, da se pridružimo točkam v varnostnem ekosistemu EU ter odpravimo ločnice med kibernetsko in fizično razsežnostjo varnosti, vključno z bojem proti organiziranemu kriminalu in terorizmu ter bojem proti radikalizaciji.

Zaradi previdnosti pa moramo nenehno preverjati, kje vse še lahko okrepimo varnost naših državljanov. V strategiji so določena prednostna področja, na katerih lahko Unija prispeva dodano vrednost v podporo državam članicam pri povečanju varnosti za vse ljudi, ki živijo v Evropi. Od njenega sprejetja so bili obravnavani vsi določeni ukrepi, vključeni pa so bili tudi novi ukrepi za odzivanje na aktualne varnostne izzive.

Komisija je v okviru strategije za varnostno unijo predstavila skupaj 36 zakonodajnih pobud. Za več kot polovico teh predlogov so se medinstitucionalna pogajanja že zaključila s trdno novo zakonodajo, kot je opisano v preglednici v Prilogi. Vendar o več ključnih pobudah, ki jih je predlagala Komisija, še vedno potekajo pogajanja v Evropskem parlamentu in Svetu. Sedanje parlamentarno obdobje se bo končalo z evropskimi volitvami junija 2024, zato je treba hitro opraviti delo v zvezi s temi nerešenimi zadevami, da bodo lahko državljani v celoti izkoristili varnostno unijo. To šesto poročilo o napredku varnostne unije je zato osredotočeno na tisto ključno zakonodajno in nezakonodajno gradivo v zvezi z varnostno unijo, ki ga je sprejela Komisija in v zvezi s katerim je treba storiti več, da bi se dokončalo in učinkovito izvajalo.

Koristi že dogovorjenih zakonov EU se bodo čutile šele, ko se bodo izvajali v praksi. Prizadevanja morajo biti osredotočena na njihove pravilne in popolne prenos, izvajanje in uporabo v državah članicah. Komisija je v letu 2023 še naprej zagotavljala rezultate strategije EU za varnostno unijo, in sicer z uporabo svojih institucionalnih pooblastil za začetek

[1] COM(2020) 605.

[2] Porazdeljeni napadi za zavrnitev storitve (DDoS): glej poročilo Europola „Cyber-attacks: the apex of crime-as-a-service“ (Kibernetski napadi: vrhunec kriminala kot storitve) z dne 13. septembra 2023.

[3] V konfliktu v Ukrajini se brisalci zlonamerne programske opreme pogosto uporabljajo za uničenje podatkov in sistemov, ki so na primer vplivali na dostop do interneta za več tisoč naročnikov v EU, pa tudi za pomembno nemško energetsko podjetje, ki je izgubilo dostop do daljinskega spremljana več kot 5 800 vetrnih turbin. „The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict“ (Vloga kibernetske varnosti v ruski vojni proti Ukrajini: njen učinek in posledice za prihodnost oboroženih spopadov), študija Evropskega parlamenta, september 2023, PE 702.594.

postopkov za ugotavljanje kršitev, kadar koli države članice zakonodaje EU niso prenesle ali so jo prenesle nepravilno.

V tem poročilu je povzeto tudi, kje je izvajanje ukrepov držav članic in/ali agencij EU osrednjega pomena. Agencije EU imajo ključno vlogo pri podpiranju izvajanja pobud na področju varnostne unije, njihove odgovornosti pa so se v zadnjih letih razširile. V poročilu so opisane nekatere glavne nove naloge, ki so jim bile dodeljene za zagotavljanje večje podpore državam članicam pri izvajanju ključnih pobud v okviru varnostne unije.

Poleg tega je bil zaradi geopolitičnih razmer poudarjen pomen zunanje varnosti za našo notranjo varnost. Močnejši notranji okvir EU na področju varnosti je neločljivo povezan s tesnejšimi partnerstvi in sodelovanjem s tretjimi državami. EU si mora še naprej dejavno prizadevati za iskanje načinov, kako lahko sodelovanje po vsem svetu prispeva k zagotovitvi varnosti državljanov doma.

II. Varnostno okolje, primerno za prihodnost

Kibernetska varnost in odpornost kritične infrastrukture

Unija je v okviru varnostne unije zavezana zagotavljanju, da so vsi evropski državljani in podjetja dobro zaščiteni, tako na spletu kot zunaj njega, ter spodbujanju odprtega, varnega in stabilnega kibernetskega prostora. Vse večji obseg, pogostost in vpliv kibernetskih incidentov močno ogrožajo delovanje omrežij in informacijskih sistemov ter notranji trg. Z rusko vojno agresijo proti Ukrajini se je ta grožnja še zaostrila, zaradi sedanjih geopolitičnih napetosti pa se stopnjujejo posredovanja številnih na državni ravni usklajenih, kriminalnih in hektivističnih akterjev. Sabotaža plinovodov Severni tok lansko jesen je poudarila, da so bistveni sektorji, kot so energetika, digitalna infrastruktura, promet in vesolje, odvisni od odporne kritične infrastrukture. Nedavni incident v zvezi s podmorskim plinovodom in podatkovnim kablom v Estoniji in na Finskem kaže, da je za spoprijemanje s tovrstnimi razmerami potrebna visoka stopnja pripravljenosti. Čeprav vzrok škode ostaja nejasen in preiskave še potekajo, je bila izmenjava informacij na različnih ravneh med državami članicami in Komisijo spodbudna. Motnje niso imele neposrednega učinka na internetno povezljivost ali zanesljivost oskrbe s plinom na evropski ali lokalni ravni. To je znak doseženega napredka in okrepljenih prizadevanj za pripravljenost v zadnjih mesecih.

Jasen in trden pravni okvir je zato bistven za zagotovitev zaščite in odpornosti teh kritičnih infrastruktur. V zvezi s tem je bil ključni preboj dosežen s hkratnim sprejetjem revidirane direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (NIS 2)[4] in direktive o odpornosti kritičnih subjektov[5], ki sta začeli veljati 16. januarja 2023. Države članice so pozvane, naj hitro in v celoti prenesejo ta temeljna zakonodajna akta, in sicer najpozneje do 17. oktobra 2024, da bi se vzpostavil trden okvir Unije za zaščito kritične infrastrukture Unije pred fizičnimi in kibernetskimi grožnjami.

[4] Direktiva (EU) 2022/2555 z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in Direktiva (EU) 2018/1972 (direktiva NIS 2).

[5] Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES.

Komisija je julija 2023 v delegirani uredbi Komisije določila bistvene storitve v 11 sektorjih, ki jih zajema direktiva o odpornosti kritičnih subjektov[6]. Naslednji korak je, da države članice izvedejo ocene tveganja za te storitve. V skladu s priporočilom Sveta[7] z dne 8. decembra 2022 se je okrepilo delo v zvezi s stresnimi testi za kritično infrastrukturo, začenši z energetskim sektorjem, ter v zvezi s krepitvijo sodelovanja z Natom in ključnimi partnerskimi državami. Na podlagi tega dela je projektna skupina EU-NATO junija 2023 pripravila poročilo o odpornosti kritične infrastrukture, v katerem so opisani sedanji varnostni izzivi za kritično infrastrukturo v štirih ključnih sektorjih (energetika, promet, digitalna infrastruktura in vesolje) ter priporočila za okrepitev odpornosti. Priporočila, vključno z okrepljenim usklajevanjem, izmenjavo informacij in dejavnostmi, izvaja osebje EU in Nata v okviru strukturiranega dialoga o odpornosti.

Hkrati je Komisija 6. septembra 2023 sprejela predlog[8] priporočila Sveta o načrtu za krepitev usklajenega odzivanja na ravni Unije na poskuse motenj na kritični infrastrukturi z velikim čezmejnim pomenom. Dne 4. oktobra 2023 je bila organizirana dejavnost v obliki razprave o načrtu na podlagi scenarijev, da bi se preizkusilo, kako bi se načrt uporabljal v praksi, in prispevalo k sedanjim pogajanjem o predlogu v okviru Sveta.

Po pozivih Sveta[9] so Komisija, visoki predstavnik in Skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov ocenjevali tveganja in oblikovali scenarije tveganja z vidika kibernetske varnosti. To delo se najprej osredotoča na sektorja telekomunikacij in električne energije. Sodelovanje vseh ustreznih agencij in mrež, civilnih in vojaških, prvič pomeni celovito in vključujočo oceno na ravni Unije. Dodatno bo dopolnjevalo usklajene ocene varnostnega tveganja kritičnih dobavnih verig, ki se izvajajo v okviru direktive NIS 2, ter ocene tveganja in stresne teste kritične infrastrukture v sektorjih energetike, komunikacij digitalne infrastrukture, prometa in vesolja. Zaradi usklajevanja in skladnosti bi se morale te dejavnosti medsebojno nadgrajevati, da bi pomagale vzpostaviti standardni pristop, ter usmerjati razvoj prihodnjih dejavnosti. Uspeh teh ukrepov bo zdaj odvisen od dejavnega sodelovanja držav članic.

Delovanje gospodarstev in družb je vse bolj odvisno od vesoljskih storitev in podatkov, zlasti na področju varnosti in obrambe. Tekma za vesolje kot strateško področje je vse večja, pomen vesolja za varnost pa se je povečal zlasti po ruski invaziji na Ukrajino. Marca 2023 je bila sprejeta vesoljska strategija EU za varnost in obrambo, da bi se okrepili naša strateška drža in avtonomija v vesolju. Kot ključni ukrep, ki izhaja iz te strategije, bo Evropska komisija leta 2024 predlagala vesoljsko pravo EU, ki bo urejalo varnost, trajnostnost in odpornost/varnost vesoljskih dejavnosti v EU.

V zvezi z zunanjo razsežnostjo je varna infrastruktura temelj odpornosti svetovnega gospodarstva in dobavnih verig[10], zato strategija EU Global Gateway vključuje močno varnostno razsežnost. Prav tako je glede na medsebojne povezave med infrastrukturo EU in partnerskih držav nadaljnje mednarodno sodelovanje bistveno za krepitev globalne kibernetske odpornosti ter podporo svobodnemu, odprtemu, varnemu in zanesljivemu kibernetskemu prostoru.

---

6 C(2023) 4878.

7 Priporočilo Sveta z dne 8. decembra 2022 o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.

8 COM(2023) 526.

9 Sklepi Sveta z dne 23. maja 2022 o oblikovanju stališča Evropske unije glede kibernetskih vprašanj in poziv iz Neversa z dne 9. marca 2022 za okrepitev zmogljivosti EU na področju kibernetske varnosti.

10 JOIN(2021) 30.

Akt o kibernetski odpornosti

Zagotavljanje, da se lahko potrošniki in podjetja zanesejo na varne digitalne izdelke, je osrednjega pomena za evropsko kibernetsko varnost. Komisija je to potrebo obravnavala v predlogu akta o kibernetski odpornosti[11], ki je bil sprejet 15. septembra 2022. Z aktom bi se uvedle obvezne horizontalne zahteve glede kibernetske varnosti za izdelke z digitalnimi elementi za obdobje petih let ali njihov celotni življenjski cikel (kar koli od tega je krajše). Ustvarili bi se pogoji za oblikovanje in razvoj varnih izdelkov z digitalnimi elementi, in sicer z zagotavljanjem, da se izdelki strojne in programske opreme dajejo na trg s čim manj ranljivostmi. To bi bil ključni mejnik pri zvišanju evropskih standardov za kibernetsko varnost na vseh področjih in bi verjetno postalo mednarodna referenčna točka, ki bo industriji kibernetske varnosti v Uniji zagotovila jasne prednosti na svetovnih trgih. Evropski parlament in Svet sta svoji stališči sprejela julija 2023, pogajanja pa naj bi hitro napredovala.

Certificiranje kibernetske varnosti ima tudi ključno vlogo pri povečanju zaupanja v izdelke in storitve IKT, saj potrošnikom, podjetjem in organom omogoča sprejemanje informiranih odločitev z ustrezno ravnjo kibernetske varnosti. Delo na področju certificiranja kibernetske varnosti napreduje, pri čemer se certifikacijska shema EU za kibernetsko varnost, ki temelji na skupnih merilih, ocenjuje v postopku v odboru. Agencija Evropske unije za kibernetsko varnost (ENISA) zdaj pripravlja predlog za certifikacijsko shemo EU za varnost v oblaku (EUCS), o kateri razpravlja Evropska certifikacijska skupina za kibernetsko varnost. Intenzivno delo s strokovnjaki iz različnih sektorjev, potrošniki in ponudniki bi moralo privesti do trdnega pravnega in tehničnega pristopa, ki bi zagotavljal potrebna varnostna jamstva v skladu s pravom Unije, mednarodnimi zavezami in obveznostmi STO. Poleg tega agencija ENISA pripravlja predlogo sheme EU5G in denarnico EU za digitalno identiteto (EUIDW). Usklajena prizadevanja vseh držav članic so bistvena za povečanje splošne varnosti izdelkov, storitev in postopkov IKT.

Uredbi o informacijski varnosti in kibernetski varnosti za institucije, organe, urade in agencije EU

Uredbi, ki naj bi urejali kibernetsko in informacijsko varnost za institucije Unije in sta bili marca 2022 predlagani skupaj, sta se razvijali različno hitro. Junija lani je bil dosežen politični dogovor o uredbi o kibernetski varnosti, ki omogoča krepitev odnosa vseh institucij, organov, uradov in agencij EU do kibernetske varnosti ter odraža pomen, ki ga EU pripisuje hitremu izvajanju tega predloga. V tem primeru je zlasti zaskrbljujoče, da vzporedni predlog o informacijski varnosti, ki je bistven za dokončanje trdnega zakonodajnega okvira za institucije, organe, urade in agencije EU, napreduje nepričakovano počasi. Oba predloga bi bilo treba sprejeti pred volitvami v Evropski parlament, da bi evropska uprava postala verodostojna in odporna v sedanjih geopolitičnih razmerah. Z minimalnim sklopom pravil in standardov informacijske varnosti za vse institucije, organe, ustanove in agencije EU bi se zagotovili varnost za vse udeležene strani ter dosledna zaščita pred spreminjajočimi se grožnjami za njihove tajne in netajne podatke. Ta nova pravila bi skupaj zagotovila stabilno podlago za varno izmenjavo informacij med institucijami, organi, uradi in agencijami EU ter z državami članicami, in sicer s standardiziranimi praksami in ukrepi za zaščito pretoka informacij. Na ta način se odzivajo na več pozivov Sveta h krepitvi odpornosti institucij, organov, uradov in agencij EU ter boljši zaščiti postopka odločanja Unije pred zlonamernim vmešavanjem.

Akt o kibernetski solidarnosti

[11] COM(2022) 454.

Predlagani akt EU o kibernetski solidarnosti[12], ki ga je Komisija sprejela 18. aprila 2023, bo na podlagi že vzpostavljenega trdnega strateškega, političnega in zakonodajnega okvira dodatno izboljšal odkrivanje kibernetskih groženj, odpornost in pripravljenost na vseh ravneh ekosistema kibernetske varnosti Unije. Ti cilji bi se izvajali s tremi glavnimi ukrepi:

(1) vzpostavitvijo ***evropskega kibernetskega ščita*** za vzpostavitev in okrepitev skupnih zmogljivosti za odkrivanje in situacijsko zavedanje. Ščit bi sestavljali vsi nacionalni centri za varnostne operacije in čezmejni centri za varnostne operacije;
(2) vzpostavitvijo ***mehanizma za izredne kibernetske razmere*** za podporo državam članicam pri pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnjem okrevanju po njih. Podpora za odzivanje na incidente bi vključevala kibernetskovarnostno rezervo EU, ki bi bila na voljo tudi institucijam, organom, uradom in agencijam Unije ter tretjim državam, pridruženim programu Digitalna Evropa, če bi to določal sporazum o pridružitvi programu Digitalna Evropa;
(3) vzpostavitvijo ***evropskega mehanizma za pregledovanje kibernetskovarnostnih incidentov*** za pregled in oceno pomembnih incidentov ali incidentov velikih razsežnosti. Poročilo o pregledu po incidentih bi usklajevala in pripravila agencija ENISA.

V Svetu in Evropskem parlamentu so se začele razprave. Z zaključkom pogajanj pred koncem sedanjega mandata Evropskega parlamenta bi se močno okrepila prizadevanja za zaščito državljanov in podjetij po vsej Uniji.

Akademija EU za kibernetske veščine

Kibernetske grožnje se povečujejo, zato EU nujno potrebuje strokovnjake s spretnostmi in kompetencami za preprečevanje, odkrivanje in odvračanje kibernetskih napadov ter za obrambo EU pred njimi. Njene potrebe po delovni sili na področju kibernetske varnosti so trenutno ocenjene na 883 000 strokovnjakov, število nezasedenih delovnih mest pa se je v letu 2022 gibalo med 260 000 in 500 000. K zapolnitvi te vrzeli bi bilo treba spodbujati vse dele družbe, vendar so zlasti v letu 2022 ženske predstavljale le 20 % diplomantov na področju kibernetske varnosti in 19 % strokovnjakov za informacijsko in komunikacijsko tehnologijo. Komisija je v okviru evropskega leta spretnosti 18. aprila 2023[13] sprejela pobudo, ki so jo države članice pozdravile[14], za ustanovitev akademije za kibernetske veščine, da bi se zapolnila vrzel na področju strokovnjakov za kibernetsko varnost. Akademija za kibernetske veščine bi združila obstoječe pobude v zvezi s spretnostmi na področju kibernetske varnosti ter izboljšala usklajevanje. Komisija države članice, regionalne in lokalne organe ter evropske javne subjekte spodbuja, naj sprejmejo namenske strategije ali pobude v zvezi s spretnostmi na področju kibernetske varnosti ali spretnosti na področju kibernetske varnosti vključijo v ustrezne strategije ali pobude s širšim področjem uporabe (npr. kibernetska varnost, digitalna znanja in spretnosti, zaposlovanje itd.). Sodelovanje zasebnih deležnikov bo prav tako bistveno za zmanjšanje vrzeli v spretnostih na področju kibernetske varnosti ter s tem povezanega pomanjkanja delovne sile v Evropi.

Droni

[12] COM(2023) 209.
[13] COM(2023) 207.
[14] Sklepi Sveta z dne 22. maja 2023 o politiki EU za kibernetsko obrambo.

Še ena vse večja grožnja za javne prostore in kritično infrastrukturo je zlonamerna uporaba dronov. Incidenti, ki vključujejo drone, so postali pogostejši v Uniji in zunaj nje, rešitve za boj proti dronom pa so ključno orodje za organe kazenskega pregona in druge javne organe v Uniji, pa tudi za zasebne upravljavce kritične infrastrukture. Hkrati zakonita uporaba dronov pomembno prispeva k dvojnemu zelenemu in digitalnemu prehodu[15]. Kot je bilo napovedano v strategiji za drone 2.0, sprejeti novembra 2022, Komisija zdaj sprejema sporočilo o tem, kako preprečiti morebitne grožnje, ki jih predstavljajo droni, ki je podprto z dvema priročnikoma s praktičnimi smernicami o ključnih tehničnih vidikih[16]. Namen pobude je zagotoviti celovit in usklajen okvir politike s skupnim razumevanjem veljavnih pravil za boj proti morebitnim grožnjam dronov in se po potrebi prilagoditi hitremu tehnološkemu razvoju. Države članice in ustrezni zasebni upravljavci so pozvani, naj tesno sodelujejo s Komisijo, da bi zagotovili njeno celovito izvajanje.

Pomorska varnost in varovanje v letalstvu

Nezakonite dejavnosti, kot so piratstvo, oboroženi ropi na morju, tihotapljenje migrantov, trgovina z ljudmi, nedovoljen promet z orožjem in nedovoljen promet s prepovedanimi drogami, pa tudi terorizem, so še vedno izziv za pomorsko varnost, povečujejo pa jih spreminjajoče se grožnje, vključno s hibridnimi in kibernetskimi napadi. Komisija in visoki predstavnik sta 10. marca 2023 sprejela skupno sporočilo o posodobitvi strategije EU za pomorsko varnost[17], ki bi jo bilo zdaj treba izvajati v skladu s posodobljenim akcijskim načrtom.

Na področju varovanja v letalstvu je Komisija 2. februarja 2023 sprejela delovni dokument služb Komisije Prizadevanja za okrepljeno in odpornejšo politiko za varovanje v letalstvu[18], ki vsebuje ambiciozen program za (1) posodobitev regulativne strukture za varovanje v letalstvu, (2) spodbujanje razvoja in uvajanja inovativnejših rešitev ter (3) posodobitev izhodišča za varovanje v letalstvu, da bodo lahko letališča v Uniji v celoti izkoristila nove in najsodobnejše tehnologije za obravnavanje najbolj prednostnih groženj. V dveh letih je treba izvesti štirinajst vodilnih ukrepov.

Komisija Evropski parlament in Svet poziva, naj v vsakem primeru pred koncem mandata sedanjega Evropskega parlamenta nujno zaključita pogajanja o:

- predlogu akta o kibernetski odpornosti,
- predlogu akta o kibernetski solidarnosti,
- predlagani uredbi o informacijski varnosti v institucijah, organih, uradih in agencijah EU.

Komisija države članice poziva, naj:

- si prizadevajo za prednostni prenos direktive o odpornosti kritičnih subjektov in stresno testiranje kritične infrastrukture v energetskem sektorju,
- sprejmejo priporočilo Sveta o načrtu za usklajeno odzivanje na motnje na kritični infrastrukturi z velikim čezmejnim pomenom,
- v celoti in nujno prenesejo direktivo NIS 2 za okrepitev kibernetske varnosti bistvenih in pomembnih subjektov,

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

- dejavno sodelujejo pri izvajanju ocen tveganja kibernetske varnosti ter oblikovanju scenarijev tveganja za kritično infrastrukturo in dobavne verige,
- sprejmejo nadaljnje ukrepe v zvezi z akademijo za kibernetske veščine z močnim sodelovanjem na evropski ravni in namenskimi nacionalnimi strategijami ali pobudami v zvezi s spretnostmi na področju kibernetske varnosti, pri čemer naj sodelujejo ključni deležniki, vključno z regionalnimi in lokalnimi organi,
- sodelujejo z ustreznimi zasebnimi upravljavci in Komisijo, da se zagotovi izvajanje vseh ukrepov, navedenih v sporočilu o preprečevanju morebitnih groženj, ki jih predstavljajo droni,
- izvajajo akcijski načrt strategije EU za pomorsko varnost in redno poročajo o dosežkih,
- izvedejo 14 vodilnih ukrepov, opredeljenih za izboljšanje varovanja v letalstvu.

III. Obravnavanje spreminjajočih se groženj

Nove geopolitične napetosti so jasno pokazale, kako se varnostni izziv za EU ne le povečuje, temveč je vse bolj nestanoviten, še bolj pa se krepi zaradi hibridne narave številnih groženj. Varnost se mora odzivati tudi na spremembe v družbi in tehnologiji. Zaradi pandemije COVID-19 so se povečale priložnosti za storilce kaznivih dejanj kibernetske kriminalitete, zlasti pa se je povečala grožnja posnetkov spolne zlorabe otrok na spletu. Storilci kaznivih dejanj in zlonamerni akterji so vedno pripravljeni izkoristiti tehnološki razvoj. Zaradi takih pogosto zapletenih in večdimenzionalnih groženj je potrebno odločno in dosledno ukrepanje EU.

Uredba o boju proti spolni zlorabi otrok na spletu

Iz Europolove ocene ogroženosti zaradi internetnega organiziranega kriminala je razvidno, da sta se v letu 2022 pogostost in resnost spolnega izkoriščanja in zlorabe otrok še povečali, storilci kaznivih dejanj pa še naprej izkoriščajo tehnične možnosti za prikrivanje svojih dejanj in identitet[19]. Sedanji sistem, ki temelji na prostovoljnem odkrivanju in prijavljanju s strani podjetij, se je izkazal za nezadostnega za zaščito otrok. Začasna uredba podjetjem omogoča prostovoljno odkrivanje in poročanje, če je to zakonito na podlagi splošne uredbe o varstvu podatkov. Začasna uredba bo prenehala veljati avgusta 2024. Komisija je maja 2022 predlagala uredbo[20] za obravnavo zlorabe spletnih storitev za namene spolne zlorabe otrok. Predlagani okvir močno poudarja preprečevanje. Podjetja bi morala oceniti tveganje spolne zlorabe otrok prek njihovih sistemov in sprejeti preventivne ukrepe. Kot skrajni ukrep bi lahko nacionalna sodišča ali neodvisni upravni organi ponudnikom storitev izdali ciljno usmerjene odredbe o zaznavanju, in sicer izključno v primeru znatnega tveganja. Novi neodvisni Center EU bi olajšal prizadevanja ponudnikov storitev, ki bi delovali kot vozlišče strokovnih izkušenj, zagotavljali zanesljive informacije o identificiranih posnetkih, prejemali in analizirali prijave spolne zlorabe otrok na spletu, ki jih vložijo ponudniki, da bi odkrili napačne naznanitve, ter zagotavljali podporo žrtvam. Bistveno je, da se nova pravila sprejmejo in začnejo izvajati čim prej, da bi otroke zaščitili pred nadaljnjo zlorabo, preprečili ponovno pojavljanje posnetkov na spletu in

[19] Europol (2023), „Internet Organised Crime Threat Assessment (IOCTA) 2023“ (Ocena ogroženosti zaradi internetnega organiziranega kriminala (IOCTA) 2023).

[20] COM(2022) 209.

storilce kaznivih dejanj privedli pred sodišče. V Svetu in Parlamentu potekajo pogajanja, da bi dogovor o zadevi dosegli pred koncem mandata Parlamenta.

Direktiva o boju proti nasilju nad ženskami in nasilju v družini

Kibernetsko nasilje nad ženskami, tudi v okviru nasilja v družini, se je začelo pojavljati kot nova oblika tovrstnega nasilja, ki se po internetu in z orodji IT širi prek meja posamezne države članice. Komisija je marca 2022 predlagala direktivo za obravnavanje nasilja nad ženskami in nasilja v družini, vključno s posebnimi pravili o kibernetskem nasilju in ukrepi za zapolnitev vrzeli pri zaščiti, dostopu do pravnega varstva in preprečevanju. Zgodnje sprejetje in izvajanje bi državam članicam zagotovilo dodatna orodja za boj proti tej obliki kaznivih dejanj. Sozakonodajalca sta julija 2023 začela medinstitucionalna pogajanja, ki naj bi jih zaključila pred koncem sedanjega mandata Evropskega parlamenta.

Kibernetska varnost omrežij 5G

Varnost omrežij 5G je pomembna prednostna naloga Komisije in bistven element njene strategije za varnostno unijo. Omrežja 5G so osrednja infrastruktura, ki zagotavlja temelje za širok nabor storitev, ki so bistvene za delovanje notranjega trga ter za ključne družbene in gospodarske funkcije. Organi držav članic EU, zastopani v Skupini za sodelovanje na področju varnosti omrežij in informacij, so 15. junija 2023 ob podpori Komisije in agencije ENISA objavili drugo poročilo o napredku pri izvajanju nabora orodij EU za kibernetsko varnost omrežij 5G. Glede na poročilo je 24 držav članic sprejelo ali pripravlja zakonodajne ukrepe, ki nacionalnim organom dajejo pooblastila za ocenjevanje dobaviteljev in izdajanje omejitev, deset držav članic pa je take omejitve uvedlo. Vendar so potrebni nadaljnji ukrepi, da bi se preprečile ranljivosti za Unijo kot celoto, ki bi lahko imele resne negativne učinke na varnost posameznih uporabnikov in podjetij po vsej Uniji ter na kritično infrastrukturo Unije. Vse države članice morajo nemudoma začeti izvajati nabor orodij. Istega dne je Komisija sprejela sporočilo o izvajanju nabora orodij v državah članicah ter lastnih korporativnih komunikacijah in dejavnostih financiranja Unije. V njem je bila poudarjena velika zaskrbljenost zaradi tveganj za varnost EU, ki jih predstavljata ponudnika opreme za mobilna omrežja Huawei in ZTE. V zvezi s tem Komisija sprejema ukrepe za preprečevanje izpostavljenosti njenih korporativnih komunikacij mobilnim omrežjem, ki kot ponudnika uporabljajo podjetji Huawei in ZTE. Javna naročila bodo izključevala nove storitve povezljivosti, ki so odvisne od opreme navedenih ponudnikov, Komisija pa bo sodelovala z državami članicami in telekomunikacijskimi operaterji, da bi zagotovila postopno opuščanje obstoječih storitev povezljivosti navedenih ponudnikov na lokacijah Komisije. Komisija preučuje tudi, kako to odločitev upoštevati v ustreznih programih in instrumentih financiranja Unije ob popolnem spoštovanju prava Unije.

Dostop do podatkov za učinkovit kazenski pregon

V sedanji digitalni dobi ima skoraj vsako kaznivo dejanje digitalni element. Tehnologije in orodja se uporabljajo tudi v kriminalne namene, vključno s tistimi, ki so potrebni za zagotavljanje kibernetske varnosti, varstva podatkov in zasebnosti naše družbe. Zato je vedno težje ohraniti učinkovit kazenski pregon po vsej EU za zaščito javne varnosti ter preprečevanje, odkrivanje, preiskovanje in pregon kaznivih dejanj. Čeprav so bila na ravni Unije in nacionalni ravni izvedena znatna prizadevanja, tudi z zakonodajo ter krepitvijo zmogljivosti in pobudami za inovacije, še vedno obstajajo pravni in tehnični izzivi. Komisija je skupaj s predsedstvom Sveta ustanovila skupino na visoki ravni o dostopu do podatkov za učinkovit kazenski pregon, da bi zagotovila platformo za sodelovanje širokega nabora deležnikov in strokovnjakov, ki bodo preučevali izzive, s katerimi se spoprijemajo strokovnjaki na področju kazenskega pregona (npr. šifriranje, hramba podatkov, omrežja 5G in standardizacija). Komisija pričakuje, da bo skupina na visoki ravni do junija 2024 oblikovala uravnotežena, trdna in uresničljiva

priporočila, ki bodo odražala zapletenost teh vprašanj, tudi z vidika kibernetske varnosti in varstva podatkov. Države članice in sodelujoči strokovnjaki se zato spodbujajo, naj dejavno sodelujejo v tem procesu ter si prizadevajo za učinkovite, zakonite in splošno sprejete rešitve.

Hibridne grožnje

Strateški kompas EU za varnost in obrambo[21] (strateški kompas) je v geopolitičnih razmerah, v katerih hibridne grožnje postajajo vse bolj zapletene in napredne, zagotovil skupno oceno groženj in izzivov, s katerimi se spoprijema Unija, ter strateški akcijski načrt. S povečanjem zlonamernega ravnanja držav in nedržavnih akterjev v kibernetskem prostoru, tudi v okviru vojne proti Ukrajini, se je še bolj poudarilo, da je kibernetski prostor področje zunanje in varnostne politike. Zaradi morebitnih tveganj zlonamernih dejanj in dezinformacij je potrebna posebna pozornost v volilnih obdobjih, med drugim pred evropskimi volitvami leta 2024.

Glede na velika tveganja učinkov prelivanja EU še naprej razvija dejavnosti za krepitev kibernetskih zmogljivosti in spodbuja partnerstva s tretjimi državami, tudi z namenskimi kibernetskimi dialogi, da bi dejavno prispevala k svoji splošni odpornosti. Razvita, revidirana in okrepljena so bila številna orodja za povečanje sposobnosti Unije za učinkovito obravnavanje hibridnih groženj, kot je opisano v sedmem poročilu o napredku glede hibridnih groženj, objavljenem 14. septembra 2023[22]. Med njimi so:

- nabor orodij EU za odzivanje na hibridne grožnje, da se zagotovi okvir za usklajen in dobro informiran odziv na hibridne grožnje in kampanje,
- tekoče delo za ustanovitev skupin za hitro odzivanje na hibridne grožnje v EU za kratkoročno prilagojeno podporo državam članicam, partnerskim državam ter misijam in operacijam skupne varnostne in obrambne politike (SVOP),
- revidirani protokol EU za preprečevanje hibridnih groženj (EU Playbook)[23], v katerem so opisani procesi in strukture Unije, ki obravnavajo hibridne grožnje in kampanje,
- revidirane izvedbene smernice okvira za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti[24] (zbirka orodij za kibernetsko diplomacijo), ki omogoča razvoj trajnostnih, prilagojenih, skladnih in usklajenih strategij za boj proti vztrajnim akterjem kibernetskih groženj,
- nabor orodij za obravnavo tujega manipuliranja z informacijami in vmešavanja za okrepitev obstoječih orodij Unije za preprečevanje tujega manipuliranja z informacijami in vmešavanja, odvračanje od njega ter odzivanje nanj,
- politika EU za kibernetsko obrambo[25] za okrepitev zmogljivosti EU za kibernetsko obrambo, izboljšanje situacijskega zavedanja in usklajevanje vseh razpoložljivih obrambnih možnosti, da bi se okrepila odpornost, odzivalo na kibernetske napade ter zagotovili solidarnost in medsebojna pomoč.

Države članice se zato spodbujajo, naj nadaljujejo in okrepijo sodelovanje na tem področju, tako da zagotovijo učinkovito izvajanje zgoraj navedenih orodij, tudi z rednimi dejavnostmi, in dosežejo dogovor o konceptu skupin za hitro odzivanje na hibridne grožnje, ki bodo zagotavljal smernice za nadaljnje ukrepe pri ustanavljanju skupin.

Umetna inteligenca v okviru kazenskega pregona

[21] Dokument Sveta 7371/22.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] Dokument Sveta 10289/23 z dne 8. junija 2023.
[25] JOIN(2022) 49.

Umetna inteligenca je hitro postala splošna značilnost vsakdanjega življenja. Učinki uporabe umetne inteligence na kibernetsko kriminaliteto in kibernetsko varnost še niso v celoti znani, vendar bodo nedvomno pomenili nove izzive. Čeprav lahko umetna inteligenca prinese koristi, če se uporablja varno in nadzorovano, ima lahko v rokah zlonamernih akterjev nevaren potencial, vključno s pomočjo storilcem kaznivih dejanj pri prikrivanju njihove identitete pri kaznivih dejanjih, kot sta terorizem in spolna zloraba otrok. Zato je ključnega pomena, da organi sledijo razvoju dogodkov ter tako preprečujejo zlorabe in se odzivajo nanje[26]. Cilj pogajanj o predlaganem aktu o umetni inteligenci je obravnavati ta vprašanja, ki so prešla v ključno fazo, pri čemer sozakonodajalca zdaj razpravljata o tehničnih in političnih vprašanjih, ki bodo določala interakcijo s to tehnologijo v prihodnjih letih. Bistveno bo poiskati uravnotežene rešitve, zlasti v zvezi z uporabami z visokim tveganjem, tudi na področju kazenskega pregona.

Komisija Evropski parlament in Svet poziva, naj v vsakem primeru pred koncem mandata sedanjega Evropskega parlamenta nujno zaključita medinstitucionalna pogajanja o naslednjih nerešenih zadevah:

- predlogu uredbe o boju proti spolni zlorabi otrok na spletu,
- predlogu direktive o boju proti nasilju nad ženskami in nasilju v družini,
- predlogu uredbe o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci).

Komisija države članice poziva, naj:

- nemudoma začnejo v celoti izvajati nabor orodij EU za kibernetsko varnost omrežij 5G,
- podpirajo delo skupine na visoki ravni o dostopu do podatkov za učinkovit kazenski pregon, da bi se oblikovala jasna, trdna in uresničljiva priporočila za sorazmerno obravnavanje sedanjih in pričakovanih izzivov,
- v sodelovanju z visokim predstavnikom sprejmejo ukrepe za zagotovitev učinkovitega izvajanja nabora orodij EU za odzivanje na hibridne grožnje, revidirane zbirke orodij za kibernetsko diplomacijo ter nabora orodij za obravnavo tujega manipuliranja z informacijami in vmešavanja, med drugim z rednimi dejavnostmi in ob upoštevanju svetovne dinamike,
- dosežejo dogovor o konceptu skupin za hitro odzivanje na hibridne grožnje.

IV. Zaščita Evropejcev in Evropejk pred terorizmom in organiziranim kriminalom

Tveganje, da bi svetovni ali lokalni dogodki povzročili nove izbruhe terorizma, je vedno prisotno. Hkrati sta organizirani kriminal in nedovoljen promet s prepovedanimi drogami med najresnejšimi grožnjami za varnost EU. Za okrepitev skupnih prizadevanj Unije v boju proti tem grožnjam poteka skupno delo pri izvajanju strategije EU za boj proti organiziranemu kriminalu[27], strategije EU za boj proti trgovini z ljudmi[28], agende in akcijskega načrta EU za

[26] Glej na primer poročilo Europola, objavljeno 17. aprila 2023, „ChatGPT - the impact of Large Language Models on Law Enforcement“ (ChatGPT – vpliv obsežnih jezikovnih modelov na kazenski pregon).
[27] COM(2021) 170.
[28] COM(2021) 171.

boj proti drogam[29] ter agende EU za boj proti terorizmu[30]. Da pa bi se odzvali na zaskrbljujoče slabšanje razmer na področju organiziranega kriminala in nedovoljenega prometa s prepovedanimi drogami, je treba dodatno okrepiti delo držav članic in EU, da bi se okrepil naš skupni odziv na kriminalne mreže in da bi se bolje zaščitile žrtve kaznivih dejanj, hkrati s tem poročilom pa je objavljen tudi načrt EU za boj proti nedovoljenemu prometu s prepovedanimi drogami in organiziranemu kriminalu[31].

EU na področju boja proti terorizmu krepi tudi svoj zunanji nabor orodij[32], tako da v celoti izkorišča dialoge na visoki ravni o boju proti terorizmu in mrežo strokovnjakov za boj proti terorizmu/varnost v delegacijah EU, pa tudi s sodelovanjem v večstranskih forumih, med drugim kot sopredsedujoča Globalnemu forumu za boj proti terorizmu.

Nedovoljen promet s prepovedanimi drogami

Z novim mandatom Evropskega centra za spremljanje drog in zasvojenosti z drogami, ki se bo začel julija 2024, bo EU bolje opremljena za reševanje zapletenega varnostnega in zdravstvenega problema, ki vpliva na več milijonov ljudi v EU in po svetu. Komisija pregleduje[33] tudi uredbi o predhodnih sestavinah za prepovedane droge[34], da bi obravnavala glavne izzive, opredeljene v oceni iz leta 2020[35], v kateri je bilo poudarjeno, da je treba obravnavati izzive, ki jih predstavljajo predhodne sestavine za dizajnerske droge[36], da bi se zmanjšala ponudba prepovedanih drog.

Vendar pa je treba zaradi doslej največjega povečanja prepovedanih drog, ki so na voljo v Evropi, boj proti nedovoljenemu prometu s prepovedanimi drogami okrepiti v sodelovanju z mednarodnimi partnerji. Za razbitje kriminalnih mrež in boljšo zaščito žrtev kaznivih dejanj so potrebni dodatni ukrepi držav članic in EU. Komisija je zdaj predstavila načrt EU za boj proti nedovoljenemu prometu s prepovedanimi drogami in organiziranemu kriminalu. V njem je določenih 17 ukrepov na štirih prednostnih področjih: okrepitev odpornosti logističnih vozlišč z evropsko zvezo pristanišč, razbitje kriminalnih mrež, povečanje prizadevanj za preprečevanje in okrepitev sodelovanja z mednarodnimi partnerji. Ti ukrepi se bodo izvajali v letih 2024 in 2025.

Strelno orožje

Nedovoljeni promet s strelnim orožjem prispeva k organiziranemu kriminalu v EU in njeni soseščini. Ocenjuje se, da imajo civilisti v EU kar 35 milijonov kosov nedovoljenega strelnega orožja, približno 630 000 kosov strelnega orožja pa je v Schengenskem informacijskem sistemu zavedenih kot ukradenih ali izgubljenih. S hitro dostavo paketov in razvojem novih tehnologij, kot je 3D-tiskanje, se pojavljajo nove oblike nedovoljenega prometa s strelnim orožjem, ki omogočajo izogibanje nadzoru. Zaradi ruske vojne agresije proti Ukrajini se je povečalo tudi tveganje širjenja strelnega orožja. Komisija je oktobra 2022 sprejela predlog za posodobitev

[29] COM(2020) 606.
[30] COM(2020) 795.
[31] COM(2023) 641.
[32] Kot je bilo pozvano v strateškem kompasu in sklepih Sveta o obravnavi zunanje razsežnosti nenehno spreminjajoče se grožnje terorizma in nasilnega ekstremizma, sprejetih junija 2022.
[33] Predhodne sestavine za prepovedane droge – zakonodaja EU (revidirana pravila) (europa.eu).
[34] Uredba (ES) št. 273/2004 o predhodnih sestavinah pri prepovedanih drogah in Uredba Sveta (ES) št. 111/2005 o določitvi pravil za nadzor trgovine s predhodnimi sestavinami za prepovedane droge med Unijo in tretjimi državami.
[35] COM(2020) 768.
[36] Ukrep 23 akcijskega načrta za boj proti drogam (COM(2020) 606).

obstoječe zakonodaje o uvozu, izvozu in tranzitu civilnega strelnega orožja, da bi odpravila vrzeli v obstoječih pravilih, zaradi katerih se lahko poveča število strelnega orožja, pretihotapljenega in preusmerjenega v EU[37]. Srednjeročno bodo ta nova pravila pripomogla k zmanjšanju tveganja za izogibanje embargom pri izvozu strelnega orožja za civilno uporabo in povečanju nadzora nad uvozom takšnega strelnega orožja iz tretjih držav. Sozakonodajalca morata še sprejeti svoji stališči o tej zadevi, da bi se dogovor o njej dosegel pred koncem mandata sedanjega Parlamenta.

Trgovina z ljudmi

Trgovina z ljudmi je posebno huda oblika organiziranega kriminala in huda kršitev temeljnih pravic. Ljudje so žrtve trgovine z ljudmi v EU predvsem zaradi spolnega izkoriščanja in izkoriščanja delovne sile, pa tudi zaradi prisilnega prosjačenja in kriminalitete ter drugih oblik. Komisija je decembra 2022 predlagala spremembo direktive o boju proti trgovini z ljudmi[38] s posodobljenimi pravili za odpravo pomanjkljivosti sedanjega pravnega okvira. Z revidirano direktivo bi se po njenem sprejetju na področje uporabe direktive dodale pod prisilo sklenjene zakonske zveze in nezakonite posvojitve ter uvedlo izrecno sklicevanje na spletno razsežnost trgovine z ljudmi. Vanjo bi se vključil tudi obvezen režim sankcij za storilce kaznivih dejanj, formalizirala pa bi se vzpostavitev nacionalnih mehanizmov za napotitev, da bi se izboljšala zgodnje odkrivanje in čezmejna napotitev za pomoč in podporo žrtvam. Zavestna uporaba storitev, ki jih ponujajo žrtve trgovine z ljudmi, bi postala kaznivo dejanje, letno zbiranje podatkov o trgovini z ljudmi, ki jih objavi Eurostat, pa bi postalo obvezno. Svet je splošni pristop sprejel junija 2023, Evropski parlament pa stališča še ni sprejel. Da bi dogovor dosegli pred koncem mandata sedanjega Parlamenta, bo potrebno hitro ukrepanje.

Okoljska kriminaliteta

Okoljska kriminaliteta je postala svetovna grožnja, ki se po ocenah vsako leto poveča za 5 do 7 %. Velik dobiček, ki ga je mogoče ustvariti, pravne vrzeli med državami članicami in majhno tveganje odkrivanja privabljajo organizirani kriminal. Po podatkih Europola obstajajo znaki, da se prihodki iz teh dejavnosti uporabljajo za financiranje terorizma. Komisija je decembra 2021 sprejela predlog za nadomestitev direktive o kazenskopravnem varstvu okolja iz leta 2008. Predlog je osredotočen na izpopolnitev in posodobitev opredelitev kategorij okoljske kriminalitete ter opredelitev učinkovitih, odvračilnih in sorazmernih vrst ter ravni sankcij za fizične in pravne osebe. Nova kazniva dejanja vključujejo kazniva dejanja, povezana z nezakonitim krčenjem gozdov, kršitvami zakonodaje EU o kemikalijah, nezakonitim zajemom površinske ali podzemne vode in nezakonitim recikliranjem ladij. Cilj predloga je znatno okrepiti verigo kazenskega pregona in čezmejno sodelovanje med organi držav članic ter agencijami in organi EU. Evropski parlament in Svet sta sprejela svoji stališči o predlogu in sta v postopku pogajanj, ki bi se lahko zaključila do konca leta. Za nadaljnjo okrepitev preprečevanja in izvrševanja je potrebno izvajanje revidiranega akcijskega načrta[39] za boj proti nezakoniti trgovini s prostoživečimi vrstami.

Povrnitev in odvzem sredstev

Odvzem nezakonitih prihodkov storilcem kaznivih dejanj je ključnega pomena za razbitje organiziranega kriminala. Zato je Komisija maja 2022 poleg predloga, ki organom kazenskega

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

pregona omogoča dostop do informacij o bančnih računih po vsej EU[40] (v zvezi s katerim je bil junija 2023 dosežen politični dogovor), predstavila predlog o povrnitvi in odvzemu sredstev[41], da bi se okrepile zmogljivosti za sledenje, identifikacijo, zamrznitev, zaplembo in upravljanje sredstev. Ključne določbe predloga se nanašajo na zahteve za finančne preiskave ter dodatna pooblastila in orodja uradov za odvzem premoženjske koristi, pa tudi na učinkovitejše ukrepe zamrznitve in zaplembe za razširjen sklop kaznivih dejanj. Eno od novih kaznivih dejanj, za katera bi se ti ukrepi uporabljali, je kršitev omejevalnih ukrepov Unije. Komisija je decembra 2022 sprejela ločen predlog za uskladitev kazenskopravnih opredelitev kršitev omejevalnih ukrepov Unije in kazni zanje. Učinkovito izvajanje in izvrševanje omejevalnih ukrepov Unije ostaja glavna prednostna naloga Komisije, ki jo krepi delo projektne skupine „Freeze and Seize“, ki jo je ustanovila Komisija v odziv na rusko vojno agresijo proti Ukrajini. Glede obeh predlogov sta Evropski parlament in Svet sprejela svoji stališči, da bi se do konca tega leta dosegel dogovor.

Sveženj o preprečevanju pranja denarja

Pranje denarja je povezano s skoraj vsemi kriminalnimi dejavnostmi, ki ustvarjajo premoženjsko korist, pridobljeno s kaznivim dejanjem, v EU[42], in je zato ključni vzvod za boj proti kriminalu v EU. Komisija je julija 2021 predstavila ambiciozne predloge za okrepitev ukrepov EU za preprečevanje pranja denarja in financiranja terorizma[43], in sicer s štirimi zakonodajnimi predlogi za okrepitev preprečevanja in odkrivanja poskusov pranja nezakonito pridobljene premoženjske koristi ali financiranja terorističnih dejavnosti s strani storilcev kaznivih dejanj prek finančnega sistema. Sozakonodajalca sta maja 2023 sprejela eno od štirih pobud iz svežnja, da bi se zagotovila sledljivost prenosov kriptosredstev[44]. Navedena uredba se bo začela uporabljati 30. decembra 2024, pri čemer bodo morali do takrat vsi ponudniki storitev v zvezi s kriptosredstvi zbirati in hraniti informacije o originatorju in upravičencu v zvezi s prenosi kriptosredstev. Cilj preostalih treh predlogov je (i) ustanoviti nov organ EU za preprečevanje pranja denarja, da se zagotovi dosleden visokokakovosten nadzor na celotnem notranjem trgu, vključno z najbolj tveganimi čezmejnimi subjekti, pri čemer bo podpiral in usklajeval delo finančnoobveščevalnih enot, (ii) določiti usklajena pravila za zasebni sektor, vključno z uvedbo vseevropske omejitve 10 000 EUR za velika gotovinska plačila v zameno za storitve in blago, ter (iii) okrepiti pooblastila in orodja za sodelovanje pristojnih organov. Pričakuje se, da se bo s tem svežnjem znatno izboljšala sposobnost EU za boj proti pranju denarja ter zaščito državljanov EU pred terorizmom in organiziranim kriminalom. O treh še nerešenih predlogih zdaj potekajo pogajanja med sozakonodajalcema, da bi se dogovor o tej zadevi dosegel pred koncem mandata sedanjega Parlamenta.

Komisija Evropski parlament in Svet poziva, naj v vsakem primeru pred koncem mandata sedanjega Evropskega parlamenta nujno zaključita medinstitucionalna pogajanja o naslednjih nerešenih zadevah:

- predlogu direktive o povrnitvi in odvzemu sredstev,
- predlogu direktive za uskladitev kazenskopravnih opredelitev kršitev omejevalnih ukrepov Unije in kazni zanje,

[40] COM(2021) 429.
[41] COM(2022) 245.
[42] Europol, „Enterprising criminals – Europe’s fight against the global networks of financial and economic crime“ (Domiselni storilci kaznivih dejanj: evropski boj proti svetovnim mrežam finančnega in gospodarskega kriminala), 2020.
[43] COM(2021) 420.
[44] Uredba (EU) 2023/1113 z dne 31. maja 2023 o informacijah, ki spremljajo prenose sredstev in nekaterih kriptosredstev, in spremembi Direktive (EU) 2015/849.

- predlogu direktive o boju proti trgovini z ljudmi,
- predlogu direktive o izboljšanju varstva okolja s kazenskim pravom,
- predlogu svežnja o preprečevanju pranja denarja,
- predlogu za posodobitev obstoječe zakonodaje o uvozu, izvozu in tranzitu civilnega strelnega orožja.

Komisija države članice, agencije in organe EU poziva k
- sodelovanju pri izvajanju 17 ukrepov iz načrta EU za boj proti nedovoljenemu prometu s prepovedanimi drogami in organiziranemu kriminalu v letih 2023 in 2024.

V. Močan evropski varnostni ekosistem

V zadnjih letih postaja narava varnostnih groženj vse bolj čezmejna, kar zahteva nadaljnje sinergije in tesnejše sodelovanje na vseh ravneh. Od sprejetja strategije za varnostno unijo so bile sprejete pomembne pobude za čim večje čezmejno sodelovanje ter racionalizacijo in nadgradnjo razpoložljivih instrumentov in postopkov na zunanjih mejah in na schengenskem območju, pa tudi za okrepitev izmenjave informacij med organi kazenskega pregona in pravosodnimi organi za boljši boj proti organiziranemu kriminalu. Glede na navedeno je učinkovito izvajanje okvira interoperabilnosti za izmenjavo podatkov pomemben steber za povečanje varnosti in učinkovitega evropskega odziva na čezmejne grožnje ob hkratnem zagotavljanju prostega gibanja znotraj Unije.

Boljša izmenjava informacij na schengenskem območju: predhodne informacije o potnikih (podatki API), evidence podatkov o potnikih (podatki PNR) in okvir Prüm II

S predlogoma o podatkih API, ki ju je Komisija sprejela decembra 2022[45] , bi se povečala notranja varnost Unije, saj bi se organom kazenskega pregona držav članic zagotovila dodatna orodja za boj proti hudim kaznivim dejanjem in terorizmu. Zlasti bi predhodne informacije o potnikih na letih znotraj EU, ki se uporabljajo skupaj s podatki PNR letalskih potnikov, organom kazenskega pregona držav članic omogočile, da z bolj ciljno usmerjenimi ukrepi znatno povečajo učinkovitost svojih posredovanj. Pomembno je, da se predlagana pravila sprejmejo čim prej, saj se s tem ne bi le podprl boj proti organiziranemu kriminalu in terorizmu, temveč bi se tudi znatno zmanjšala potreba po sistematičnih kontrolah vseh potnikov v primeru začasne ponovne uvedbe kontrol na notranjih mejah, kar bi olajšalo zračni promet in prosto gibanje. Evropska komisija je 6. septembra 2023 Svetu priporočila, naj odobri pogajanja s Švico, Islandijo in Norveško o sporazumih o prenosu podatkov PNR. Sprejetje teh treh priporočil bi pomenilo podporo dosledni in učinkoviti zunanji politiki EU o podatkih PNR.

Policija za boj proti organiziranemu kriminalu, drogam, terorizmu, spolnemu izkoriščanju in trgovini z ljudmi vsakodnevno uporablja prümske izmenjave. Predlog uredbe o avtomatizirani izmenjavi podatkov za policijsko sodelovanje (okvir Prüm II)[46] spreminja obstoječi prümski okvir, da bi se odpravile vrzeli v informacijah ter spodbudili preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v EU. Revidirana pravila o avtomatizirani izmenjavi podatkov za policijsko sodelovanje dopolnjujejo predloge za policijsko sodelovanje v tem mandatu, skupaj z že sprejetim priporočilom Sveta za okrepitev operativnega čezmejnega policijskega

[45] COM(2022) 729, COM(2022) 73.
[46] COM(2021) 784.

sodelovanja in direktivo o izmenjavi informacij med organi kazenskega pregona. S hitrim sprejetjem in izvajanjem teh povezanih instrumentov bi se izboljšala, olajšala in pospešila izmenjava podatkov med organi kazenskega pregona ter pomagalo identificirati storilce kaznivih dejanj.

Popolnoma interoperabilen sistem upravljanja meja za varno, močno, digitalno in enotno schengensko območje

Dobro delujoče schengensko območje brez notranjih meja je odvisno od medsebojnega zaupanja med državami članicami. To pa je odvisno od učinkovitih kontrol na zunanjih mejah Unije ali kot alternativni ukrep na ozemlju držav članic. Predlog spremembe zakonika o schengenskih mejah[47], ki ga je predlagala Komisija, določa, kako lahko države članice bolje izkoristijo alternative kontrolam na notranjih mejah, ki lahko zagotovijo visoko raven varnosti. Pomembno je, da se sprememba zakonika o schengenskih mejah sprejme in izvede v celoti, da se zagotovi visoka in sorazmerna raven varnosti na schengenskem območju. Še naprej se razvija tudi nova arhitektura informacijskih sistemov EU, da bi se bolje podprla prizadevanja nacionalnih organov za zagotavljanje varnosti ter upravljanja meja. To zajema prenovljen Schengenski informacijski sistem, Evropski sistem za potovalne informacije in odobritve, sistem vstopa/izstopa, posodobitev Vizumskega informacijskega sistema ter okvir interoperabilnosti za popolnoma varno povezavo sistemov. Ko bo ta nova struktura v celoti dokončana, bo nacionalnim organom zagotovila celovitejše in zanesljivejše varnostne informacije. Vsi deli okvira interoperabilnosti so bistveni, kar pomeni, da zamuda pri enem vidiku ali v eni državi članici povzroči zamudo pri uvajanju za vse. Zamude pri tehničnem razvoju sistema vstopa/izstopa bi bilo treba čim bolj zmanjšati, da bi lahko sistem vstopa/izstopa začel delovati čim prej in da bi se lahko vzpostavili vsi ključni elementi okvira interoperabilnosti.

S predlogom o preverjanju[48] bi se izboljšala varnost na schengenskem območju, in sicer z oblikovanjem enotnih pravil za identifikacijo državljanov tretjih držav, ki ne izpolnjujejo pogojev za vstop iz zakonika o schengenskih mejah, ter opravljanjem zdravstvenih pregledov in izvajanjem varnostnega preverjanja teh oseb na zunanjih mejah. Predlagani sistem Eurodac bi podprl te cilje in nakazal, kje se po preverjanju zdi, da bi lahko posameznik ogrozil notranjo varnost. To bi nato olajšalo izvajanje predlagane uredbe o upravljanju azila in migracij. Komisija sozakonodajalca spodbuja, naj hitro, tj. pred koncem sedanjega zakonodajnega obdobja, zaključita pogajanja o teh zadevah.

Boj proti korupciji

Korupcija močno škoduje našim demokracijam, gospodarstvu in naši varnosti, saj omogoča organizirani kriminal in sovražno tuje vmešavanje. Uspešno preprečevanje korupcije in boj proti njej sta bistvenega pomena za zaščito vrednot EU in učinkovitosti politik EU ter za ohranjanje pravne države in zaupanja v tiste, ki vladajo, in v javne institucije. Kot je predsednica Ursula von der Leyen napovedala v govoru o stanju v Uniji leta 2022, je Komisija 3. maja 2023 sprejela sveženj protikorupcijskih ukrepov[49]. Predlog Komisije za direktivo o boju proti korupciji vključuje strožja pravila, ki inkriminirajo dejanja korupcije in usklajujejo kazni po vsej EU. Omogoča tudi učinkovite preiskave in pregon ter daje velik poudarek na preprečevanje in ustvarjanje kulture integritete, v kateri korupcija ni dopustna. V Evropskem parlamentu in Svetu so se začele razprave o tem predlogu. Poleg tega so države članice pozvane, naj

[47] COM(2021) 891.
[48] COM(2020) 612.
[49] COM(2023) 234.

upoštevajo priporočila, ki izhajajo iz protikorupcijskega stebra poročila o stanju pravne države za leto 2023, sprejetega 5. julija 2023. V okviru predloga visokega predstavnika, ki ga je podprla Komisija, bi se vzpostavil tudi poseben režim sankcij v okviru skupne zunanje in varnostne politike (SZVP) za boj proti hudim kaznivim dejanjem korupcije po vsem svetu.

Krepitev pravic žrtev

Komisija je 12. julija 2023 predlagala spremembe direktive o pravicah žrtev, da bi se povečali dostop žrtev do informacij, podpore in zaščite, sodelovanje v kazenskem postopku in dostop do odškodnine. Eden od splošnih ciljev revizije je prispevati k visoki ravni varnosti z ustvarjanjem varnejšega okolja za žrtve, da bi se spodbudilo prijavljanje kaznivih dejanj in zmanjšali strahovi pred povračilnimi ukrepi.

Komisija Evropski parlament in Svet poziva, naj v vsakem primeru pred koncem mandata sedanjega Evropskega parlamenta nujno zaključita medinstitucionalna pogajanja o naslednjih nerešenih zadevah:

- predlogu uredbe Prüm II,
- predlogih o predhodnih informacijah o potnikih (podatkih API),
- predlogih za boj proti korupciji in zlasti za vzpostavitev posebnega režima sankcij v okviru skupne zunanje in varnostne politike (SZVP),
- predlogu spremembe uredbe o zakoniku o schengenskih mejah,
- predlogu direktive o pravicah žrtev,
- predlogu o preverjanju.

Komisija države članice poziva, naj:

- čim prej zagotovijo začetek veljavnosti sistema vstopa/izstopa, da se dokonča izvajanje strukture EU za izmenjavo informacij.

VI. Izvajanje

Zagotavljanje varnosti Evrope kot celote je skupna odgovornost in vsak akter mora izpolniti svojo vlogo, od tega, da Komisija in sozakonodajalca sprejemajo nova trdna, celovita in praktična pravila, do tega, da države članice taka pravila pravočasno prenesejo, izvedejo in uporabijo ter da različni organi, organizacije in deležniki na terenu opravljajo operativno delo. Ključno vlogo imajo tudi agencije EU na področju pravosodja, notranjih zadev in kibernetske varnosti, ki se je z nedavnimi razširitvami njihovih odgovornosti še povečala.

Okrepljeno preverjanje upravičencev do sredstev EU

Komisija mora pri izvrševanju proračuna EU zagotoviti, da upravičenci do sredstev EU spoštujejo vrednote EU. Mehanizmi in nadzorni sistemi, ki določajo, kdo je lahko upravičen do sredstev EU, so že zdaj trdni, namen pogajanj o prenovitvi finančne uredbe, ki trenutno potekajo, pa je Komisiji zagotoviti močnejša pravna sredstva za ukrepanje, če je to potrebno. Poleg tega Komisija zdaj išče načine za nadaljnjo krepitev preverjanja sedanjih in morebitnih prihodnjih upravičencev do sredstev EU, in sicer z izboljšanjem smernic o obveznostih v zvezi s spoštovanjem vrednot EU in posledicah, ki bi morale slediti kršenju vrednot EU. To bo pojasnilo odgovornosti upravičencev in tistih, ki izvajajo kontrole na ravni EU, ter je lahko vir navdiha za nacionalno raven. V primeru kršitve pogojev financiranja Komisija ne omahuje in ne bo omahovala pri ustavitvi sodelovanja z upravičenci zadevnega projekta ter po potrebi pri izterjavi sredstev. Pomembno je, da države članice proaktivno izmenjujejo informacije s

Komisijo, če se zavedajo morebitnih tveganj v zvezi z organizacijami, ki zaprosijo za sredstva EU.

Kršitve

Na področju varnosti je Komisija izvedla številne postopke za ugotavljanje kršitev. Leta 2023 je bilo na primer začetih veliko postopkov za ugotavljanje kršitev zaradi neizpolnjevanja obveznosti iz uredbe o razširjanju terorističnih spletnih vsebin iz leta 2021 (16 držav članic)[50], v letih 2022 in 2023 pa je 20 držav članic prejelo dodatne uradne opomine zaradi nepravilnega izvajanja direktive o boju proti spolni zlorabi otrok iz leta 2011[51]. Veliko število postopkov za ugotavljanje kršitev je še vedno odprtih zaradi neskladnosti nacionalne zakonodaje z direktivo o boju proti terorizmu iz leta 2017[52] in zaradi neprenosa pravil, ki olajšujejo uporabo finančnih informacij in drugih informacij za preprečevanje, odkrivanje, preiskovanje ali pregon nekaterih kaznivih dejanj[53]. Druga področja, na katerih potekajo postopki za ugotavljanje kršitev, vključujejo zakonodajo o strelnem orožju, pravila o psihoaktivnih snoveh, ki se uporabljajo v drogah, boj proti goljufijam in ponarejanju v zvezi z negotovinskimi plačilnimi sredstvi, boj proti pranju denarja, izmenjavo kazenskih evidenc med državami članicami EU in direktivo o pravicah žrtev. Državam članicam, ki izvajajo dogovorjene pobude in ukrepe, je na voljo podpora (tehnična in finančna), Komisija pa ostaja na voljo za sodelovanje z državami članicami za optimizacijo izvajanja.

Spremljanje s schengenskimi ocenjevanji in novim schengenskim sistemom upravljanja

Schengenski ocenjevalni in spremljevalni mehanizem še naprej prispeva k učinkovitemu izvajanju schengenskih pravil, namenjenih povečanju varnosti na območju brez notranjih kontrol. Leta 2023 so bila izvedena prva ocenjevanja v okviru okrepljenega schengenskega ocenjevalnega in spremljevalnega mehanizma, kar je omogočilo pravočasno prepoznavanje in odpravo strateških ranljivosti, ki imajo čezmejni učinek na zaščito in varnost v EU. Poleg tega je Komisija leta 2023 začela tematsko schengensko ocenjevanje, da bi ocenila prakse držav članic, ki se spoprijemajo s podobnimi izzivi v boju proti nedovoljenemu prometu s prepovedanimi drogami v EU, pri čemer se je zlasti osredotočila na velik obseg nedovoljenega prometa s prepovedanimi drogami. S temi ocenjevanji je bil uveden okrepljen in celovitejši poudarek na varnostnih elementih schengenskega območja. Svet je junija 2023 na podlagi rezultatov rednih, tematskih in nenapovedanih schengenskih ocenjevanj določil prednostne naloge schengenskega cikla za obdobje 2023–2024. Določena so prednostna področja, ki zahtevajo dodatno spodbudo za varnejše in močnejše schengensko območje. Učinkovito in hitro izvajanje teh prednostnih nalog skupaj z boljšim usklajevanjem politik Schengenskega sveta bo dodatno okrepilo boj proti organiziranemu kriminalu in čim bolj povečalo čezmejno operativno sodelovanje.

Vloga agencij in organov EU

Ključno za izvajanje pobud na področju varnostne unije je partnerstvo, saj je za doseganje konkretnih rezultatov potrebno delo različnih nacionalnih in evropskih organov. EMPACT (Evropska večdisciplinarna platforma proti grožnjam kriminala) na primer omogoča strukturirano večdisciplinarno sodelovanje držav članic, ki ga podpirajo vse institucije, organi

[50] Uredba (EU) 2021/784 o razširjanju terorističnih spletnih vsebin.

[51] Direktiva (EU) 2011/93 o boju proti spolni zlorabi otrok.

[52] Direktiva (EU) 2017/541 Evropskega parlamenta in Sveta z dne 15. marca 2017 o boju proti terorizmu in nadomestitvi Okvirnega sklepa Sveta 2002/475/PNZ ter o spremembi Sklepa Sveta 2005/671/PNZ.

[53] Direktiva (EU) 2019/1153 Evropskega parlamenta in Sveta z dne 20. junija 2019 o določitvi pravil za lažjo uporabo finančnih in drugih informacij za namene preprečevanja, odkrivanja, preiskovanja ali pregona nekaterih kaznivih dejanj ter o razveljavitvi Sklepa Sveta 2000/642/PNZ.

in agencije EU (kot so Europol, Frontex, Eurojust, CEPOL, OLAF in EU-LISA). Operacije, ki jih izvaja EMPACT, tudi prek namenskih operativnih projektnih skupin, usklajujejo prizadevanja držav članic in operativnih partnerjev v boju proti kriminalnim mrežam in hudim kaznivim dejanjem. Samo v letu 2022 je bilo v okviru EMPACT skupaj izvedenih 9 922 aretacij, zaseženih več kot 180 milijonov EUR sredstev in denarja, začetih 9 263 preiskav, identificiranih 4 019 žrtev, zaseženih več kot 62 ton drog, identificiranih 51 in aretiranih 12 pomembnejših obdolžencev ter izvedenih več operacij v okviru vojne agresije proti Ukrajini, zlasti za boj proti trgovini z ljudmi in grožnjam, povezanim s strelnim orožjem[54].

Agencija Frontex, Evropska agencija za pomorsko varnost (EMSA) in Evropska agencija za nadzor ribištva (EFCA) še naprej krepijo sodelovanje na področju nalog obalne straže, da bi nacionalnim organom pomagale povečati varnost in zaščito na morju. Te agencije bodo pomembno prispevale k izvajanju strategije EU za pomorsko varnost.

Več pobud na področju varnostne unije je ustreznim agencijam prineslo nove odgovornosti in naloge, ki včasih vplivajo na človeške vire.

Agencija Evropske unije za kibernetsko varnost (ENISA)

Kar zadeva pripravljenost in odzivanje na incidente za povečanje kibernetske varnosti, je Komisija vzpostavila kratkoročne ukrepe za podporo državam članicam, pri čemer je sredstva prenesla iz programa Digitalna Evropa na **Agencijo Evropske unije za kibernetsko varnost (ENISA)**, da bi okrepila pripravljenost in zmogljivosti za odzivanje na večje kibernetske incidente. Predlog akta o kibernetski solidarnosti, sprejet aprila 2023, temelji na tem ukrepu in lahko, ko ga sozakonodajalca sprejmeta, agenciji ENISA zaupa dodatne naloge, kot sta delovanje in upravljanje prihodnje rezerve Unije za kibernetsko varnost ali priprava poročila o pregledu incidentov po kibernetskih incidentih velikih razsežnosti. Predlagani akt o kibernetski odpornosti bi določal, da mora agencija ENISA od proizvajalcev prejeti obvestila o ranljivostih izdelkov z digitalnimi elementi in incidentih, ki vplivajo na varnost teh izdelkov, agencija ENISA pa bi jih morala posredovati ustreznim skupinam za odzivanje na incidente na področju računalniške varnosti ali ustreznim enotnim kontaktnim točkam držav članic. Agencija ENISA bi morala pripraviti tudi dvoletno tehnično poročilo o novih trendih glede tveganj za kibernetsko varnost pri izdelkih z digitalnimi elementi ter ga predložiti skupini za sodelovanje na področju varnosti omrežij in informacijskih sistemov.

Evropski kompetenčni center za kibernetsko varnost

Evropski kompetenčni center za kibernetsko varnost (ECCC) je skupaj z mrežo nacionalnih koordinacijskih centrov nov organ Unije za podporo inovacijam in industrijski politiki na področju kibernetske varnosti. Ta ekosistem bo okrepil zmogljivosti skupnosti za tehnologije kibernetske varnosti, ohranjal raziskovalno odličnost in krepil konkurenčnost industrije Unije na tem področju. ECCC in mreža nacionalnih koordinacijskih centrov bosta sprejemala strateške naložbene odločitve ter združevala vire Unije, njenih držav članic in posredno industrije, da bi se izboljšale in okrepile tehnološke in industrijske zmogljivosti na področju kibernetske varnosti. ECCC ima zato ključno vlogo pri uresničevanju ambicioznih ciljev na področju kibernetske varnosti iz programov Digitalna Evropa in Obzorje Evropa.

[54] Pregledi rezultatov platforme EMPACT iz leta 2022: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf.

ECCC je zaposlil več kot polovico svojega osebja in bo kmalu zaposlil izvršnega direktorja. Delo, ki že poteka, vključuje del programa DIGITAL o kibernetski varnosti ter nov strateški program[55] za razvoj in uvajanje tehnologije, ki določa prednostne ukrepe za podporo MSP pri razvoju in uporabi strateških tehnologij, storitev in procesov na področju kibernetske varnosti, podporo in rast strokovne delovne sile ter okrepitev strokovnega znanja na področju raziskav, razvoja in inovacij v širšem evropskem ekosistemu kibernetske varnosti.

Europol

Europol bo s popolnoma novim mandatom bolje opremljen za podporo državam članicam v boju proti organiziranemu kriminalu. Boj proti nedovoljenemu prometu s prepovedanimi drogami je ključna prednostna naloga zaradi njegovega vse večjega pomena in vse večjega negativnega vpliva na varnost državljanov EU. Na podlagi pooblastila Sveta Evropske unije z dne 15. maja 2023 si Komisija dejavno prizadeva za sklenitev mednarodnih sporazumov z Bolivijo, Brazilijo, Ekvadorjem, Mehiko in Perujem o izmenjavi osebnih podatkov z Europolom za preprečevanje hudih kaznivih dejanj in terorizma ter boj proti njim.

Eurojust

Eurojust je z več kot 20 leti izkušenj z zagotavljanjem pravosodne podpore nacionalnim organom v boju proti številnim hudim in zapletenim čezmejnim kaznivim dejanjem utrdil svoj položaj na območju svobode, varnosti in pravice v EU. Da bi Komisija okrepila sodelovanje na vseh področjih, se pogaja o mednarodnih sporazumih za lažje sodelovanje med Eurojustom in 13 tretjimi državami za izmenjavo osebnih podatkov v boju proti organiziranemu kriminalu in terorizmu[56]. Pogajanja z Armenijo in Libanonom so že zaključena, pogajanja z Alžirijo in Kolumbijo potekajo, začela pa so se pogajanja z Bosno in Hercegovino. Komisija Evropski parlament in Svet spodbuja, naj sporazume s temi državami skleneta pred koncem parlamentarnega obdobja, da bi se okrepilo nadnacionalno pravosodno sodelovanje in razširil boj proti čezmejnim kaznivim dejanjem.

EJT

Evropsko javno tožilstvo (EJT) se je od začetka operativnih dejavnosti junija 2021 izkazalo za močno orodje v naboru orodij Unije za preiskovanje in pregon kaznivih dejanj, ki škodijo proračunu Unije, vključno s kaznivimi dejanji, povezanimi s sodelovanjem v hudodelski združbi, kadar je poudarek na kaznivih dejanjih zoper proračun Unije. Komisija države članice, ki še niso vključene v okrepljeno sodelovanje EJT, spodbuja, naj se čim prej vključijo, da bi se uresničil celoten potencial EJT pri zaščiti denarja davkoplačevalcev EU.

EUDA

Z novim mandatom, ki sta ga sozakonodajalca sprejela junija 2023, se bo obstoječi Evropski center za spremljanje drog in zasvojenosti z drogami (EMCDDA) preoblikoval v agencijo z vsemi pristojnostmi, tj. **Agencijo Evropske unije za droge (EUDA)**, ki bo imela okrepljeno vlogo. Agencija bo lahko celoviteje ocenila nove zdravstvene in varnostne izzive, ki jih predstavljajo prepovedane droge, ter učinkoviteje prispevala k delu na ravni držav članic in mednarodni ravni. Zbiranje, analiza in razširjanje podatkov bodo še naprej glavna naloga agencije, vendar bo okrepljeni mandat agenciji omogočil tudi razvoj splošnih zmogljivosti za ocenjevanje zdravstvenih in varnostnih groženj, da bo lahko prepoznala nastajajoče grožnje, vključno z uporabo več snovi, okrepila sodelovanje prek nacionalnih kontaktnih točk in

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

[56] Te države so Alžirija, Argentina, Armenija, Bosna in Hercegovina, Brazilija, Kolumbija, Egipt, Izrael, Jordanija, Libanon, Maroko, Tunizija in Turčija.

vzpostavila mrežo laboratorijev, ki ji bodo zagotavljali forenzične in toksikološke informacije. To bo agenciji pomagalo izdajati opozorila, kadar se bodo na trgu pojavile posebej nevarne snovi, in ozaveščati o njih.

Komisija Evropski parlament in Svet poziva, naj v vsakem primeru pred koncem mandata sedanjega Evropskega parlamenta nujno zaključita medinstitucionalna pogajanja o naslednji nerešeni zadevi:

- predlogu o prenovitvi finančne uredbe.

Komisija države članice poziva, naj:

- proaktivno izmenjujejo informacije s Komisijo, če se zavedajo morebitnih tveganj v zvezi z organizacijami, ki zaprosijo za sredstva EU,
- hitro izvedejo prednostne naloge schengenskega cikla za obdobje 2023–2024 za varnejše in močnejše schengensko območje,
- obravnavajo postopke za ugotavljanje kršitev, ki so bili sproženi proti njim, da se zagotovi pravilen prenos zadevne zakonodaje.

VII. Sklep

Zadnja tri leta so zaznamovala stalna in odločna prizadevanja za uresničitev ambicij glede vzpostavitve varnostne unije za EU. Na celotnem področju varnostne politike je bil dosežen velik napredek. Zdaj so zaradi nenehno spreminjajočih se groženj potrebna stalna prizadevanja z novo motivacijo. Delo v zvezi z zakonodajnim okvirom je treba pravočasno zaključiti še pred koncem parlamentarnega obdobja spomladi 2024. Države članice so stalno odgovorne za prenos, izvajanje in uporabo novih zakonov. Za izvajanje so potrebna usklajena prizadevanja, tudi ob podpori agencij EU, in zelo pogosto vse tesnejše sodelovanje z našimi mednarodnimi partnerji.

Samo s skupnimi in odločnimi prizadevanji vseh deležnikov bomo dosegli raven varnosti in zaščite v EU, ki jo državljani pričakujejo, v sedanjih razmerah pa bi morala biti prednostna naloga vsakega akterja, da prispeva k povečanju varnosti EU.