



Vijeće
Europske unije

Bruxelles, 18. listopada 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

POP RATNA BILJEŠKA

Od: Glavna tajnica Europske komisije, potpisala direktorica Martine
DEPREZ

Datum primitka: 18. listopada 2023.

Za: Thérèse BLANCHET, glavna tajnica Vijeća Europske unije

Br. dok. Kom.: COM(2023) 665 final

Predmet: KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU o
šestom izvješću o napretku u provedbi strategije EU-a za sigurnosnu
uniju

Za delegacije se u prilogu nalazi dokument COM(2023) 665 final.

Priloženo: COM(2023) 665 final



Bruxelles, 18.10.2023.
COM(2023) 665 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU
o šestom izvješću o napretku u provedbi strategije EU-a za sigurnosnu uniju

I. Uvod

Komisija je prije tri godine donijela strategiju za sigurnosnu uniju za razdoblje 2020.–2025.¹, kojom se utvrđuju glavni prioriteti Unije u području sigurnosti. Od tada smo znatno napredovali u okviru svih četiriju stupova te strategije donošenjem ključnog zakonodavstva za razna područja, od zaštite kritičnih subjekata do jačanja kibernetičke otpornosti. Međutim, u međuvremenu se pojavljuju nove sigurnosne prijetnje u Europi i našem susjedstvu. Nedavni teroristički napadi u školi u Francuskoj i na ulicama Bruxellesa snažan su podsjetnik na hitnost daljnje prilagodbe i jačanja naše sigurnosne strukture. Opasnost koju predstavljaju kibernetički napadi i dalje raste, potaknuta i zlonamjernim akterima u aktualnim sukobima Sve je više hibridnih prijetnji, uključujući dezinformacije. Europol je utvrdio da je ruska agresija na Ukrajinu jedan od razloga značajnog porasta kibernetičkih napada na ciljeve u EU-u, pri čemu su najsnažniji napadi imali političku pozadinu i koordinirale su ih proruski orijentirane hakerske skupine². Napadi su se doveli do blokade pristupu internetu i prekida ključnih usluga kao što su energetske mreže.³

Strategija za sigurnosnu uniju osmišljena je kako bi pripremila EU da se bolje odupre novim prijetnjama. Dok se suočavamo s krizama izazvanim pandemijom i ratom, pokazalo se koliko je važan pristup iz strategije koji se odnosi na našu odlučnost u povezivanju sigurnosnog ekosustava EU-a i ukidanju strogih podjela između kibernetičke i fizičke dimenzije sigurnosti, uključujući suzbijanje organiziranog kriminala i terorizma te borbu protiv radikalizacije.

Međutim, pojačan oprez zahtijeva da neprestano tražimo nedostatke u nastojanjima da zaštitimo svoje građane. U strategiji su utvrđena prioritetna područja kojima Unija može dodatno pridonijeti kako bi poduprla države članice u jačanju sigurnosti za sve europske građane. Od njezina donošenja poduzimaju se sve u njoj navedene mjere i uključuju se nove kako bi se reagiralo na postojeće sigurnosne prijetnje.

Komisija je predstavila ukupno 36 zakonodavnih inicijativa u okviru strategije za sigurnosnu uniju. Za više od polovine tih prijedloga međuinstitucijski pregovori već su rezultirali čvrstim novim zakonodavstvom kako je opisano u tablici u Prilogu. Međutim, Europski parlament i Vijeće i dalje pregovaraju o nekoliko ključnih inicijativa koje je predložila Komisija. S obzirom na to da se trenutni parlamentarni saziv približava kraju jer se u lipnju 2024. održavaju europski izbori, nužno je brzo poduzeti radnje u pogledu preostalih dokumenata kako bi građani mogli u potpunosti imati koristi od sigurnosne unije. Ovo šesto izvješće o napretku sigurnosne unije stoga je usmjereno na pregled ključnih zakonodavnih i nezakonodavnih dokumenata o sigurnosnoj uniji koje je donijela Komisija, a za koje je potrebno poduzeti daljnje korake u smislu njihova dovršavanja i djelotvorne provedbe.

Koristi od već dogovorenog zakonodavstva EU-a osjetit će se tek kad se počne provoditi. Rad treba usmjeriti na njegovo ispravno i potpuno prenošenje, provedbu i primjenu u državama članicama. Komisija je 2023. nastavila osiguravati da se strategijom EU-a za sigurnosnu uniju

¹ COM(2020) 605.

² Distribuirani napadi uskraćivanjem usluga (DDoS): vidjeti Europolovo izvješće *Cyber-attacks: the apex of crime-as-a-service* (Kibernetički napadi: vrhunac kriminala kao usluge), 13. rujna 2023.

³ Tijekom sukoba u Ukrajini u velikoj su mjeri korišteni brisači zlonamjernog softvera kako bi se uništili podaci i sustavi koji su, primjerice, utjecali na pristup internetu za tisuće pretplatnika u EU-u, kao i veliko njemačko energetske poduzeće koje je izgubilo pristup više od 5800 vjetroturbina na daljinu. *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict* (Uloga kibernetike u ruskom ratu protiv Ukrajine: njezin utjecaj i posljedice za budućnost oružanog sukoba), studija Europskog parlamenta, rujna 2023. – PE 702.594.

postiću rezultati primjenom svojih institucionalnih ovlasti za pokretanje postupaka zbog povrede kad god države članice nisu prenijele ili su nepravilno prenijele zakonodavstvo Unije.

U ovom se izvješću sažeto navodi i kad je djelovanje država članica i/ili agencija EU-a ključno za postizanje rezultata. Agencije EU-a igraju ključnu ulogu u podupiranju provedbe inicijativa sigurnosne unije, a proteklih godina imaju sve više odgovornosti. U izvješću se navode neki od glavnih novih zadataka koji su im dodijeljeni kako bi dodatno poduprli države članice u provedbi ključnih inicijativa sigurnosne unije.

Osim toga, geopolitička situacija ukazala je na važnost vanjske sigurnosti za našu unutarnju sigurnost. Snažniji unutarnji okvir EU-a u području sigurnosti suštinski je povezan s jačim partnerstvima i suradnjom s trećim zemljama. EU mora nastaviti aktivno raditi na načinima na koje suradnja na globalnoj razini može pomoći u osiguravanju sigurnosti svojih građana.

II. Sigurnosno okruženje otporno na promjene u budućnosti

Kibernetička sigurnost i otpornost kritične infrastrukture

Unija se u okviru sigurnosne unije zalaže za djelotvornu zaštitu svih europskih građana i poduzeća na internetu i izvan njega te promicanje otvorenog, sigurnog i stabilnog kibernetičkog prostora. Porast razmjera, učestalosti i ozbiljnosti kibernetičkih incidenata velika je prijetnja funkcioniranju mrežnih i informacijskih sustava te unutarnjem tržištu. Agresivni rat Rusije protiv Ukrajine dodatno je pogoršao tu prijetnju, a trenutačne geopolitičke napetosti rastu zbog intervencija mnoštva državi bliskih, kriminalnih i haktivističkih aktera. Sabotaža plinovoda Sjeverni tok prošle je jeseni pokazala kako ključni sektori kao što su energetika, digitalna infrastruktura, promet i svemir ovise o otpornoj kritičnoj infrastrukturi. Nedavni incident s podmorskim plinovodom i podatkovnim kabelom u Estoniji i Finskoj ukazuje na potrebu za visokom razinom pripravnosti za suočavanje s takvim situacijama. Iako je uzrok štete i dalje nejasan, a istrage su u tijeku, razmjena informacija na različitim razinama između država članica i Komisije djeluje ohrabrujuće. Prekidi nisu imali neposredni učinak u smislu internetske povezivosti niti su utjecali na sigurnost opskrbe plinom na europskoj ili lokalnoj razini. To je znak postignutog napretka i pojačanih napora u pripravnosti proteklih mjeseci.

Stoga je jasan i čvrst pravni okvir ključan za osiguravanje zaštite i otpornosti te kritične infrastrukture. U tom je kontekstu ključan iskorak postignut usporednim donošenjem revidirane Direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (NIS 2)⁴ i Direktive o otpornosti kritičnih subjekata (CER)⁵, koje su stupile na snagu 16. siječnja 2023. Države članice sad se pozivaju da brzo i u potpunosti prenesu te temeljne zakonodavne akte, najkasnije do 17. listopada 2024., kako bi uspostavile čvrst okvir Unije za zaštitu kritične infrastrukture Unije od fizičkih i kibernetičkih prijetnji.

U srpnju 2023. Komisija je u delegiranoj uredbi Komisije utvrdila osnovne usluge u 11 sektora obuhvaćenih Direktivom o otpornosti kritičnih subjekata⁶. Sljedeći je korak da države članice

⁴ Direktiva (EU) 2022/2555 od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i Direktiva (EU) 2018/1972 (Direktiva NIS 2).

⁵ Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ.

⁶ C(2023) 4878.

provedu procjene rizika za te usluge. Nakon Preporuke Vijeća⁷ od 8. prosinca 2022. intenziviran je rad na testiranju otpornosti na stres kritične infrastrukture, počevši od energetskog sektora, te na jačanju suradnje s NATO-om i ključnim partnerskim zemljama. Taj je rad doveo do izvješća radne skupine EU-a i NATO-a o otpornosti kritične infrastrukture u lipnju 2023., u kojem se prikazuju trenutačne sigurnosne prijetnje koje se odnose na kritičnu infrastrukturu u četirima ključnim sektorima (energetika, promet, digitalna infrastruktura i svemir) i navode preporuke za jačanje otpornosti. Preporuke, uključujući povećanu koordinaciju, razmjenu informacija i vježbe, provodi osoblje EU-a i NATO-a u kontekstu strukturiranog dijaloga o otpornosti.

Komisija je usporedno s tim 6. rujna 2023. donijela prijedlog⁸ preporuke Vijeća o Planu za poboljšanje koordiniranog odgovora na razini EU-a na pokušaje remećenja kritične infrastrukture od znatne prekogranične važnosti. Vježba u obliku rasprave o Planu na temelju scenarija organizirana je 4. listopada 2023. kako bi se testiralo kako bi se on primijenio u praksi i pružio uvid za trenutačne pregovore o prijedlogu u Vijeću.

Nakon poziva Vijeća⁹ Komisija, visoki predstavnik i Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava (NIS) provode procjene rizika i pripremaju scenarije rizika iz perspektive kibernetičke sigurnosti. Taj je rad prvenstveno usmjeren na sektore telekomunikacija i električne energije. Uključivanje svih relevantnih agencija i mreža, civilnih i vojnih, prvi put omogućuje sveobuhvatnu i uključivu procjenu na razini Unije. Dopunit će koordinirane procjene rizika ključnih lanaca opskrbe koje se provode u okviru Direktive NIS 2 te procjene rizika i testiranje otpornosti na stres kritične infrastrukture u sektoru energetike, digitalne infrastrukture, komunikacija, prometa i svemira. U interesu koordinacije i usklađenosti te bi se aktivnosti trebale nadograđivati jedna na drugu kako bi se lakše uspostavio standardni pristup, a buduće vježbe trebale bi se temeljiti na tim aktivnostima. Uspjeh tih mjera sada će ovisiti o aktivnom sudjelovanju država članica.

Funkcioniranje gospodarstava i društava sve više ovisi o uslugama i podacima koji se odnose na svemir, posebice u području sigurnosti i obrane. Svemir kao strateško područje sve je češće predmet prijepora i njegova je važnost za sigurnost porasla, posebno nakon ruske invazije na Ukrajinu. Svemirska strategija EU-a za sigurnost i obranu donesena je u ožujku 2023. kako bi se ojačao naš strateški položaj i autonomija u svemiru. Kao ključnu mjeru koja proizlazi iz te strategije Europska komisija predložit će 2024. Akt EU-a o svemiru kojim se uređuju sigurnost, održivost i otpornost/sigurnost aktivnosti u svemiru u EU-u.

U kontekstu vanjske dimenzije sigurna infrastruktura temelj je otpornosti globalnog gospodarstva i lanaca opskrbe¹⁰ i iz tog razloga EU-ova strategija Global Gateway uključuje čvrstu sigurnosnu dimenziju. Jednako tako, s obzirom na međusobnu povezanost infrastrukture EU-a i partnerskih zemalja, nastavak međunarodne suradnje ključan je za jačanje globalne kibernetičke otpornosti i podupiranje slobodnog, otvorenog, sigurnog i zaštićenog kibernetičkog prostora.

Akt o kibernetičkoj otpornosti

⁷ Preporuka Vijeća od 8. prosinca 2022. o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture.

⁸ COM(2023) 526.

⁹ Zaključci Vijeća od 23. svibnja 2022. o razvoju položaja Europske unije u pogledu kiberprostora i poziv iz Neversa za jačanje kapaciteta EU-a za kibernetičku sigurnost od 9. ožujka 2022.

¹⁰ JOIN(2021) 30.

Za europsku kibernetičku sigurnost od temeljne je važnosti osigurati da se potrošači i poduzeća mogu osloniti na sigurne digitalne proizvode. Komisija je pokušala zadovoljiti tu potrebu u svojem prijedlogu Akta o kibernetičkoj otpornosti¹¹, donesenom 15. rujna 2022. Njime bi se uveli obvezni horizontalni zahtjevi u području kibernetičke sigurnosti za proizvode s digitalnim elementima na pet godina ili za cijelog vijeka trajanja proizvoda (ovisno o tome što je kraće). Osiguravanjem da hardverski i softverski proizvodi koji se stavljaju na tržište budu što manje ranjivi stvorili bi se uvjeti za dizajn i razvoj sigurnih proizvoda s digitalnim elementima. To bi bila ključna prekretnica u podizanju europskih standarda kibernetičke sigurnosti u svim područjima i vjerojatno će postati međunarodna referentna točka, koja omogućuje jasne prednosti za industriju kibernetičke sigurnosti u Uniji na globalnim tržištima. Europski parlament i Vijeće donijeli su svoja stajališta u srpnju 2023. i pregovori bi trebali brzo napredovati.

Važnu ulogu u jačanju povjerenja u IKT proizvode i usluge ima i certifikacija u području kibernetičke sigurnosti jer omogućuje potrošačima, poduzećima i nadležnim tijelima da donose utemeljene odluke uz odgovarajuću razinu kibernetičke sigurnosti. Rad na certifikaciji kibernetičke sigurnosti napreduje pa se tako zajednički EU-ov program certifikacije u području kibernetičke sigurnosti koji se temelji na kriterijima ocjenjuje u okviru postupka odbora. Agencija Europske unije za kibersigurnost (ENISA) trenutačno priprema prijedlog EU-ova programa certifikacije sigurnosti usluga u oblaku (EUCS), o kojem se raspravlja u Europskoj skupini za certifikaciju u području kibernetičke sigurnosti. Intenzivan rad sa stručnjacima iz raznih sektora, potrošačima i pružateljima usluga trebao bi rezultirati odgovarajućim pravnim i tehničkim pristupom koji pruža potrebna sigurnosna jamstva u skladu s pravom Unije, međunarodnim obvezama i obvezama u okviru WTO-a. Osim toga, ENISA priprema prijedlog programa EU5G i EU-ovu lisnicu za digitalni identitet (EUIDW). Usklađeni naponi svih država članica ključni su za poboljšanje ukupne sigurnosti IKT proizvoda, IKT usluga i IKT procesa.

Uredbe o informacijskoj sigurnosti i kibernetičkoj sigurnosti u institucijama, tijelima i agencijama EU-a

Uredbe za upravljanje kibernetičkom sigurnošću i informacijskom sigurnošću za institucije Unije zajedno su predložene u ožujku 2022., ali napredovale su različitim tempom. U lipnju prošle godine postignut je politički dogovor o Uredbi o kibernetičkoj sigurnosti, čime se omogućuje jačanje kibernetičke sigurnosti svih institucija, tijela, ureda i agencija EU-a i odražava važnost koju EU pridaje brzom provedbi tog prijedloga. U toj situaciji posebno zabrinjava to što usporedni prijedlog o informacijskoj sigurnosti, ključan za dovršetak čvrstog zakonodavnog okvira za institucije, tijela i agencije EU-a, neočekivano sporo napreduje. Oba bi prijedloga trebala donijeti prije europskih parlamentarnih izbora kako bi europska uprava bila vjerodostojna i otporna u trenutačnom geopolitičkom kontekstu. Minimalni skup pravila i standarda o informacijskoj sigurnosti za sve institucije, tijela i agencije EU-a uspostavio bi sigurnost za sve uključene strane i osigurao dosljednu zaštitu od novih prijetnji njihovim podacima, koji uključuju i klasificirane i neklasificirane podatke EU-a. Ta bi nova pravila zajedno pružila stabilan temelj za sigurnu razmjenu informacija među institucijama, tijelima i agencijama EU-a i s državama članicama, uz standardiziranu praksu i mjere za zaštitu protoka informacija. U tom su smislu usklađena s brojnim pozivima Vijeća da se poboljša otpornost institucija, tijela i agencija EU-a te da se bolje zaštiti proces donošenja odluka u Uniji od zlonamjernog uplitanja.

Akt o kibernetičkoj solidarnosti

¹¹ COM(2022) 454.

Akt o kibernetičkoj solidarnosti¹², koji je Komisija donijela 18. travnja 2023. i koji se temelji se na postojećem čvrstom strateškom, političkom i zakonodavnom okviru, dodatno će poboljšati otkrivanje kibernetičkih prijetnji, otpornost i pripravnost na svim razinama ekosustava kibernetičke sigurnosti Unije. Ti bi se ciljevi postigli trima ključnim mjerama:

- (1) uvođenjem **europskog kibernetičkog štita** radi razvoja i poboljšanja zajedničkih sposobnosti za otkrivanje i informiranost o stanju. Sastojao bi se od nacionalnih centara za sigurnosne operacije („nacionalni SOC-ovi”) i prekograničnih centara za sigurnosne operacije („prekogranični SOC-ovi”);
- (2) uspostavom **mehanizma za izvanredne situacije u području kibernetičke sigurnosti** kako bi se državama članicama pomoglo u pripremi za značajne incidente u području kibernetičke sigurnosti i incidente velikih razmjera u području kibernetičke sigurnosti, odgovoru na njih i hitnom oporavku od njih. Potpora za odgovor na incidente uključivala bi pričuvu EU-a za kibernetičku sigurnost, koja bi također bila dostupna europskim institucijama, tijelima, uredima i agencijama Unije te trećim zemljama pridruženima programu Digitalna Europa, pod uvjetom da je to predviđeno njihovim sporazumom o pridruživanju programu Digitalna Europa;
- (3) uspostavom **europskog mehanizma za incidente u području kibernetičke sigurnosti** radi istraživanja i procjene konkretnih značajnih incidenata ili incidenata velikih razmjera. Izvješće o preispitivanju nakon incidenta koordinirala bi i pripremila ENISA.

Započele su rasprave u Vijeću i Europskom parlamentu. Dovršetak pregovora prije kraja sadašnjeg mandata Europskog parlamenta dao bi veliki poticaj naporima za zaštitu građana i poduzeća u cijeloj Uniji.

Akademija za vještine u području kibernetičke sigurnosti

S obzirom na to da su kibernetičke prijetnje sve brojnije, EU hitno treba stručnjake s vještinama i kompetencijama za sprečavanje, otkrivanje, odvrćanje i obranu EU-a od kibernetičkih napada. Procjenjuje se da je za područje kibernetičke sigurnosti u EU-a trenutačno potrebno 883 000 stručnjaka, a 2022. bilo je između 260 000 i 500 000 nepopunjenih radnih mjesta. Trebalo bi potaknuti sve dijelove društva da pomognu popuniti ta radna mjesta, ali 2022., žene su činile samo 20 % diplomiranih stručnjaka za kibernetičku sigurnost i 19 % stručnjaka za informacijske i komunikacijske tehnologije. U okviru Europske godine vještina 2023. Komisija je 18. travnja 2023.¹³ donijela inicijativu za osnivanje Akademije za vještine u području kibernetičke sigurnosti kako bi se smanjio nedostatak stručnjaka za kibernetičku sigurnost, koju su poduprle države članice¹⁴. Akademija za vještine u području kibernetičke sigurnosti objedinila bi postojeće inicijative za vještine u području kibernetičke sigurnosti i poboljšala koordinaciju. Komisija potiče države članice, regionalna i lokalna nadležna tijela te europske javne subjekte da donesu posebne strategije ili inicijative za vještine u području kibernetičke sigurnosti ili da te vještine integriraju u relevantne strategije ili inicijative sa širim područjem primjene (npr. kibernetička sigurnost, digitalne vještine, zapošljavanje itd.). Uključivanje privatnih dionika isto će biti ključno da se smanji nedostatak vještina u području kibernetičke sigurnosti i povezanog manjka radne snage u Europi.

Dronovi

¹² COM(2023) 209.

¹³ COM(2023) 207.

¹⁴ Zaključci Vijeća od 22. svibnja 2023. o politici kibernetičke obrane EU-a.

Sve veća prijetnja javnim prostorima i kritičnoj infrastrukturi zlonamjerna je upotreba dronova. Incidenti koji uključuju dronove sve su češći unutar i izvan Unije, a rješenja za borbu protiv dronova ključan su alat za tijela kaznenog progona i druga javna tijela u Uniji, kao i za privatne operatere kritične infrastrukture. Za razliku od toga, legitimna upotreba dronova uvelike pridonosi usporednoj zelenoj i digitalnoj tranziciji¹⁵. Kako je najavljeno u Strategiji za dronove 2.0 donesenoj u studenom 2022., Komisija je danas donijela komunikaciju o suzbijanju mogućih prijetnji koje predstavljaju dronovi, potkrijepljenu dvama priručnicima s praktičnim smjernicama o ključnim tehničkim aspektima¹⁶. Tom se inicijativom nastoji odrediti sveobuhvatan i usklađen okvir politike sa zajedničkim poimanjem pravila za borbu protiv mogućih prijetnji koje predstavljaju dronovi te se prema potrebi nastoji prilagoditi brzom razvoju tehnologije. Države članice i relevantni privatni operateri pozivaju se da blisko surađuju s Komisijom kako bi osigurali potpunu provedbu te inicijative.

Zaštita zračnog prometa i pomorska sigurnost

Nezakonite aktivnosti, kao što su piratstvo, oružana pljačka na moru, krijumčarenje migranata te trgovina ljudima, oružjem i opojnim drogama, kao i terorizam, i dalje su prepreke pomorskoj sigurnosti, koju pogoršavaju sve brojnije prijetnje, uključujući hibridne i kibernetičke napade. Komisija i visoki predstavnik donijeli su 10. ožujka 2023. zajedničku komunikaciju kojom se ažurira Strategija pomorske sigurnosti EU-a¹⁷, koju bi sad trebalo provoditi u skladu s ažuriranim akcijskim planom.

U području zaštite zračnog prometa Komisija je 2. veljače 2023. donijela radni dokument službi Komisije „Rad na poboljšanoj i otpornijoj politici zaštite zračnog prometa”¹⁸, koji sadržava ambiciozan program za: 1. modernizaciju regulatorne strukture za zaštitu zračnog prometa; 2. poticanje razvoja i primjene inovativnijih rješenja i 3. ažuriranje temelja zaštite zračnog prometa kako bi zračne luke Unije mogle potpuno iskoristiti prednosti novih i najsuvremenijih tehnologija za otklanjanje prijetnji najvišeg prioriteta. U roku od dvije godine potrebno je provesti 14 glavnih mjera.

Komisija poziva Europski parlament i Vijeće da brzo, a svakako prije isteka mandata sadašnjeg Europskog parlamenta, dovrše pregovore o sljedećim dokumentima:

- Prijedlogu akta o kibernetičkoj otpornosti,
- Prijedlogu akta o kibernetičkoj solidarnosti,
- Prijedlogu uredbe o informacijskoj sigurnosti za institucije, tijela i agencije EU-a.

Komisija poziva države članice:

- da nastave s prioritarnim prenošenjem Direktive o otpornosti kritičnih subjekata u nacionalno pravo te s testiranjem otpornosti na stres kritične infrastrukture u energetske sektoru,
- da donesu Preporuku Vijeća o Planu za koordinaciju odgovora na poremećaje u kritičnoj infrastrukturi od znatne prekogranične važnosti,
- da potpuno i hitno prenesu Direktivu NIS 2 kako bi se povećala kibernetička sigurnost ključnih i važnih subjekata,
- da aktivno sudjeluju u provođenju procjena rizika kibernetičke sigurnosti i izradi scenarija rizika za kritičnu infrastrukturu i lance opskrbe,

¹⁵ COM(2022) 652.

¹⁶ COM(2023) 659.

¹⁷ JOIN(2023) 8.

¹⁸ SWD(2023) 37.

- da nastave s radom na Akademiji za vještine u području kibernetičke sigurnosti aktivnim sudjelovanjem na europskoj razini i posebnim nacionalnim strategijama ili inicijativama za vještine u području kibernetičke sigurnosti, kao i okupljanjem ključnih dionika, uključujući regionalna i lokalna nadležna tijela,
- da surađuju s relevantnim privatnim operaterima i Komisijom kako bi se osigurala provedba svih mjera navedenih u Komunikaciji o suzbijanju mogućih prijetnji koje predstavljaju dronovi,
- da provedu akcijski plan Strategije pomorske sigurnosti EU-a i redovito izvješćuju o postignutim rezultatima,
- da provedu 14 glavnih mjera utvrđenih za poboljšanje zaštite zračnog prometa.

III. Suočavanje s novim prijetnjama

Nove geopolitičke napetosti jasno su dokazale da se sigurnosne prijetnje EU-u povećavaju, ali i da su sve nestabilnije i dodatno pogoršane hibridnom prirodom mnogih prijetnji. Sigurnost mora pratiti i promjene u društvu i tehnologiji. Pandemija bolesti COVID-19 pružila je više mogućnosti kibernetičkim kriminalcima, a posebno se istaknula povećana prijetnja od materijala koji sadržava seksualno zlostavljanje djece na internetu. Kriminalci i zlonamjerni akteri uvijek su spremni iskoristiti tehnološki razvoj. U kontekstu takvih često složenih i višedimenzionalnih prijetnji EU treba djelovati snažno i dosljedno.

Uredba o suzbijanju seksualnog zlostavljanja djece na internetu

Europolova ocjena prijetnje organiziranog kriminala na internetu otkrila je da se 2022. dodatno povećala učestalost i ozbiljnost seksualnog iskorištavanja i zlostavljanja djece, a počinitelji su nastavili iskorištavati tehničke mogućnosti za prikrivanje svojih radnji i identiteta¹⁹. Sadašnji sustav temelji se na tome da poduzeća dobrovoljno otkrivaju i prijavljuju seksualno zlostavljanje djece na internetu, što se pokazalo nedostatnim za zaštitu djece. Privremena uredba dopušta poduzećima dobrovoljno otkrivanje i prijavljivanje pod uvjetom da je to zakonito prema Općoj uredbi o zaštiti podataka (OUZP). Ta privremena uredba istječe u kolovozu 2024. Komisija je u svibnju 2022. predložila Uredbu²⁰ za rješavanje problema zlouporabe internetskih usluga u svrhu seksualnog zlostavljanja djece. U predloženom okviru snažno se naglašava prevencija. Poduzeća bi bila obvezna putem svojih sustava procijeniti rizik od seksualnog zlostavljanja djece i poduzeti preventivne mjere. Kao krajnju mjeru, samo u slučaju znatnog rizika, nacionalni sudovi ili neovisna upravna tijela mogu pružateljima usluga izdati ciljane naloge za otkrivanje. Kao središte stručnosti, novi neovisni EU-ov Centar olakšao bi rad pružateljima usluga pružanjem pouzdanih informacija o identificiranom materijalu, primanjem i analiziranjem prijava pružatelja usluga o seksualnom zlostavljanju djece na internetu kako bi se utvrdile pogrešne prijave te pružanjem potpore žrtvama. Ključno je da se nova pravila donesu i provedu što prije kako bi se djeca zaštitila od daljnjeg zlostavljanja, spriječilo ponovno pojavljivanje materijala na internetu i kako bi se počinitelji priveli pravdi. U tijeku su pregovori u Vijeću i Parlamentu da bi se prije kraja mandata Parlamenta postigao dogovor o tom dokumentu.

¹⁹ Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* (Procjena prijetnje organiziranog kriminala na internetu, IOCTA, 2023.).

²⁰ COM(2022) 209.

Direktiva o suzbijanju nasilja nad ženama i nasilja u obitelji

Nasilje na internetu nad ženama, među ostalim u kontekstu nasilja u obitelji, pojavilo se kao novi oblik takvog nasilja koji se širi izvan granica pojedinih država članica putem interneta i informatičkih alata. Komisija je u ožujku 2022. predložila Direktivu o suzbijanju nasilja nad ženama i nasilja u obitelji, uključujući posebna pravila o kibernetičkom nasilju i mjere za uklanjanje nedostataka u zaštiti, pristupu pravosuđu i prevenciji. Njezinim ranim donošenjem i provedbom države članice dobile bi dodatne alate za suzbijanje takvog kriminala. Suzakonodavci su započeli međuinstitucijske pregovore u srpnju 2023. i nastoje ih dovršiti prije kraja sadašnjeg mandata Europskog parlamenta.

Kibernetička sigurnost 5G mreža

Sigurnost 5G mreža glavni je prioritet Komisije i ključni dio njezine strategije za sigurnosnu uniju. 5G mreže središnja su infrastruktura koja je temelj za brojne usluge neophodne za funkcioniranje unutarnjeg tržišta te za vitalne društvene i gospodarske funkcije. Tijela država članica EU-a iz Skupine za suradnju NIS objavila su 15. lipnja 2023. uz potporu Komisije i ENISA-e drugo izvješće o napretku u provedbi paketa instrumenata EU-a za kibernetičku sigurnost 5G mreža. Prema tom izvješću 24 države članice donijele su ili pripremaju zakonodavne mjere koje nacionalnim tijelima daju ovlasti za procjenu dobavljača i izdavanje ograničenja, a deset država članica uvelo je takva ograničenja. Međutim, potrebno je poduzeti daljnje mjere kako bi se izbjegla ranjivost Unije kao cjeline s potencijalno ozbiljnim negativnim učincima za sigurnost pojedinačnih korisnika i poduzeća u cijeloj Uniji i kritične infrastrukture Unije. Sve države članice moraju bez odgode provesti taj paket instrumenata. Komisija je istog dana donijela Komunikaciju o provedbi paketa instrumenata u državama članicama te o korporativnim komunikacijama Komisije i aktivnostima financiranja Unije. Istaknuta je duboka zabrinutost zbog rizika za sigurnost EU-a koje predstavljaju dobavljači opreme za komunikaciju putem mobilne mreže Huawei i ZTE. U tom kontekstu Komisija poduzima mjere kako bi izbjegla izloženost svojih korporativnih komunikacija mobilnim mrežama čiji su dobavljači Huawei i ZTE. Iz nabave su isključene nove usluge povezivosti koje se oslanjaju na opremu tih dobavljača, a Komisija će surađivati s državama članicama i telekomunikacijskim operaterima kako bi se ti dobavljači postupno isključili iz postojećih usluga povezivanja na Komisijinim internetskim stranicama. Komisija istražuje i kako tu odluku prenijeti u relevantne programe i instrumente financiranja Unije potpuno u skladu s pravom Unije.

Pristup podacima za djelotvorno izvršavanje zakonodavstva

U današnje digitalno doba gotovo svaki zločin ima digitalnu komponentu. Tehnologije i alati upotrebljavaju se i u kriminalne svrhe, uključujući one koji su nužni da se ostvari potreba našega društva za kibernetičkom sigurnošću, zaštitom podataka i privatnošću. Stoga je sve teže djelotvorno izvršavati zakonodavstvo u cijelom EU-u radi zaštite javne sigurnosti te sprečavanja i otkrivanja kaznenih djela, njihove istrage i progona. Iako su na razini Unije i nacionalnim razinama uloženi znatni naponi, među ostalim putem zakonodavstva, izgradnje kapaciteta i inovacijskih inicijativa, i dalje postoje pravni i tehnički izazovi. Komisija je s predsjedništvom Vijeća uspostavila Skupinu na visokoj razini za pristup podacima za djelotvorno izvršavanje zakonodavstva kako bi pružila platformu za suradnju s brojnim dionicima i stručnjacima za istraživanje problema s kojima se susreću službenici za izvršavanje zakonodavstva (npr. enkripcija, zadržavanje podataka, 5G i standardizacija). Komisija očekuje da će Skupina na visokoj razini do lipnja 2024. izraditi uravnotežene, čvrste i ostvarive preporuke koje odražavaju složenost tih pitanja, među ostalim iz perspektive kibernetičke sigurnosti i zaštite podataka. Stoga se države članice i stručnjaci koji sudjeluju potiču da se aktivno uključe u taj proces i rade na učinkovitim, zakonitim i općeprihvatljivim rješenjima.

Hibridne prijetnje

U geopolitičkom kontekstu u kojem hibridne prijetnje postaju sve složenije i sofisticiranije, u Strateškom kompasu EU-a za sigurnost i obranu²¹ (Strateški kompas) zajednički se procjenjuju prijetnje i izazovi s kojima se Unija suočava te se navodi strateški akcijski plan. Porastom zlonamjernog ponašanja država i nedržavnih aktera u kibernetičkom prostoru, među ostalim u kontekstu rata protiv Ukrajine, kibernetički prostor još se više ističe kao područje vanjske i sigurnosne politike. Zbog potencijalnih rizika od zlonamjernih radnji i dezinformacija potreban je poseban oprez u izbornim razdobljima, među ostalim u razdoblju koje prethodi europskim izborima 2024.

Uzimajući u obzir visoke rizike od učinaka prelijevanja, EU je nastavio razvijati aktivnosti izgradnje kibernetičkih kapaciteta i poticati partnerstva s trećim zemljama, među ostalim u okviru posebnih kibernetičkih dijaloga, kako bi aktivno ojačao svoju opću otpornost. Razvijeni su, revidirani i ojačani brojni alati kako bi se poboljšala sposobnost Unije za djelotvoran odgovor na hibridne prijetnje, kako je opisano u Sedmom izvješću o napretku u pogledu hibridnih prijetnji objavljenom 14. rujna 2023.²² Među njima su:

- EU-ov paket instrumenata protiv hibridnih prijetnji kojim će se osigurati okvir za koordinirani i utemeljeni odgovor na hibridne prijetnje i kampanje,
- kontinuirani rad na uspostavljanju timova EU-a za brzi odgovor na hibridne prijetnje za kratkoročnu prilagođenu potporu državama članicama, partnerskim zemljama te misijama i operacijama zajedničke sigurnosne i obrambene politike (ZSOP),
- revidirani protokol EU-a za suzbijanje hibridnih prijetnji („EU Playbook”)²³, u kojem se opisuju procesi i strukture Unije koji se bave hibridnim prijetnjama i kampanjama,
- revidirane provedbene smjernice okvira za zajednički diplomatski odgovor EU-a na zlonamjerne kibernetičke aktivnosti²⁴ („paket instrumenata za kibernetičku diplomaciju”), koje omogućuju razvoj trajnih, prilagođenih, usklađenih i koordiniranih strategija protiv upornih aktera kibernetičkih prijetnji,
- paket instrumenata za borbu protiv vanjske manipulacije informacijama i vanjskog uplitanja (FIMI) za jačanje postojećih alata Unije za sprečavanje, odvracanje i odgovor na vanjske manipulacije informacijama i uplitanje,
- politika kiberobrane EU-a²⁵ za jačanje kapaciteta EU-a za kibernetičku obranu, poboljšanje informiranosti o stanju i koordinaciju cijelog niza dostupnih obrambenih opcija radi jačanja otpornosti, odgovora na kibernetičke napade i osiguravanja solidarnosti i uzajamne pomoći.

Države članice stoga se potiču da nastave poboljšavati suradnju u tom području osiguravanjem djelotvorne provedbe navedenih paketa instrumenata, primjerice redovitim vježbama te postizanjem dogovora o konceptu timova za brzi odgovor na hibridne prijetnje, koji će pružiti smjernice za daljnje korake za uspostavljanje timova.

Umjetna inteligencija u kontekstu izvršavanja zakonodavstva

Umjetna inteligencija brzo je postala uobičajeni dio svakodnevnog života. Učinci upotrebe umjetne inteligencije na kibernetički kriminal i kibernetičku sigurnost još nisu u potpunosti

²¹ Dokument Vijeća 7371/22.

²² SWD(2023) 315.

²³ SWD(2023) 116.

²⁴ 10289/23 od 8. lipnja 2023.

²⁵ JOIN(2022) 49.

poznati, ali očito će donijeti nove izazove. Iako umjetna inteligencija može biti korisna kad se upotrebljava na siguran i kontroliran način, može imati opasan potencijal u rukama zlonamjernih aktera, među ostalim pomaganjem kriminalcima da sakriju svoj identitet u kaznenim djelima kao što su terorizam i seksualno zlostavljanje djece. Stoga je važno da nadležna tijela prate razvoj događaja kako bi spriječila zlostavljanje i odgovorile na zloporabu²⁶. Pregovori o predloženom Aktu o umjetnoj inteligenciji usmjereni su na rješavanje tih pitanja i ušli su u ključnu fazu, a suzakonodavci sad raspravljaju o tehničkim i političkim pitanjima koja će odrediti interakcije s tom tehnologijom u narednim godinama. Bit će ključno pronaći uravnotežena rješenja, posebno u pogledu visokorizičnih primjena, među ostalim u području izvršavanja zakonodavstva.

Komisija poziva Europski parlament i Vijeće da brzo, a svakako prije isteka mandata sadašnjeg Europskog parlamenta, dovrše međuinstitucionalne pregovore o sljedećim preostalim dokumentima:

- Prijedlog uredbe o suzbijanju seksualnog zlostavljanja djece na internetu,
- Prijedlog direktive o suzbijanju nasilja nad ženama i nasilja u obitelji,
- Prijedlog uredbe o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji).

Komisija poziva države članice:

- da bez odgode provedu paket instrumenata EU-a za kibernetičku sigurnost 5G mreža,
- da podupru rad Skupine na visokoj razini za pristup podacima za djelotvorno izvršavanje zakonodavstva radi oblikovanja jasnih, čvrstih i ostvarivih preporuka za rješavanje postojećih i očekivanih problema na proporcionalan način,
- da u suradnji s visokim predstavnikom poduzmu korake kako bi se osigurala djelotvorna provedba EU-ova paketa instrumenata protiv hibridnih prijetnji, revidiranog paketa instrumenata za kibernetičku diplomaciju te paket instrumenata FIMI, primjerice redovitim vježbama i uzimajući u obzir globalnu dinamiku,
- da postignu dogovor o konceptu timova za brzi odgovor na hibridne prijetnje.

IV. Zaštita Europljana od terorizma i organiziranog kriminala

Rizik da globalni ili lokalni događaji izazovu nove terorističke napade uvijek je prisutan. Organizirani kriminal i trgovina drogom ujedno su među najozbiljnijim prijetnjama sigurnosti EU-a. Kako bi se pojačali zajednički naponi Unije u borbi protiv tih prijetnji, u tijeku je zajednički rad na provedbi Strategije EU-a za suzbijanje organiziranog kriminala²⁷, Strategije EU-a za suzbijanje trgovine ljudima²⁸, Agende i akcijskog plana EU-a za borbu protiv droga²⁹ te Agende EU-a za borbu protiv terorizma³⁰. Međutim, kako bismo odgovorili na zabrinjavajuće sve lošiju situaciju u pogledu organiziranog kriminala i trgovine drogom,

²⁶ Vidjeti na primjer Europolovo izvješće objavljeno 17. travnja 2023.: *ChatGPT - the impact of Large Language Models on Law Enforcement* (ChatGPT – utjecaj velikih jezičnih modela na izvršavanje zakonodavstva).

²⁷ COM(2021) 170.

²⁸ COM(2021) 171.

²⁹ COM(2020) 606.

³⁰ COM(2020) 795.

potrebno je daljnje intenziviranje rada država članica i EU-a kako bismo ojačali svoj zajednički odgovor na kriminalne mreže i bolje zaštitili žrtve zločina, a istodobno s ovim izvješćem objavljuje se plan EU-a za borbu protiv trgovine drogom i organiziranog kriminala³¹.

U području borbe protiv terorizma EU jača i svoj paket instrumenata za vanjsko djelovanje³² iskorištavanjem punog potencijala dijaloga na visokoj razini za borbu protiv terorizma i mreže stručnjaka za borbu protiv terorizma i stručnjaka za sigurnost u delegacijama EU-a, kao i svojim sudjelovanjem u multilateralnim forumima, što uključuje supredsjedanje Globalnim forumom za borbu protiv terorizma.

Trgovina drogom

S novim mandatom Agencije EU-a za droge, koji će započeti u srpnju 2024., EU će biti spremniji za rješavanje složenog sigurnosnog i zdravstvenog problema koji pogađa milijune ljudi u EU-u i cijelom svijetu. Komisija revidira³³ i uredbe o prekursorima za droge³⁴ kako bi nastojala riješiti glavne probleme utvrđene evaluacijom iz 2020.³⁵, u kojoj je istaknuta potreba rješavanja problema koje uzrokuju dizajnerski prekursori³⁶ kako bi se smanjila ponuda nedopuštenih droga.

Međutim, zbog nezapamćenog porasta nedopuštenih droga dostupnih u Europi, borba protiv trgovine drogom mora se intenzivirati u suradnji s međunarodnim partnerima. Potrebne su dodatne mjere država članica i EU-a kako bi se razbile kriminalne mreže i bolje zaštitile žrtve zločina. Komisija danas predstavlja plan EU-a za borbu protiv trgovine drogom i organiziranog kriminala. U njemu se utvrđuje 17 mjera u četirima prioritetnim područjima: jačanje otpornosti logističkih čvorišta s Europskim savezom luka, razbijanje kriminalnih mreža, povećanje napora u prevenciji i jačanje suradnje s međunarodnim partnerima. Te bi se mjere trebale provesti 2024. i 2025.

Vatreno oružje

Trgovina vatrenim oružjem pomaže organiziranom kriminalu unutar EU-a, kao i u susjedstvu. Procjenjuje se da je čak 35 milijuna komada nezakonitog vatrenog oružja u rukama civila u EU-u, a približno 630 000 komada vatrenog oružja evidentirano je u Schengenskom informacijskom sustavu kao ukradeno ili izgubljeno. Razvojem brze dostave paketa i novih tehnologija, kao što je 3D ispis, trgovina vatrenim oružjem poprima nove oblike kako bi izbjegla kontrolu. Ruska ratna agresija na Ukrajinu također je povećala rizik od širenja vatrenog oružja. U listopadu 2022. Komisija je donijela prijedlog za ažuriranje postojećeg zakonodavstva o uvozu, izvozu i provožu vatrenog oružja za civilnu upotrebu kako bi se uklonili nedostaci u postojećim pravilima koji mogu povećati broj vatrenog oružja prokrijumčarenog i preusmjerenog u EU³⁷. Ta nova pravila srednjoročno će pridonijeti smanjenju rizika od zaobilaženja embarga kad je riječ o izvozu vatrenog oružja za civilnu upotrebu i povećanju kontrole uvoza te vrste vatrenog oružja iz trećih zemalja. Oba su zakonodavaca tek trebaju

³¹ COM(2023) 641.

³² Na što se poziva u Strateškom kompasu i zaključcima Vijeća „Rješavanje vanjske dimenzije terorističke i nasilne ekstremističke prijetnje koja se stalno mijenja s naglaskom na vanjskoj dimenziji” donesenima u lipnju 2022.

³³ Prekursori za droge – zakonodavstvo EU-a (revidirana pravila) (europa.eu).

³⁴ Uredba (EZ) br. 273/2004 o prekursorima za droge i Uredba Vijeća (EZ) br. 111/2005 o utvrđivanju pravila za nadzor trgovine prekursorima za droge između Zajednice i trećih zemalja.

³⁵ COM(2020) 768.

³⁶ Mjera 23. Akcijskog plana za borbu protiv droga, COM(2020) 606.

³⁷ COM(2022) 480.

donijeti svoja stajališta o tom dokumentu kako bi postigli dogovor o njemu prije kraja ovog mandata Parlamenta.

Trgovina ljudima

Trgovina ljudima posebno je težak oblik organiziranog kriminala i teško kršenje temeljnih prava. Žrtvama se trguje unutar EU-a, uglavnom za seksualno iskorištavanje i izrabljivanje radne snage, ali i za prisilno prosjačenje, prisilni kriminal i druge oblike kriminala. Komisija je u prosincu 2022. predložila izmjenu Direktive o suzbijanju trgovine ljudima³⁸ s ažuriranim pravilima za uklanjanje nedostataka u trenutnom pravnom okviru. Konkretnije, kad se donese, u revidiranoj bi se Direktivi prisilni brak i nezakonito posvajanje dodali u njezino područje primjene i uvelo bi se izričito upućivanje na internetsku dimenziju trgovine ljudima. Sadržavala bi i obvezni režim sankcija za počinitelje i formalizirala uspostavu nacionalnih mehanizama upućivanja radi poboljšanja rane identifikacije i prekograničnih zahtjeva za pomoć i potporu žrtvama. Svjesno korištenje uslugama koje pružaju žrtve trgovine ljudima postalo bi kazneno djelo, a godišnje prikupljanje podataka o trgovini ljudima koje bi objavljivao Eurostat postalo bi obvezno. Vijeće je donijelo opći pristup u lipnju 2023., a Europski parlament tek treba donijeti svoje stajalište. Potrebno je brzo djelovati kako bi se postigao dogovor prije kraja ovog mandata Parlamenta.

Ekološki kriminal

Ekološki kriminal postao je globalna prijetnja i svake godine približno raste između 5 i 7 %. Znatno profit koji se može ostvariti, rupe u zakonima među državama članicama i nizak rizik od otkrivanja privlače organizirani kriminal. Europol smatra da postoje naznake da se prihodi od tih aktivnosti koriste za financiranje terorizma. Komisija je u prosincu 2021. donijela prijedlog za zamjenu Direktive iz 2008. o zaštiti okoliša putem kaznenog prava. Prijedlog je usmjeren na doradu i ažuriranje definicija kategorija ekološkog kriminala te na utvrđivanje učinkovitih, odvraćajućih i proporcionalnih vrsta i razina sankcija za fizičke i pravne osobe. Nova kaznena djela uključuju kaznena djela povezana s nezakonitom deforestacijom, kršenjem zakonodavstva EU-a o kemikalijama, nezakonitim crpljenjem površinskih ili podzemnih voda i nezakonitim recikliranjem brodova. Prijedlogom se nastoji znatno ojačati lanac izvršavanja zakonodavstva i prekograničnu suradnju među tijelima država članica te agencijama i tijelima EU-a. Europski parlament i Vijeće donijeli su svoja stajališta o prijedlogu i u tijeku su pregovori koje bi trebali moći dovršiti do kraja godine. Revidirani akcijski plan³⁹ za suzbijanje nezakonite trgovine divljom faunom i florom treba provesti kako bi se dodatno ojačale prevencija i provedba.

Povrat i oduzimanje imovine

Oduzimanje nezakonito stečenih prihoda kriminalcima ključno je za suzbijanje organiziranog kriminala. Zbog toga je, uz prijedlog kojim se tijelima kaznenog progona daje pristup informacijama o bankovnim računima u cijelom EU-u⁴⁰ (za što je politički dogovor postignut u lipnju 2023.), Komisija u svibnju 2022. podnijela prijedlog o povratu i oduzimanju imovine⁴¹ kako bi ojačala kapacitete za praćenje, identifikaciju, zamrzavanje i oduzimanje imovine te upravljanje njome. Ključne odredbe prijedloga odnose se na zahtjeve za financijske istrage te dodatne ovlasti i alate ureda za oduzimanje imovinske koristi, kao i na djelotvornije mjere zamrzavanja i oduzimanja imovine za širi skup kaznenih djela. Kršenje Unijinih mjera

³⁸ COM(2022) 732.

³⁹ COM(2022) 581.

⁴⁰ COM(2021) 429.

⁴¹ COM(2022) 245.

ograničavanja novo je kazneno djelo na koje bi se te mjere primjenjivale. Komisija je u prosincu 2022. donijela zasebni prijedlog za usklađivanje kaznenih definicija i kazni za kršenje Unijinih mjera ograničavanja. Djelotvorna primjena i provedba Unijinih mjera ograničavanja i dalje je glavni prioritet Komisije, koji podupire rad radne skupine „Zamrzavanje i privremeno oduzimanje”, koju je Komisija uspostavila kao odgovor na rusku ratnu agresiju na Ukrajinu. Europski parlament i Vijeće donijeli su svoja stajališta za oba prijedloga radi postizanja dogovora do kraja ove godine.

Paket mjera za borbu protiv pranja novca

Pranje novca povezano je s gotovo svim kriminalnim aktivnostima koje rezultiraju imovinskom koristi ostvarenom kaznenim djelima u EU-u⁴² i stoga je glavni pokretač borbe protiv kriminala u EU-u. Komisija je u srpnju 2021. iznijela ambiciozne prijedloge za jačanje mjera EU-a za sprečavanje pranja novca i financiranja terorizma⁴³, s četiri zakonodavna prijedloga za jačanje prevencije i otkrivanja pokušaja kriminalaca da operu nezakonitu imovinsku korist ili financiraju terorističke aktivnosti putem financijskog sustava. Suzakonodavci su u svibnju 2023. donijeli jednu od četiri inicijative iz tog paketa kako bi se osigurala sljedivost prijenosa kriptoinovine⁴⁴. Ta uredba počinje se primjenjivati 30. prosinca 2024., a do tog će datuma svi pružatelji usluga povezanih s kriptoinovinom morati prikupljati i čuvati informacije o pošiljatelju i korisniku prijenosa kriptoinovine. Svrha je preostalih triju prijedloga: i. osnovati novo tijelo EU-a za borbu protiv pranja novca kako bi se osigurao dosljedan visokokvalitetan nadzor na unutarnjem tržištu, uključujući najrizičnije prekogranične subjekte, te za podupiranje i koordinaciju rada financijsko-obavještajnih jedinica, ii. utvrditi usklađena pravila za privatni sektor, uključujući uvođenje ograničenja od 10 000 EUR za velika gotovinska plaćanja u zamjenu za usluge i robu na razini cijelog EU-a i iii. ojačati ovlasti i alate za suradnju nadležnih tijela. Očekuje se da će taj paket znatno poboljšati sposobnost EU-a za borbu protiv pranja novca i zaštitu građana EU-a od terorizma i organiziranog kriminala. Suzakonodavci trenutačno pregovaraju o tri preostala prijedloga kako bi postigli dogovor o tom dokumentu prije kraja ovog mandata Parlamenta.

Komisija poziva Europski parlament i Vijeće da brzo, a svakako prije isteka mandata sadašnjeg Europskog parlamenta, dovrše međuinstitucionalne pregovore o sljedećim preostalim dokumentima:

- Prijedlog direktive o povratu i oduzimanju imovine,
- Prijedlog direktive za usklađivanje kaznenih definicija i kazni za kršenje Unijinih mjera ograničavanja,
- Prijedlog direktive o suzbijanju trgovine ljudima,
- Prijedlog direktive o unapređenju zaštite okoliša putem kaznenog prava,
- Prijedlog paketa mjera za borbu protiv pranja novca,
- Prijedlog za ažuriranje postojećeg zakonodavstva o uvozu, izvozu i provožu vatrenog oružja za civilnu upotrebu.

Komisija poziva države članice, agencije i tijela EU-a:

⁴² Europol, *Enterprising criminals – Europe’s fight against the global networks of financial and economic crime* (Kriminalna poduzeća – Europa u borbi protiv globalnih mreža financijskog i gospodarskog kriminala), 2020.

⁴³ COM(2021) 420.

⁴⁴ Uredba (EU) 2023/1113 od 31. svibnja 2023. o informacijama koje su priložene prijenosima novčanih sredstava i određene kriptoinovine i o izmjeni Direktive (EU) 2015/849.

- | |
|--|
| <ul style="list-style-type: none">- da zajedno rade na provedbi 17 mjera iz plana EU-a za borbu protiv trgovine drogom i organiziranog kriminala 2023. i 2024. |
|--|

V. Snažan europski sigurnosni ekosustav

Proteklih godina sigurnosne prijetnje sve više postaju prekogranične, što zahtijeva daljnje sinergije i pojačanu suradnju na svim razinama. Od donošenja strategije za sigurnosnu uniju poduzete su važne inicijative za maksimalno povećanje prekogranične suradnje, a one uključuju pojednostavnjenje i unapređenje dostupnih instrumenata i postupaka i na vanjskim granicama i unutar schengenskog područja te poboljšanje razmjene informacija između tijela kaznenog progona i pravosudnih tijela za učinkovitiju borbu protiv organiziranog kriminala. U tom kontekstu djelotvorna provedba okvira za interoperabilnost za razmjenu podataka važan je stup poboljšanja sigurnosti i djelotvornog europskog odgovora na prekogranične prijetnje, a ujedno jamči slobodno kretanje unutar EU-a.

Poboljšana razmjena informacija unutar schengenskog područja: unaprijed dostavljene informacije o putnicima (API), evidencija podataka o putnicima (PNR) i Prüm II

Dva prijedloga za unaprijed dostavljene informacije o putnicima, koja je Komisija donijela u prosincu 2022.⁴⁵, poboljšala bi unutarnju sigurnost Unije pružajući tijelima za izvršavanje zakonodavstva u državama članicama dodatne alate za borbu protiv teških kaznenih djela i terorizma. Konkretnije, unaprijed dostavljene informacije o putnicima na letovima unutar EU-a, koje se upotrebljavaju zajedno s evidencijom podataka o putnicima u zračnom prometu, omogućile bi tijelima za izvršavanje zakonodavstva u državama članicama da znatno povećaju učinkovitost svojih istraga intervencijama koje su bolje ciljane. Važno je da se predložena pravila donesu što prije. Osim što bi se time poduprla borba protiv organiziranog kriminala i terorizma, znatno bi se smanjila potreba za sustavnim provjerama svih putnika u slučaju privremenog ponovnog uvođenja unutarnjih graničnih provjera, što bi olakšalo zračni prijevoz i slobodu kretanja. Europska komisija preporučila je Vijeću 6. rujna 2023. da odobri pregovore sa Švicarskom, Islandom i Norveškom radi postizanja sporazuma o prijenosu podataka iz evidencije podataka o putnicima. Donošenjem tih triju preporuka poduprla bi se dosljedna i djelotvorna vanjska politika o evidenciji podataka o putnicima u EU-u.

Policija svakodnevno primjenjuje razmjene u okviru Prüma u borbi protiv organiziranog kriminala, droge, terorizma, seksualnog iskorištavanja i trgovine ljudima. Prijedlogom uredbe o automatskoj razmjeni podataka za policijsku suradnju („Prüm II”)⁴⁶ revidira se postojeći okvir iz Prüma radi uklanjanja problema nedostatka informacija i jačanja prevencije, otkrivanja i istrage kaznenih djela u EU-u. Revidirana pravila o automatskoj razmjeni podataka za policijsku suradnju upotpunjuju prijedloge za policijsku suradnju u ovom mandatu, uz već donesenu preporuku Vijeća o jačanju operativne prekogranične policijske suradnje i Direktivu o razmjeni informacija između tijela za izvršavanje zakonodavstva. Brzo donošenje i provedba tih povezanih instrumenata poboljšali bi, olakšali i ubrzali razmjenu podataka među tijelima za izvršavanje zakonodavstva i pomogli u identificiranju kriminalaca.

⁴⁵ COM(2022) 729, COM(2022) 73.

⁴⁶ COM(2021) 784.

Potpuno interoperabilan sustav upravljanja državnim granicama za sigurno, snažno, digitalno i ujedinjeno schengensko područje

Schengensko područje bez unutarnjih granica koje dobro funkcionira temelji se na uzajamnom povjerenju među državama članicama. To pak počiva na djelotvornom nadzoru, bez obzira na to provodi li se na vanjskim granicama Unije ili kao alternativna mjera na državnom području država članica. Izmjenom Zakonika o schengenskim granicama⁴⁷ koju je predložila Komisija utvrđuje se kako države članice mogu bolje iskoristiti alternative nadzoru unutarnjih granica, koje mogu osigurati visoku razinu sigurnosti. Važno je da se izmjena Zakonika o schengenskim granicama donese i provede u cijelosti kako bi se osigurala visoka i proporcionalna razina sigurnosti unutar schengenskog područja. Nastavlja se razvijati i nova arhitektura informacijskih sustava EU-a radi bolje podrške nacionalnim tijelima u sigurnosnim naporima te upravljanju granicama. Sastoji se od obnovljenog Schengenskog informacijskog sustava, sustava EU-a za informacije o putovanjima i odobravanje putovanja, sustava ulaska/izlaska, ažuriranja viznog informacijskog sustava i okvira za interoperabilnost za povezivanje sustava uz potpunu sigurnost. Nakon što se potpuno dovrši, ta bi nova arhitektura nacionalnim tijelima pružala sveobuhvatnije i pouzdanije sigurnosne informacije. Ključne su sve komponente okvira za interoperabilnosti, što znači da kašnjenje u jednom aspektu ili u jednoj državi članici dovodi do odgođenog uvođenja u svim državama članicama. Kašnjenja u tehničkom razvoju sustava ulaska/izlaska treba svesti na najmanju moguću mjeru kako bi što prije mogao početi s radom i kako bi se uspostavili svi ključni elementi okvira za interoperabilnost.

Prijedlogom o dubinskoj provjeri⁴⁸ povećala bi se sigurnost unutar schengenskog područja uspostavljanjem jedinstvenih pravila za identifikaciju državljana trećih zemalja koji ne ispunjavaju uvjete za ulazak kako je navedeno u Zakoniku o schengenskim granicama te za njihovo podvrgavanje zdravstvenim i sigurnosnim provjerama na vanjskim granicama. Predloženi sustav Eurodac podupro bi te ciljeve ukazujući na pojedince za koje se dubinskom provjerom utvrdi da bi mogli predstavljati prijetnju unutarnjoj sigurnosti. To bi zauzvrat olakšalo provedbu predložene Uredbe o upravljanju azilom i migracijama. Komisija potiče suzakonodavce da brzo dovrše pregovore o tim dokumentima prije kraja važećeg parlamentarnog saziva.

Borba protiv korupcije

Korupcija je vrlo štetna za naše demokracije, gospodarstvo i našu sigurnost jer pogoduje organiziranom kriminalu i zlonamjernom stranom uplitanju. Uspješno sprečavanje i borba protiv korupcije bitni su za zaštitu vrijednosti EU-a i učinkovitost politika EU-a te za poštovanje vladavine prava i povjerenja u one na vlasti i u javne institucije. Kako je predsjednica von der Leyen najavila u govoru o stanju Europske unije 2022., Komisija je 3. svibnja 2023. donijela paket antikorupcijskih mjera⁴⁹. Komisijin Prijedlog direktive o borbi protiv korupcije uključuje ojačana pravila kojima se kriminaliziraju kaznena djela korupcije i usklađuju kazne u cijelom EU-u. Omogućuje i učinkovite istrage i kazneni progon te u prvi plan stavlja prevenciju i stvaranje kulture integriteta u kojoj se korupcija ne tolerira. U Europskom parlamentu i Vijeću započele su rasprave o tom prijedlogu. Osim toga, države članice pozivaju se da provedu preporuke koje proizlaze iz stupa izvješća o vladavini prava za 2023. donesenog 5. srpnja 2023. koji se odnosi na borbu protiv korupcije. Na temelju prijedloga visokog predstavnika, uz

⁴⁷ COM(2021) 891.

⁴⁸ COM(2020) 612.

⁴⁹ COM(2023) 234.

potporu Komisije, uspostavio bi se poseban režim sankcija za zajedničku vanjsku i sigurnosnu politiku (ZVSP) usmjeren na teška djela korupcije u cijelom svijetu.

Jačanje prava žrtava

Komisija je 12. srpnja 2023. predložila izmjene Direktive o pravima žrtava kako bi se ojačao pristup žrtava informacijama, potpori i zaštiti, njihovo sudjelovanje u kaznenom postupku i pristup naknadi. Jedan od općih ciljeva revizije doprinos je visokoj razini sigurnosti stvaranjem sigurnijeg okruženja za žrtve kako bi se smanjenjem straha od odmazde potaknulo prijavljivanje kaznenih djela.

Komisija poziva Europski parlament i Vijeće da brzo, a svakako prije isteka mandata sadašnjeg Europskog parlamenta, dovrše međuinstitucionalne pregovore o sljedećim preostalim dokumentima:

- Prijedlog uredbe Prüm II,
- prijedlozi o unaprijed dostavljenim informacijama o putnicima (API),
- prijedlozi o borbi protiv korupcije, a posebno o uspostavi posebnog režima sankcija zajedničke vanjske i sigurnosne politike (ZVSP),
- Prijedlog izmjene Zakonika o schengenskim granicama,
- Prijedlog direktive o pravima žrtava,
- Prijedlog o dubinskoj provjeri.

Komisija poziva države članice:

- da što prije osiguraju stupanje na snagu sustava ulaska/izlaska kako bi se dovršila provedba arhitekture EU-a za razmjenu informacija.

VI. Provedba

Jamčenje sigurnosti Europe u cjelini zajednička je odgovornost u okviru koje svaki sudionik ima svoju ulogu, od Komisije i zakonodavaca, koji donose nova stroga i sveobuhvatna i praktična pravila, preko država članica, koje pravodobno prenose, provode i primjenjuju takva pravila, do raznih tijela, organizacija i dionika, koji obavljaju operativni rad na terenu. Agencije EU-a u područjima pravosuđa, unutarnjih poslova i kibernetičke sigurnosti također imaju ključnu ulogu, koja se povećala nedavnim proširenjem njihovih odgovornosti.

Pojačana provjera korisnika financijskih sredstava Unije

Komisija pri izvršavanju proračuna EU-a ima odgovornost osigurati da korisnici financijskih sredstava Unije poštuju vrijednosti EU-a. Mehanizmi i sustavi kontrole kojima se određuje tko može imati koristi od financijskih sredstava Unije već su pouzdani, a u pregovorima o preinaci Financijske uredbe koji su u tijeku Komisiji se nastoje dati snažnija pravna sredstva za djelovanje ako je potrebno. Osim toga, Komisija trenutačno radi na daljnjem unaprjeđenju dubinske provjere sadašnjih i potencijalnih budućih korisnika financijskih sredstava Unije poboljšanjem smjernica o obvezama u vezi s poštovanjem vrijednosti EU-a i posljedicama koje bi trebale uslijediti nakon kršenja vrijednosti EU-a. Time će se pojasniti odgovornosti korisnika i subjekata koji provode kontrole na razini EU-a, a može poslužiti i kao izvor inspiracije na nacionalnoj razini. Ako se prekrše uvjeti financiranja, Komisija neće oklijevati prekinuti suradnju s korisnicima predmetnog projekta i prema potrebi osigurati povrat sredstava. Važno je da države članice proaktivno dijele informacije s Komisijom kad imaju saznanja o mogućim rizicima u vezi s organizacijama koje se prijavljuju za financijska sredstva Unije.

Povrede

U području sigurnosti Komisija je provela mnoge postupke zbog povrede. Na primjer, 2023. pokrenut je velik broj postupaka zbog povrede uzrokovane neispunjavanjem obveza na temelju Uredbe o borbi protiv širenja terorističkog sadržaja na internetu iz 2021. (16 država članica)⁵⁰, a 2022. i 2023. 20 država članica primilo je dodatne službene opomene zbog netočne provedbe Direktive o suzbijanju seksualnog zlostavljanja djece iz 2011.⁵¹ Još uvijek je otvoren znatan broj postupaka zbog povrede uzrokovane neusklađenosti nacionalnog zakonodavstva s Direktivom o suzbijanju terorizma iz 2017.⁵² i neuspjelim prenošenjem pravila koja olakšavaju upotrebu financijskih i drugih informacija za sprječavanje, otkrivanje, istragu ili kazneni progon određenih kaznenih djela⁵³. Ostala područja u kojima su u tijeku postupci zbog povrede uključuju zakonodavstvo o vatrenom oružju, pravila o psihoaktivnim tvarima koje se koriste u drogama, suzbijanje prijevара i krivotvorenja instrumenata bezgotovinskog plaćanja, borbu protiv pranja novca, razmjenu podataka iz kaznene evidencije među državama članicama EU-a i Direktivu o pravima žrtava. Državama članicama koje provode dogovorene inicijative i mjere na raspolaganje je stavljena potpora (tehnička i financijska), a Komisija je dostupna za suradnju s državama članicama na optimizaciji provedbe.

Praćenje putem evaluacija Schengena i njegov novi sustav upravljanja

Mehanizam evaluacije i praćenja Schengena nastavio je pridonositi djelotvornoj provedbi schengenskih pravila usmjerenih na jačanje sigurnosti unutar područja bez unutarnjih kontrola. Tijekom 2023. provedene su prve evaluacije u okviru pojačanog mehanizma evaluacije i praćenja Schengena, koje su omogućile pravovremeno prepoznavanje i otklanjanje strateških ranjivosti koje imaju prekogranični učinak na sigurnost i zaštitu unutar EU-a. Nadalje, Komisija je 2023. pokrenula tematsku evaluaciju Schengena kako bi procijenila prakse država članica koje se suočavaju sa sličnim problemima u borbi protiv trgovine drogom u EU-u, a posebno trgovine drogom u velikim količinama. Te evaluacije stavile su jači i sveobuhvatniji naglasak na sigurnosne elemente Schengena. Na temelju rezultata periodičnih, tematskih i nenajavljenih evaluacija Schengena Vijeće je u lipnju 2023. utvrdilo prioritete schengenskog ciklusa 2023.–2024. Njime se utvrđuju glavna područja kojima je potreban dodatni poticaj za sigurnije i jače schengensko područje. Djelotvorna i brza provedba tih prioriteta usporedno s povećanom koordinacijom politike Schengenskog vijeća dodatno će ojačati borbu protiv organiziranog kriminala i maksimalno povećati prekograničnu operativnu suradnju.

Uloga agencija i tijela EU-a

Partnerstvo je ključno za provedbu inicijativa sigurnosne unije jer je za postizanje konkretnih rezultata potreban rad raznih nacionalnih i europskih nadležnih tijela. Na primjer, EMPACT (Europska multidisciplinarna platforma za borbu protiv kaznenih djela) omogućuje strukturiranu multidisciplinarnu suradnju država članica, koju podupiru sve institucije, tijela i agencije EU-a (kao što su Europol, Frontex, Eurojust, CEPOL, OLAF, eu-LISA). Operacije koje provodi EMPACT, među ostalim putem namjenskih operativnih radnih skupina, koordiniraju napore država članica i operativnih partnera u borbi protiv kriminalnih mreža i teških kaznenih djela. Zahvaljujući EMPACT-u samo u 2022. izvršena su 9922 uhićenja,

⁵⁰ Uredba (EU) 2021/784 o borbi protiv širenja terorističkog sadržaja na internetu.

⁵¹ Direktiva (EU) 2011/93 o suzbijanju seksualnog zlostavljanja djece.

⁵² Direktiva (EU) 2017/541 Europskog parlamenta i Vijeća od 15. ožujka 2017. o suzbijanju terorizma i zamjeni Okvirne odluke Vijeća 2002/475/PUP i o izmjeni Odluke Vijeća 2005/671/PUP.

⁵³ Direktiva (EU) 2019/1153 Europskog parlamenta i Vijeća od 20. lipnja 2019. o utvrđivanju pravila kojima se olakšava uporaba financijskih i drugih informacija u svrhu sprečavanja, otkrivanja, istrage ili progona određenih kaznenih djela i stavljanju izvan snage Odluke Vijeća 2000/642/PUP.

zaplijenjeni su imovina i novac u vrijednosti većoj od 180 milijuna EUR, pokrenute su 9263 istrage, identificirano je 4019 žrtava, zaplijenjeno je više od 62 tone droge, identificirana je 51 meta visoke vrijednosti, od kojih je 12 uhićeno, te su provedene operacije u kontekstu agresije na Ukrajinu, posebno radi suzbijanja trgovanja ljudima i prijetnji povezanih s vatrenim oružjem⁵⁴.

Frontex, Europska agencija za pomorsku sigurnost (EMSA) i Europska agencija za kontrolu ribarstva (EFCA) nastavljaju jačati svoju suradnju na funkcijama obalne straže kako bi poduprli nacionalna tijela u povećanju sigurnosti i zaštite na moru. Te će agencije uvelike pridonijeti provedbi Strategije pomorske sigurnosti Europske unije.

U okviru nekoliko inicijativa sigurnosne unije uvedene su nove odgovornosti i zadaci relevantnim agencijama, ponekad s implikacijama za osoblje.

Agencija Europske unije za kibersigurnost (ENISA)

Kad je riječ o pripravnosti i odgovoru na incidente kako bi se poboljšala kibernetička sigurnost, Komisija je uspostavila kratkoročnu mjeru za potporu državama članicama koja uključuje prijenos sredstava iz programa Digitalna Europa u **Agenciju Europske unije za kibersigurnost (ENISA)** kako bi se ojačala pripravnost i kapacitet za odgovor na velike kibernetičke incidente. Prijedlog akta o kibernetičkoj solidarnosti donesen u travnju 2023. nadograđuje se na tu mjeru i, nakon što ga donesu suzakonodavci, ENISA-i će se moći povjeriti dodatne zadaće kao što su rad buduće pričuve EU-a za kibernetičku sigurnost i upravljanje njome ili priprema izvješća o preispitivanju incidenta nakon kibernetičkih incidenata velikih razmjera. Prema predloženom Aktu o kibernetičkoj otpornosti ENISA bi bila zadužena da od proizvođača prima obavijesti o ranjivostima proizvoda s digitalnim elementima te o incidentima koji utječu na sigurnost tih proizvoda, a koje bi ENISA trebala proslijediti relevantnim timovima za odgovor na računalne sigurnosne incidente ili relevantnim jedinstvenim kontaktnim točkama država članica. Očekuje se i da ENISA izrađuje dvogodišnje tehničko izvješće o novim trendovima u području kibernetičkih rizika proizvoda s digitalnim elementima i da ga dostavlja Skupini za suradnju NIS.

Europski stručni centar u području kibernetičke sigurnosti

Europski stručni centar u području kibernetičke sigurnosti (ECCC), zajedno s mrežom nacionalnih koordinacijskih centara (NCC), novo je tijelo Unije za potporu inovacijama i industrijskoj politici u području kibernetičke sigurnosti. Taj će ekosustav ojačati kapacitete zajednice za tehnologiju kibernetičke sigurnosti, održati izvrsnost istraživanja i ojačati konkurentnost industrije Unije u tom području. Europski stručni centar u području kibernetičke sigurnosti i nacionalni koordinacijski centri donosit će strateške odluke o ulaganjima i prikupljati resurse iz Unije, njezinih država članica i, neizravno, industrije kako bi se poboljšali i ojačali tehnološki i industrijski kapaciteti kibernetičke sigurnosti. Europski stručni centar u području kibernetičke sigurnosti stoga ima ključnu ulogu u ispunjavanju ambicioznih ciljeva kibernetičke sigurnosti iz programa Digitalna Europa i Obzor Europa.

⁵⁴ EMPACT, Informativni članci o rezultatima u 2022.: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf

Europski stručni centar u području kibernetičke sigurnosti zaposlio je više od polovine svojeg osoblja, a uskoro će zaposliti i svojeg izvršnog direktora. Rad koji je već u tijeku uključuje dio programa DIGITAL koji se odnosi na kibernetičku sigurnost i novi strateški program⁵⁵ za razvoj i uvođenje tehnologije, kojim se utvrđuju prioritetne mjere za potporu malim i srednjim poduzećima u razvoju i upotrebi strateških tehnologija, usluga i postupaka u području kibernetičke sigurnosti, za podupiranje i razvoj profesionalne radne snage te za povećanje stručnog znanja i iskustva u području istraživanja, razvoja i inovacija u širem europskom ekosustavu kibernetičke sigurnosti.

Europol

S potpuno novim mandatom **Europol** će lakše moći pružiti potporu državama članicama u borbi protiv organiziranog kriminala. Borba protiv trgovine drogom ključni je prioritet s obzirom na njezinu sve veću važnost i sve veći negativan učinak na sigurnost građana EU-a. Nakon odobrenja Vijeća Europske unije 15. svibnja 2023. Komisija aktivno radi na sklapanju međunarodnih sporazuma s Bolivijom, Brazilom, Ekvadorom, Meksikom i Peruom o razmjeni osobnih podataka s Europolom radi sprečavanja i borbe protiv teških kaznenih djela i terorizma.

Eurojust

S više od 20 godina iskustva u pružanju pravosudne potpore nacionalnim tijelima u borbi protiv cijelog niza teških i složenih kaznenih djela s prekograničnim elementima **Eurojust** je učvrstio svoju poziciju u području slobode, sigurnosti i pravde u EU-u. Kako bi ojačala sveobuhvatnu suradnju, Komisija pregovara o međunarodnim sporazumima za olakšavanje suradnje između Eurojusta i 13 trećih zemalja radi razmjene osobnih podataka u borbi protiv organiziranog kriminala i terorizma⁵⁶. Pregovori su već dovršeni s Armenijom i Libanom, u tijeku su s Alžirskom i Kolumbijom, a započeli su s Bosnom i Hercegovinom. Komisija potiče Europski parlament i Vijeće da sklope sporazume s tim zemljama prije kraja parlamentarnog saziva kako bi se ojačala transnacionalna pravosudna suradnja i proširila borba protiv prekograničnog kriminala.

EPPO

Od početka svojih operativnih aktivnosti u lipnju 2021. **Ured europskog javnog tužitelja (EPPO)** pokazao se moćnim alatom u paketu instrumenata Unije za istragu i kazneni progon kaznenih djela koja utječu na proračun Unije, uključujući kaznena djela povezana sa sudjelovanjem u zločinačkoj organizaciji, kad je fokus na kaznenim djelima na štetu proračuna Unije. Komisija potiče države članice koje još ne sudjeluju u pojačanoj suradnji EPPO-a da počnu sudjelovati što prije kako bi se ostvario puni potencijal EPPO-a u zaštiti novca poreznih obveznika EU-a.

EUDA

S novim mandatom koji su suzakonodavci donijeli u lipnju 2023. postojeći Europski centar za praćenje droga i ovisnosti o drogama (EMCDDA) pretvorit će se u punopravnu agenciju s većom ulogom, **Agenciju Europske unije za droge (EUDA)**. Agencija će moći procijeniti nove zdravstvene i sigurnosne prijetnje koje uzrokuju nedopuštene droge na sveobuhvatniji način i djelotvornije pridonijeti radu na razini država članica i na međunarodnoj razini. Prikupljanje, analiza i širenje podataka i dalje će biti glavna zadaća te agencije, no prošireni mandat omogućit će joj i da razvije opće kapacitete za procjenu prijetnji zdravlju i sigurnosti

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

⁵⁶ Alžir, Argentina, Armenija, Bosna i Hercegovina, Brazil, Kolumbija, Egipat, Izrael, Jordan, Libanon, Maroko, Tunis i Turska.

kako bi otkrila nove prijetnje, uključujući upotrebu više vrsta tvari, da ojača svoju suradnju putem nacionalnih kontaktnih točaka te da uspostavi mrežu laboratorija koji će joj pružati forenzičke i toksikološke informacije. To će joj pomoći da izda upozorenja kad se posebno opasne tvari pojave na tržištu i da javnosti skrene pozornost na to.

Komisija poziva Europski parlament i Vijeće da brzo, a svakako prije isteka mandata sadašnjeg Europskog parlamenta, dovrše međuinstitucionalne pregovore o sljedećim preostalim dokumentima:

- Prijedlog preinake Financijske uredbe.

Komisija poziva države članice:

- da proaktivno dijele informacije s Komisijom kad su svjesne mogućih rizika u vezi s organizacijama koje se prijavljuju za financijska sredstva Unije,
- da brzo provedu prioritete schengenskog ciklusa 2023.–2024. za sigurnije i jače schengensko područje,
- da riješe postupke zbog povrede koji su pokrenuti protiv njih kako bi se osigurao pravilan prijenos predmetnog zakonodavstva.

VII. Zaključak

Protekle tri godine obilježene su stalnim i odlučnim naporima da se težnja stvaranja sigurnosne unije za EU pretvori u stvarnost. Učinjeni su veliki pomaci u cijelom nizu područja sigurnosne politike. Nove prijetnje koje se stalno mijenjaju sad zahtijevaju kontinuirane napore s novom motivacijom. Rad na zakonodavnom okviru treba se pravodobno dovršiti prije kraja parlamentarnog saziva u proljeće 2024. Države članice imaju stalnu odgovornost za prenošenje, provedbu i primjenu novih zakonodavnih akata. Provedba zahtijeva usklađene napore, uključujući potporu agencija EU-a, i vrlo često sve jaču suradnju s našim međunarodnim partnerima.

Samo uz zajedničke i odlučne napore svih zainteresiranih strana postići ćemo razinu sigurnosti i zaštite u EU-u koju građani očekuju, a u današnjim okolnostima svakom bi akteru trebao biti prioritet odigrati svoju ulogu u jačanju sigurnosti EU-a.