Vijeće
Europske unije

Bruxelles, 3. travnja 2025.
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**

POPRATNA BILJEŠKA

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	2. travnja 2025.
Za:	Thérèse BLANCHET, glavna tajnica Vijeća Europske unije
Br. dok. Kom.:	COM(2025) 148 final
Predmet:	KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA ProtectEU: europska strategija unutarnje sigurnosti

Za delegacije se u prilogu nalazi dokument COM(2025) 148 final.

Priloženo: COM(2025) 148 final

EUROPSKA
KOMISIJA

Strasbourg, 1.4.2025.
COM(2025) 148 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA

ProtectEU: europska strategija unutarnje sigurnosti

1. ProtectEU: europska strategija unutarnje sigurnosti

Sve naše slobode temelje se na našoj sigurnosti. Demokracija, vladavina prava, temeljna prava, dobrobit Europljana, konkurentnost i blagostanje – sve to ovisi o našoj sposobnosti da svima zajamčimo osnovnu sigurnost. U novom dobu obilježenom sigurnosnim prijetnjama u kojem sad živimo sposobnost država članica EU-a da svojim građanima zajamče sigurnost više nego ikad ovisi o **jedinstvenom europskom pristupu zaštiti naše unutarnje sigurnosti**. U promjenjivom geopolitičkom okruženju Europa mora i dalje ispunjavati svoje trajno obećanje mira.

Prvi koraci prema izgradnji europskog sigurnosnog aparata već su napravljeni. U proteklom desetljeću Uniji smo pružili poboljšane kolektivne mehanizme djelovanja u područjima izvršavanja zakonodavstva i pravosudne suradnje, sigurnosti granica, borbe protiv teškog i organiziranog kriminala, borbe protiv terorizma i nasilnog ekstremizma te zaštite fizičke i digitalne kritične infrastrukture EU-a. Pravilna provedba već donesenog zakonodavstva i oblikovanih politika i dalje je neophodna.

Zbog prirode današnjih prijetnji i suštinske veze između unutarnje i vanjske sigurnosti EU-a moramo ići korak dalje.

Prijetnje su velike. Granica između **hibridnih prijetnji** i otvorenog rata teško se razaznaje. Rusija vodi hibridnu kampanju na internetu i izvan njega protiv EU-a i njegovih partnera kako bi poremetila i ugrozila društvenu koheziju i demokratske procese i dovela u pitanje solidarnost EU-a s Ukrajinom. Neprijateljske strane države i akteri koje sponzoriraju države nastoje se infiltrirati u našu kritičnu infrastrukturu i lance opskrbe i poremetiti ih, krasti osjetljive podatke i pozicionirati se tako u budućnosti uzrokuju najveće moguće poremećaje. Kriminal koriste kao uslugu, a kriminalce kao pomagače. Osim toga, naša ovisnost o trećim zemljama kad je riječ o lancima opskrbe čini nas ranjivijima na hibridne kampanje neprijateljskih država.

Kako je istaknuto u procjeni prijetnje teškog i organiziranog kriminala u EU-u (SOCTA), koju je nedavno predstavio Europol, moćne mreže **organiziranog kriminala** šire se u Europi, jačaju na internetu, infiltriraju se u naše gospodarstvo i utječu na naše društvo[1]. Jednom kad se organizirani kriminal ukorijeni u zajednici ili gospodarskom sektoru, njegovo iskorjenjivanje postaje mukotrpna bitka: trećina najopasnijih kriminalnih mreža aktivna je već više od deset godina. Kriptovalute i paralelni financijski sustavi pomažu im u pranju i prikrivanju imovinske koristi ostvarene kaznenim djelima.

Prijetnja terorizma i dalje se nadvija nad Europom. Posljedice regionalnih kriza izvan EU-a šire se izvan svojih izvorišta, što terorističkim akterima iz cijelog ideološkog spektra pruža priliku da vrbuju nove pristaše, mobiliziraju ili povećavaju svoje kapacitete. Njihova nastojanja da provode radikalizaciju i vrbuju posebno su usmjerena na najranjivije skupine u našem društvu, konkretno na određene grupe mladih. Nadahnjuju individualne napade i porast rušilačkog ekstremizma čiji je cilj poremetiti demokratski pravni poredak.

Vrtoglav **tehnološki napredak** omogućava nam poboljšanje našeg sigurnosnog aparata. Međutim, kibernetički napadi i inozemna manipulacija informacijama sve su raširenija jer se u njima koriste nove tehnologije kao što je umjetna inteligencija. Na internetu su posebno ugroženi djeca, mladi i starije osobe, a širenje mržnje na internetu ugrožava slobodu izražavanja i socijalnu koheziju.

Naši su životi postali nesigurniji i Europljani to sve više osjećaju: njihova **percepcija zaštićenosti i sigurnosti u EU-u** narušena je do te mjere da 64 % njih iskazuje zabrinutost za

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

sigurnost EU-a kad im se postave pitanja o budućnosti[2]. Poduzeća su također sve zabrinutija pa se među deset najvećih rizika utvrđenih u Izvješću Svjetskog gospodarskog foruma o globalnim rizicima za 2025. navode pogrešne informacije i dezinformacije, kriminal i nezakonite aktivnosti i kibernetička špijunaža[3].

Europljani bi trebali moći **živjeti bez straha**, bilo na ulicama, kod kuće, na javnim mjestima, na podzemnoj željeznici ili na internetu. Zaštita ljudi, posebno onih koji su najosjetljiviji na napade, što nerazmjerno uključuje djecu, žene i manjine, uključujući židovske i muslimanske zajednice, u središtu je mjera koje EU poduzima u području sigurnosti. To je ključno za izgradnju otpornih i povezanih društava.

Komisija predstavlja **europsku strategiju unutarnje sigurnosti** za bolje suzbijanje prijetnji u narednim godinama. Strožim paketom pravnih instrumenata, dubljom suradnjom i povećanom razmjenom informacija poboljšat ćemo našu otpornost i kolektivnu sposobnost djelotvornog predviđanja, sprečavanja, otkrivanja i odgovora na sigurnosne prijetnje. Jedinstven pristup unutarnjoj sigurnosti pomoći će državama članicama da moć tehnologije iskoriste za jačanje sigurnosti, a ne njezino slabljenje, uz promicanje sigurnog digitalnog prostora za svakoga. Osim toga, bit će koristan i za zajednički odgovor država članica na globalne političke i gospodarske promjene koje utječu na unutarnju sigurnost Unije.

Ova strategija ima **tri glavna načela**, a temelji se na poštovanju vladavine prava i temeljnih prava.

Prvo, u njoj se utvrđuje ambicija promjene kulture sigurnosti. Potreban nam je **pristup koji obuhvaća cijelo društvo** i uključuje sve građane i dionike, a posebno civilno društvo, istraživače, akademsku zajednicu i privatne subjekte. Zbog toga je glavna značajka mjera iz ove strategije integrirani pristup koji uključuje više dionika kad god je to moguće.

Drugo, **sigurnosna pitanja treba integrirati i redovito uključivati u cjelokupno zakonodavstvo, politike i programe EU-a**, uključujući vanjsko djelovanje EU-a. Zakonodavstvo, politike i programi morat će se pripremati, preispitivati i provoditi imajući na umu sigurnosni aspekt i uzimajući u obzir bitna sigurnosna pitanja kako bi se promicao dosljedan i sveobuhvatan pristup sigurnosti.

Naposljetku, za sigurnost, zaštitu i otpornost Europe potrebna su **ozbiljna ulaganja EU-a, njegovih država članica i privatnog sektora.** Za stvarnu provedbu prioriteta i mjera utvrđenih u ovoj strategiji potrebni su dostatni ljudski i financijski resursi. Kako je utvrđeno u Komunikaciji o putu prema sljedećem višegodišnjem financijskom okviru[4], Europa će morati povećati javnu potrošnju za sigurnost i promicati istraživanja i ulaganja u području sigurnosti kako bi povećala svoju stratešku autonomiju.

Ovom strategijom dopunjuju se **Strategija za Uniju pripravnosti**[5], u kojoj se predstavlja primjena integriranog pristupa kojim se obuhvaćaju sve opasnosti na pripravnost za sukobe, katastrofe uzrokovane ljudskim djelovanjem i prirodne katastrofe te krize, i **Bijela knjiga o europskoj obrambenoj spremnosti 2030.**[6]., koja pomaže u razvoju i stjecanju obrambenih sposobnosti na razini cijelog EU-a radi odvraćanja stranih protivnika. Komisija će predložiti i **europski štit za zaštitu demokracije** u svrhu jačanja demokratske otpornosti u EU-u. Te inicijative zajedno postavljaju temelj sigurnog, zaštićenog i otpornog EU-a.

[2] Istraživanje Flash Eurobarometar FL550: Izazovi i prioriteti za EU.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, str. 17.
[4] COM(2025) 46 final.
[5] JOIN (2025) 130 final.
[6] JOIN (2025) 120 final.

Nov način upravljanja unutarnjom sigurnošću u Europi

Komisija će blisko surađivati s državama članicama i agencijama EU-a kako bi unaprijedila pristup EU-a unutarnjoj sigurnosti na strateškoj i operativnoj razini.

To će se postići:

- **dosljednom identifikacijom potencijalnih implikacija novih i revidiranih inicijativa Komisije u odnosu na sigurnost i pripravnost od početka i tijekom cijelog pregovaračkog procesa**
- **redovitim sastancima Komisijine projektne skupine za europsku unutarnju sigurnost, uz stratešku međusektorsku suradnju u cijeloj Komisiji**
- **prezentacijom analiza prijetnji u pogledu unutarnje sigurnosti kako bi se Kolegiju za sigurnost pomoglo u radu**
- **raspravom s državama članicama u Vijeću o novim izazovima u području unutarnje sigurnosti na temelju analize prijetnji i razmjenom informacija o glavnim prioritetima politike**
- **redovitim izvješćivanjem Europskog parlamenta i Vijeća radi praćenja i podupiranja sustavne provedbe glavnih sigurnosnih inicijativa.**

2. Integrirana informiranost o stanju i analiza prijetnji

Pružit ćemo EU-u nove načine razmjene i kombiniranja informacija i redovitu analizu prijetnji unutarnjoj sigurnosti u EU-u, čime ćemo pridonijeti sveobuhvatnoj procjeni rizika i prijetnji.

Preduvjet za sigurnost je **djelotvorno predviđanje**. EU se mora osloniti na sveobuhvatnu, dovoljno autonomnu i aktualnu informiranost o stanju i analizu prijetnji. Provedivi obavještajni podaci, na čije se dodatno poboljšanje angažiranjem Službe za jedinstvenu obavještajnu analizu (SIAC) kao jedinstvene ulazne točke za obavještajne podatke država članica potiču države članice, ključni su za procjenu i suzbijanje prijetnji, čime se u konačnici podupiru političke i zakonodavne mjere[7]. Moramo u većoj mjeri djelotvorno i zajednički iskorištavati **analizu utemeljenu na obavještajnim podacima** i **procjene prijetnji** na razini EU-a.

Na temelju raznih procjena rizika i prijetnji na razini EU-a i za određene sektore[8] Komisija će **redovito pripremati analizu prijetnji unutarnjoj sigurnosti EU-a** kako bi se identificirali glavni sigurnosni izazovi i tako pomoglo u oblikovanju prioriteta politike. Ti će prioriteti pomoći u razvoju agilne i prilagodljive politike unutarnje sigurnosti, koja će biti djelotvoran odgovor na nove prijetnje i bolje zaštititi ljude i poduzeća od napada te omogućiti pravodobne ciljane intervencije politike. Te analize prijetnji unutarnjoj sigurnosti EU-a pridonijet će i **sveobuhvatnoj procjeni rizika i prijetnji za EU (međusektorska, obuhvaćajući sve opasnosti)** koju oblikuju Komisija i Visoki predstavnik, kako je utvrđeno u Strategiji za Uniju pripravnosti.

Povjerenje i sigurno postupanje ključni su za razmjenu informacija, a za to je potrebna pouzdana i sigurna infrastruktura. Institucije, tijela i agencije EU-a moraju imati mogućnost služiti se **sigurnim komunikacijskim kanalima** za razmjenu osjetljivih i klasificiranih

[7] Zajedno smo sigurniji – Jačanje europske civilne i vojne pripravnosti i spremnosti, str. 23.

[8] Sektorske procjene prijetnji koje će pridonijeti toj analizi prijetnji uključuju procjenu prijetnje teškog i organiziranog kriminala u EU-u (SOCTA), Izvješće o stanju i kretanjima u području terorizma u EU-u (TE-SAT), Zajedničko izvješće o stanju kibernetičke sigurnosti (JCAR) i buduće procjene prijetnji, rizika i metoda pranja novca i financiranja terorizma koje će provesti Komisija i Tijelo za sprečavanje pranja novca.

podataka međusobno i s državama članicama. Ulaganja u **interoperabilne sigurne sustave** i pouzdanu tehnologiju povećat će autonomiju EU-a i njegovu sposobnost da se nosi s krizama i osigura operativnu otpornost. U tom kontekstu Komisija poziva suzakonodavce da dovrše pregovore o **predloženoj uredbi o sigurnosti podataka u institucijama, tijelima, uredima i agencijama Unije**, posebno radi stvaranja zajedničkog okvira za rukovanje osjetljivim neklasificiranim i klasificiranim podacima[9].

Kako bi osigurala vlastitu operativnu sigurnost i informiranost o stanju, Komisija će revidirati svoj okvir za korporativno upravljanje sigurnošću i uspostaviti **integrirani centar za sigurnosne operacije (ISOC)** radi zaštite osoba, fizičke imovine i operacija na svim lokacijama Komisije. Komisija će ojačati i svoje operativne i analitičke kapacitete za utvrđivanje i ublažavanje hibridnih prijetnji.

U skladu sa Strategijom za Uniju pripravnosti pitanja pripravnosti i sigurnosti redovito će se uključivati i uvoditi u zakonodavstvo i sve politike i programe EU-a. Tijekom pripreme novih ili preispitivanja postojećih zakonodavnih akata, politika i programa, imajući pritom u vidu pitanja pripravnosti i sigurnosti, Komisija će dosljedno utvrđivati moguće učinke najpoželjnije opcije politike na pripravnost i sigurnost. Da bi se to olakšalo, provodit će se redovita osposobljavanja oblikovatelja politika u Komisiji.

Kako bi podržala države članice, Komisija će s Vijećem raspravljati o pitanjima koja se pojave u području unutarnje sigurnosti i ključnim prioritetima politike i redovito ga izvješćivati o provedbi strategije. Osim toga, Komisija će pružati informacije i redovito komunicirati s Europskim parlamentom i relevantnim dionicima o svim relevantnim mjerama.

Ključne mjere

Komisija će:

- **pripremati i predstavljati redovite analize prijetnji u odnosu na pitanja unutarnje sigurnosti EU-a.**

Države članice pozivaju se da:

- **poboljšaju razmjenu obavještajnih podataka sa SIAC-om i osiguraju bolju razmjenu informacija s agencijama i tijelima EU-a.**

Europski parlament i Vijeće pozivaju se da:

- **dovrše pregovore o predloženoj Uredbi o sigurnosti podataka u institucijama, tijelima, uredima i agencijama Unije.**

3. Jačanje sigurnosnih kapaciteta EU-a

Razvit ćemo nove instrumente za izvršavanje zakonodavstva, kao što je novi ojačani Europol, i bolje načine koordinacije i osiguravanja sigurne razmjene podataka i zakonitog pristupa podacima.

Kako bi se djelotvorno suzbile nove prijetnje, EU mora poboljšati svoje sigurnosne kapacitete i poticati inovacije. Tijelima za izvršavanje zakonodavstva i pravosudnim tijelima kao glavnim akterima u borbi protiv prijetnji unutarnjoj sigurnosti potrebni su odgovarajući operativni alati i kapaciteti za brze i djelotvorne mjere. Radi učinkovitog sprečavanja, otkrivanja, istrage i kaznenog progona važna je prekogranična i međusobna komunikacija i koordinacija tih tijela i relevantnih službi.

[9] COM(2022) 119 final

Agencije i tijela EU-a za unutarnju sigurnost

Agencije i tijela EU-a u području pravosuđa, unutarnjih poslova i kibernetičke sigurnosti imaju ključnu ulogu u sigurnosnoj arhitekturi EU-a, koja se nastavlja širiti zajedno s njihovim odgovornostima.

Danas, 25 godina nakon osnivanja, **Europol** je u sigurnosnom okviru EU-a važniji nego što je ikad bio. Podupire složene prekogranične istrage, olakšava razmjenu informacija, razvija inovativne alate za rad policije i pruža napredno stručno znanje tijelima za izvršavanje zakonodavstva. Međutim, nekoliko čimbenika sprečava Europol da u potpunosti ostvari svoj operativni potencijal u podupiranju istražnih i operativnih aktivnosti radi suzbijanja prekograničnog kriminala, počevši od nedovoljnih resursa do činjenice da njegov aktualni mandat ne obuhvaća nove sigurnosne prijetnje, kao što su sabotaža, hibridne prijetnje i manipulacija informacijama. Zbog toga će Komisija predložiti **ambicioznu reformu mandata Europola** kako bi ga se pretvorilo u istinski operativnu policijsku agenciju koja pruža bolju potporu državama članicama. Cilj je unaprijediti tehnološko stručno znanje i kapacitete Europola za potporu nacionalnim agencijama za izvršavanje zakonodavstva, poboljšati koordinaciju s drugim agencijama i tijelima te s državama članicama, ojačati strateška partnerstva s partnerskim zemljama i privatnim sektorom te osigurati pojačani nadzor nad Europolom.

Nadalje, Komisija će raditi na daljnjem **poboljšanju djelotvornosti i komplementarnosti agencija i tijela EU-a za unutarnju sigurnost i na olakšavanju njihove suradnje**.

Mandat **Eurojusta** ocijenit će se i ojačati kako bi se omogućila djelotvornija pravosudna suradnja, što će poboljšati komplementarnost i suradnju s Europolom. To uključuje poboljšanje učinkovitosti Eurojusta i njegovih kapaciteta za pružanje proaktivne potpore i analize pravosudnim tijelima država članica. Nadalje, s obzirom na jedinstvenu nadležnost **EPPO-a** za istragu i kazneni progon kaznenih djela koja utječu na financijske interese Unije, Komisija će razmotriti najbolje načine za poboljšavanje kapaciteta EPPO-a za zaštitu sredstava Unije. Među ostalim, to će podrazumijevati jačanje suradnje između EPPO-a i Europola.

Učinkovita i sigurna razmjena informacija među agencijama neophodna je za suradnju. Europolu i Frontexu potrebna je brza uzajamna razmjena informacija, među ostalim u operativne svrhe. Na temelju Zajedničke izjave iz siječnja 2024.[10] **eu-LISA** ima središnju ulogu u osiguravanju sigurne pohrane i dostupnosti podataka radi bolje koordinacije i učinkovitije razmjene informacija među agencijama. **Agencija EU-a za temeljna prava** pruža stručno znanje o zaštiti temeljnih prava tijekom razvoja i provedbe sigurnosnih politika.

Tijelo EU-a za sprečavanje pranja novca (AMLA) ovlašteno je primjenom metode pogodak / nema pogotka uspoređivati svoje informacije s informacijama koje su radi provedbe zajedničkih analiza prekograničnih slučajeva na raspolaganje stavili Europol, EPPO, Eurojust i Ured EU-a za borbu protiv prijevara.

ENISA ima glavnu ulogu u provedbi europskog zakonodavstva o kibernetičkoj sigurnosti. U predstojećoj **reviziji Akta o kibersigurnosti** Komisija će preispitati njegovo područje primjene i predložiti njegovu modernizaciju kako bi se povećala njegova dodana vrijednost EU-a.

Suradnja između carinskih tijela i drugih tijela za izvršavanje zakonodavstva povećat će se predloženim osnivanjem **carinskog tijela EU-a** i **centra EU-a za carinske podatke** u okviru paketa carinskih reformi EU-a. Informacije iz budućeg centra i povezani podaci koje posjeduju Europol, Eurojust, EPPO, OLAF, AMLA i Frontex, u okviru svojih nadležnosti, poboljšat će zajedničku analizu i

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

doprinijeti usklađenosti operativnih aktivnosti, posebno na vanjskim granicama. Komisija potiče suzakonodavce da što brže dovrše pregovore o carinskoj reformi EU-a i nastavit će im pomagati u tome.

Poboljšanje komplementarnosti između EPPO-a, OLAF-a, Europola, Eurojusta, AMLA-e i predloženog carinskog tijela EU-a temeljit će se i na rezultatima aktualnog preispitivanja **strukture EU-a za borbu protiv prijevara**. Takav sveobuhvatan pristup može biti koristan za unutarnju sigurnost jer su mu ciljevi bolja upotreba kaznenih i administrativnih sredstava, interoperabilnost IT sustava i poboljšana suradnja.

Strateška komunikacija

Strateški komunikacijski sustavi[11] danas uglavnom funkcioniraju samo na nacionalnoj razini. To znači da interventne službe koje prelaze preko granice u druge države članice često ne mogu komunicirati sa svojim kolegama iz tih država. U nekim je državama članicama ograničena i komunikacija između različitih vrsta interventnih službi (npr. policije i vozila hitne pomoći). Standardi većine sustava ne ispunjavaju suvremen zahtjeve u pogledu funkcionalnosti i otpornosti, što znatno ograničava sposobnost interventnih službi za reakcije, posebno one prekogranične.

Kako bi se povećala sposobnost EU-a da reagira na krize, Komisija će predložiti zakonodavne akte za stvaranje **strateškog komunikacijskog sustava EU-a (EUCCS)**, koji će povezati strateške komunikacijske sustave država članica u cijelom EU-u. Cilj je da se EUCCS temelji na tri strateška stupa: operativnoj mobilnosti, snažnoj otpornosti i strateškoj autonomiji. U inicijativi za EUCCS utvrdit će se usklađeni zahtjevi i pomoći u modernizaciji strateških komunikacijskih sustava država članica, što će omogućiti njihovo uredno funkcioniranje. Osim toga, dostupnost usluga tih sustava proširit će i budući višeorbitalni sustav IRIS[212] U okviru projekata koje financira EU razvit će se tehničke sposobnosti za EUCCS, oslanjajući se pritom prvenstveno na europske pružatelje tehnoloških usluga, kako bi se promicala strateška autonomija EU-a u tom osjetljivom sektoru.

Zakonit pristup podacima

Tijela kaznenog progona i pravosudna tijela trebaju imati kapacitete za istragu kaznenih djela i poduzimanje mjera protiv njih. Danas gotovo svi oblici teškog i organiziranog kriminala imaju digitalni trag[13]. Oko 85 % kaznenih istraga sad se oslanja na sposobnost tijela kaznenog progona da pristupe digitalnim informacijama.[14]

Skupina na visokoj razini za pristup podacima za djelotvorno izvršavanje zakonodavstva istaknula je u svojem završnom izvješću[15] da su tijela za izvršavanje zakonodavstva i pravosuđe tijekom proteklog desetljeća kaskala za kriminalcima jer se kriminalci koriste alatima i proizvodima iz drugih jurisdikcija koje su im na raspolaganje stavili dobavljači koji su mjerama koje su uveli sami sebi uskratili mogućnost da surađuju u rješavanju zakonitih zahtjeva u pojedinačnim kaznenim predmetima. Stoga je sustavna suradnja između tijela za izvršavanje zakonodavstva i privatnih subjekata, uključujući pružatelje usluga, ključan element budućih nastojanja da se suzbiju najopasnije kriminalne mreže i pojedinci u Uniji i izvan nje.

[11] To su mreže koje koriste tijela za izvršavanje zakonodavstva, službenici graničnog nadzora, carinska tijela, civilna zaštita, vatrogasci, hitne medicinske službe i drugi ključni akteri javne sigurnosti i zaštite.
[12] Infrastruktura EU-a za otpornost, međusobnu povezanost i sigurnost putem satelita
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
[14] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52019PC0070.
[15] Završno izvješće Skupine na visokoj razini za pristup podacima za djelotvorno izvršavanje zakonodavstva – 15. 11. 2024., 4802e306-c364-4154-835b-e986a9a49281_en.

Budući da je digitalizacija sve raširenija i kriminalcima osigurava nove alate, nužan je okvir za pristup podacima usklađen s potrebama za provedbom propisa i zaštitom naših vrijednosti. Jednako je važno da digitalni sustavi ostanu zaštićeni od neovlaštenog pristupa kako bismo očuvali kibernetičku sigurnost i zaštitili se od novih sigurnosnih prijetnji. U takvim okvirima za pristup moraju se poštovati i temeljna prava i osigurati, među ostalim, odgovarajuća zaštita privatnosti i osobnih podataka.

Posljednjih godina EU je donošenjem pravila o elektroničkim dokazima koja će se u potpunosti primjenjivati od kolovoza 2026.[16] uveo mjere za suzbijanje **kriminala na internetu i lakši pristup digitalnim dokazima za sva kaznena djela**. To će se dopuniti međunarodnim pravnim instrumentima za razmjenu informacija i dokaza. Komisija će uskoro predložiti potpisivanje i sklapanje nove **Konvencije UN-a protiv kibernetičkog kriminala**.

Kako bi postupila u skladu s preporukama Skupine na visokoj razini[17], Komisija će u prvoj polovini 2025. predstaviti **plan u kojem će predstaviti pravne i praktične mjere** koje predlaže kako bi se osigurao **zakonit i djelotvoran pristup podacima**. U okviru daljnjeg postupanja u vezi s tim planom Komisija će dati prednost procjeni učinka **pravila o zadržavanju podataka** na razini EU-a i pripremi **plana tehnološkog razvoja u području šifriranja** kako bi se identificirala i ocijenila tehnološka rješenja koja bi tijelima za izvršavanje zakonodavstva omogućila zakonit pristup šifriranim podacima, uz zaštitu kibernetičke sigurnosti i temeljnih prava.

Operativna suradnja

Komisija će surađivati s državama članicama, agencijama i tijelima EU-a i partnerskim zemljama na jačanju operativne suradnje, koja je ključna za djelotvorniji pristup borbi protiv transnacionalnog organiziranog kriminala i terorizma.

Glavni okvir EU-a za zajedničko djelovanje protiv teškog i organiziranog kriminala, **Europska multidisciplinarna platforma za borbu protiv kaznenih djela (EMPACT)**, postigla je značajne operativne rezultate. Sljedeći ciklus EMPACT-a, u razdoblju 2026. – 2029., prilika je za daljnje jačanje tog okvira. Kako bi se suzbile najopasnije kriminalne mreže i pojedinci, Unija mora racionalizirati i usmjeriti svoje djelovanje na najhitnije prioritete, pridonositi mjerama država članica i osigurati učinkovito korištenje resursa.

Komisija će zato surađivati s predsjedništvima Vijeća i državama članicama kako bi se **maksimalno povećao potencijal EMPACT-a i rješavala najvažnija prioritetna pitanja za sljedeći ciklus EMPACT-a, u razdoblju 2026. – 2029.** U svim tim prioritetnim područjima potrebni su obavještajni podaci o najopasnijim kriminalnim mrežama, zajedničke istrage i operativne radne skupine te odlučan pravosudni odgovor, uključujući pristup „slijedi novac”. Nadalje, Unija se treba boriti protiv kriminalnog vrbovanja i infiltracije te ojačati višeagencijsku i međunarodnu suradnju i osposobljavanje u području izvršavanja zakonodavstva.

Komisija će podupirati i druge oblike **prekogranične operativne suradnje u području izvršavanja zakonodavstva među državama članicama i zemljama pridruženima Schengenu**. Za šengensko područje bez kontrola na unutarnjim granicama potrebna je bliska suradnja i razmjena informacija među tijelima za izvršavanje zakonodavstva država članica

[16] Uredba (EU) 2023/1543 Europskog parlamenta i Vijeća od 12. srpnja 2023. o europskim nalozima za dostavljanje i europskim nalozima za čuvanje elektroničkih dokaza u kaznenim postupcima i za izvršenje kazni zatvora nakon kaznenog postupka, SL L 191, 28.7.2023.

[17] Zaključci Vijeća o pristupu podacima za učinkovito izvršavanje zakonodavstva (12. prosinca 2024.) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/hr/pdf.

kako bi se osigurala visoka razina unutarnje sigurnosti. Službenici tijela za izvršavanje zakonodavstva i dalje se suočavaju s poteškoćama pri nadzoru ili provedbi hitnih prekograničnih intervencija[18], a pojačana prekogranična suradnja potrebna je i za suzbijanje hibridnih prijetnji. Trebalo bi osnovati **skupinu na visokoj razini za budućnost operativne suradnje u području izvršavanja zakonodavstva** kako bi se oblikovala zajednička strateška vizija.

Za djelotvornu prekograničnu suradnju izuzetno je među ostalim bitna i učinkovita razmjena podataka među tijelima za izvršavanje zakonodavstva. **Arhitektura za interoperabilnost**, nakon što bude uspostavljena, omogućit će tijelima za izvršavanje zakonodavstva i Europolu djelotvoran pristup ključnim informacijama. Istodobno bi EU i njegove države članice trebali kao prioritet odrediti bilateralnu i multilateralnu razmjenu informacija, i to pravnom i tehničkom provedbom **Uredbe Prüm II**[19] u suradnji s agencijom eu-LISA i Europolom. Tako će se omogućiti sigurna automatizirana razmjena otisaka prstiju, profila DNK-a, podataka iz registra vozila, prikaza lica i policijskih evidencija preko usmjerivača EU-a. Na nacionalnoj razini države članice trebaju provesti **Direktivu o razmjeni informacija**[20] kako bi se poboljšali kanali za razmjenu informacija i tako omogućio neometan prekogranični protok informacija i istodobno osigurala njihova integracija sa sustavima na razini Unije, kao što je SIENA[21].

Djelotvornost prekogranične suradnje ovisi i o poticanju **zajedničke kulture izvršavanja zakonodavstva u EU-u.** Za postizanje tog cilja ključni su zajednički programi osposobljavanja, centri izvrsnosti i mobilnost. Komisija će proučiti kako EU može najbolje poduprijeti osposobljavanje tijela država članica, oslanjajući se pritom na **CEPOL** kao agenciju EU-a za osposobljavanje u području izvršavanja zakonodavstva.

Jačanje sigurnosti granica

Jačanje otpornosti i sigurnosti vanjskih granica ključno je za suzbijanje hibridnih prijetnji, kao što je korištenje migracija kao oružja, za sprečavanje ulaska aktera i robe koji su prijetnja za EU i za djelotvornu borbu protiv prekograničnog kriminala i terorizma. **Plan je da se** 2026. **Šengenski informacijski sustav (SIS) poboljša** tako da se državama članicama omogući da unose upozorenja o državljanima trećih zemalja koji su uključeni u terorizam, što uključuje strane terorističke borce, i u druga teška kaznena djela, na temelju podataka koje treće zemlje podijele s Europolom.

Zahvaljujući poboljšanoj **interoperabilnosti** opsežnih informacijskih sustava EU-a države članice imat će pristup ključnim informacijama o pojedincima iz trećih zemalja koji prelaze ili namjeravaju prijeći vanjske granice, što će tijelima pomoći u procjeni uvjeta za odobravanje ulaska na državno područje država članica[22]. Komisija će nastaviti blisko surađivati s državama

[18] Kako je navedeno u Komisijinoj procjeni učinka za Preporuku Vijeća (EU) 2022/915 od 9. lipnja 2022. o operativnoj suradnji tijela kaznenog progona (5909/25).

[19] Uredba (EU) 2024/982 Europskog parlamenta i Vijeća od 13. ožujka 2024. o automatskom pretraživanju i razmjeni podataka za policijsku suradnju i izmjeni odluka Vijeća 2008/615/PUP i 2008/616/PUP te uredaba (EU) 2018/1726, (EU) 2019/817 i (EU) 2019/818 Europskog parlamenta i Vijeća (Uredba Prüm II), SL L, 2024/982, 5.4.2024).

[20] Direktiva (EU) 2023/977 Europskog parlamenta i Vijeća od 10. svibnja 2023. o razmjeni informacija između tijelâ za izvršavanje zakonodavstva država članica i o stavljanju izvan snage Okvirne odluke Vijeća 2006/960/PUP, SL L 134, 22.5.2023., str. 1.

[21] Mrežna aplikacija za sigurnu razmjenu informacija.

[22] Konkretno, sustav ulaska/izlaska (EES) omogućit će državama članicama da identificiraju državljane trećih zemalja na vanjskim granicama šengenskog područja i bilježe njihove ulaske i izlaske, što će omogućiti sustavnu identifikaciju osoba koje su prekoračile trajanje dopuštenog boravka. Europski sustav za informacije o putovanjima i odobravanje putovanja (ETIAS) i vizni informacijski sustav (VIS) omogućit će državama članicama da prije dolaska državljana treće zemlje na vanjske granice procijene bi li njihova prisutnost na području EU-a predstavljala sigurnosni rizik.

članicama i agencijom eu-LISA na brzom uvođenju tih sustava, posebno **sustava ulaska/izlaska (EES), europskog sustava za odobravanje putovanja (ETIAS) i revidiranog viznog informacijskog sustava (VIS)**, kako bi se osigurao njihov uredan rad i korist za sigurnost.

Kako bi se dodatno poboljšala sigurnost granica i ojačala suradnja u EU-u s obzirom na rastuće prijetnje, **Komisija će predložiti jačanje Frontexa**. Europska granična i obalna straža trebala bi se postupno utrostručiti na 30 000 zaposlenih. Ta agencija trebala bi biti opremljena naprednom tehnologijom za nadzor i informiranost o stanju, uključujući obavještajne podatke relevantne za europsko integrirano upravljanje granicama i pristup pouzdanim državnim uslugama EU-a za promatranje Zemlje za potrebe granične kontrole koje će biti puštene u rad do 2027. To bi trebalo dodatno poboljšati sposobnost otkrivanja, sprečavanja i suzbijanja prekograničnog kriminala na vanjskim granicama i ojačati podršku državama članicama u provedbi vraćanja, posebno u odnosu na državljane trećih zemalja koji predstavljaju sigurnosni rizik.

Krivotvorenje isprava i krađa identiteta olakšavaju krijumčarenje migranata, trgovanje ljudima, nezakonito kriminalno kretanje i trgovinu nezakonitom robom. Kad **detektor višestrukih identiteta (MID)**[23] postane operativan, poboljšat će se sposobnost nacionalnih tijela da identificiraju pojedince koji se koriste višestrukim identitetima i da se bore protiv krađe identiteta. Komisija će razmotriti načine za poboljšanje sigurnosti putnih i boravišnih isprava koje se izdaju građanima EU-a i državljanima trećih zemalja. Osim toga, Komisija će procijeniti kako EU-ove lisnice za digitalni identitet, koje će se uvesti do kraja 2026. kao dio europskog okvira za digitalni identitet, mogu doprinijeti poboljšanju sigurnosti putnih isprava i provjere identiteta. To će biti dopuna prijedlozima o digitalnim putnim vjerodajnicama i EU-ovoj digitalnoj aplikaciji za putovanja[24].

Informacije o putovanjima izuzetno su bitne nadležnim tijelima u njihovim nastojanjima da utvrde i istraže kretanje kriminalaca, terorista i drugih koji predstavljaju sigurnosne prijetnje. Iako postoji okvir EU-a za informacije o komercijalnom zračnom prijevozu[25], obrada podataka iz drugih vrsta prijevoza za potrebe izvršavanja zakonodavstva je fragmentirana. Stoga kriminalci i teroristi mogu koristiti razne vrste prijevoza za prikrivanje svojih nezakonitih aktivnosti. Komisija će s državama članicama i sektorom prijevoza raditi na **jačanju okvira za informacije o putovanjima** tako što će se razmotriti program Unije u okviru kojeg bi se od operatora privatnih letova zahtijevalo da prikupljaju i šalju podatke o putnicima, ocjenjivala pravila o obradi evidencije podataka o putnicima i procjenjivali načini za pojednostavnjenje obrade informacija o putovanjima u pomorskom prometu. Komisija će ocijeniti proširenu upotrebu **sustava za automatsko prepoznavanje registarskih pločica (ANPR)** u cestovnom prometu i proširiti mogućnosti za sinergije sa sustavom SIS.

Predviđanje, inovacije i pristup temeljen na kapacitetima

Komisija će osmisliti **sveobuhvatan pristup predviđanju stanja unutarnje sigurnosti na razini EU-a**, oslanjajući se na najbolju praksu utvrđenu na nacionalnoj razini. Taj će pristup biti koristan za oblikovanje politika i usmjeravanje ulaganja u relevantna istraživanja i inovacije u području sigurnosti koje financira EU.

[23] MID je jedna od komponenata interoperabilnosti uvedenih Uredbom (EU) 2019/818 i Uredbom 2019/817.
[24] https://ec.europa.eu/commission/presscorner/detail/hr/ip_24_5047.
[25] Okvir za evidenciju podataka o putnicima (PNR) i unaprijed dostavljene informacije o putnicima (API), uspostavljen Direktivom (EU) 2016/681 („Direktiva o PNR-u”) i uredbama (EU) 2025/12 i (EU) 2025/13 („uredbe o API-ju”).

Istraživanja i inovacije imaju nezaobilaznu ulogu u unutarnjoj sigurnosti jer stvaraju rješenja za suzbijanje novih prijetnji, među ostalim zloporabe tehnologije[26]. Preko istraživanja i inovacija u području sigurnosti koje financira[27] EU mora nastaviti ulagati u razvoj inovativnih alata i rješenja za suzbijanje sigurnosnih prijetnji uz poštovanje pravila EU-a i temeljnih prava. Komisija bi trebala pomagati u prelasku s istraživanja na primjenu kako bi se osiguralo stvarno korištenje tih modernih kapaciteta, s naglaskom na **moderne tehnologije** kao što je umjetna inteligencija. Taj bi pristup trebao uključivati osposobljavanje u tijelima za izvršavanje zakonodavstva i pravosudnih tijelima za bolje korištenje sustava umjetne inteligencije i drugih tehničkih kapaciteta. Nadalje, prema potrebi, potencijal tehnologija s dvojnom namjenom trebalo bi koristiti u oba smjera (od civilne prema obrambenoj i od obrambene prema civilnoj)[28].

Inovacijski centar EU-a za unutarnju sigurnost[29], mreža laboratorija za inovacije u kojima nastaju najnovije inovacije i djelotvorna rješenja koja akterima u području unutarnje sigurnosti u EU-u i državama članicama pomažu u radu, pomoći će u integraciji istraživanja u praksu i politiku. Da bi se povećala djelotvornost Europola, potrebno je unaprijediti repozitorij njegovih alata (ETR) kako bi mu se omogućilo da operativno identificira, razvije, zajednički nabavlja i primjenjuje napredne tehnologije. Osim toga, Komisija će u sklopu svojeg Zajedničkog istraživačkog centra uspostaviti **kampus za istraživanja i inovacije u području sigurnosti**, koji će okupiti istraživače kako bi se skratio ciklus od rezultata istraživanja do inovacija, razvoja i uspješne provedbe, uz istodobno smanjenje troškova za razvoj, testiranje i validaciju.

Naš **europski istraživački prostor** sam je po sebi kolaborativan i stoga osjetljiv na inozemno upletanje i dezinformacije. Nakon donošenja Preporuke Vijeća o sigurnosti istraživanja[30] Komisija i države članice poduzimaju mjere za potporu relevantnim akterima, među ostalim osnivanjem stručnog centra za sigurnost istraživanja.

Ključne mjere

Komisija će 2026. donijeti:

- **zakonodavni prijedlog za preobrazbu Europola u zaista operativnu agenciju za izvršavanje zakonodavstva,**
- **zakonodavni prijedlog za jačanje Eurojusta,**
- **zakonodavni prijedlog za jačanje uloge i zadaća Frontexa,**
- **zakonodavni prijedlog za uspostavu europskog sustava za kritične komunikacije.**

Komisija će:

- **u 2025. predstaviti plan u kojem se utvrđuju daljnji koraci u pogledu zakonitog i djelotvornog pristupa podacima za tijela za izvršavanje zakonodavstva,**
- **u 2025., prema potrebi, izraditi procjenu učinka radi ažuriranja pravila o zadržavanju podataka na razini EU-a**
- **u 2026. predstaviti plan tehnološkog razvoja u području šifriranja kako bi se identificirala i ocijenila tehnološka rješenja koja bi tijelima za izvršavanje zakonodavstva omogućila zakonit pristup podacima,**

[26] Vidjeti izvješće Zajedničkog istraživačkog centra Komisije „Novi rizici i prilike za unutarnju sigurnost EU-a koji proizlaze iz novih tehnologija" https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] Studija o jačanju istraživanja i inovacija u području sigurnosti koje financira EU – 20 godina istraživanja i inovacija u području civilne sigurnosti financiranih sredstvima EU-a – 2025., https://data.europa.eu/doi/10.2837/0004501.
[28] Kako je predstavljeno u Niinistöovom izvješću.
[29] Inovacijski centar EU-a za unutarnju sigurnost | Europol.
[30] SL C/2024/3510, 30.5.2024.

- **raditi na osnivanju skupine na visokoj razini za jačanje operativne suradnje u području izvršavanja zakonodavstva,**
- **u 2026. u okviru Zajedničkog istraživačkog centra uspostaviti kampus za istraživanja i inovacije u području sigurnosti.**

U suradnji s državama članicama i relevantnim agencijama EU-a Komisija će:

- **ojačati strukturu EMPACT-a,**
- **raditi na brzom uvođenju arhitekture za interoperabilnost i provedbi Uredbe Prüm II,**
- **ojačati okvir za informacije o putovanjima.**

Države članice pozivaju se da:

- **prenesu i potpuno provedu Direktivu o razmjeni informacija.**

4. Otpornost na hibridne prijetnje i druge neprijateljske radnje

Otpornost na hibridne prijetnje povećat ćemo poboljšanjem zaštite kritične infrastrukture, jačanjem kibersigurnosti, zaštitom prometnih čvorišta i luka i suzbijanjem prijetnji na internetu.

Povećala se učestalost i sofisticiranost neprijateljskih radnji koje ugrožavaju sigurnost EU-a, a zlonamjerni akteri znatno su proširili raspon sredstava kojima se služe. Pojačane su hibridne kampanje usmjerene protiv EU-a, njegovih država članica i partnera, što uključuje sabotažu kritične infrastrukture, podmetanje požara, kibernetičke napade, uplitanja u izbore, inozemno upletanje i manipuliranje informacijama (FIMI), uključujući dezinformacije, i korištenje migracija kao oružja. Zbog svoje političke i operativne uloge i prirode informacija kojima raspolažu nisu pošteđene ni institucije, tijela, uredi i agencije Unije („subjekti Unije”).

EU mora **postati još otporniji** te i sada i u budućnosti djelotvorno koristiti postojeće alate i osmišljavati nove načine za suočavanje s tim rastućim prijetnjama koje dolaze i od državnih i od nedržavnih aktera.

Kritična infrastruktura

Prijetnje **kritičnoj infrastrukturi**, uključujući hibridne prijetnje kao što su sabotaža i zlonamjerne kibernetičke aktivnosti, velik su problem, posebno za promet i za infrastrukturu koja povezuje države članice, bilo da je riječ o interkonekcijskim vodovima ili prekograničnim komunikacijskim kabelima. Od početka agresivnog rata Rusije protiv Ukrajine, a posebno u 2024., povećan je broj sabotaža kritične infrastrukture, što je pogodilo brojne države članice. Suradnja tijela za izvršavanje zakonodavstva, službi za sigurnost i kibernetičku sigurnost, vojne i civilne zaštite i privatnih subjekata važna je za predviđanje, otkrivanje, sprečavanje i djelotvoran odgovor na takve radnje.

Smanjenje ranjivosti i jačanje otpornosti kritičnih subjekata nužno je za kontinuirano pružanje ključnih usluga koje su neophodne za gospodarstvo i društvo. Zbog toga je nužno da sve države članice što prije prenesu i pravilno provedu **Direktivu o otpornosti kritičnih subjekata**

(CER)[31] i **Direktivu o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (NIS2)**[32].

Radi brzog napretka Komisija će u suradnji sa **Skupinom za otpornost kritičnih subjekata i Skupinom za suradnju NIS** podupirati države članice u identifikaciji kritičnih subjekata[33] i razmjeni dobre prakse o nacionalnim strategijama i procjenama rizika u pogledu ključnih usluga. Bude li poremećaja u kritičnoj infrastrukturi sa znatnim prekograničnim posljedicama, odgovor na razini EU-a koordinirat će se u skladu s **Planom EU-a za kritičnu infrastrukturu**. Komisija potiče Vijeće da brzo donese **Plan EU-a za kibernetička pitanja**, koji će dodatno ojačati koordinaciju u kontekstu upravljanja krizama i pospješivati suradnju među tijelima u području fizičke i digitalne otpornosti. Nastavno na uspješna testiranja otpornosti energetskog sektora 2023. Komisija će promicati **dobrovoljna testiranja otpornosti** u drugim sektorima važnima za unutarnju sigurnost. Osim toga, Komisija će za osnovne usluge **sastaviti pregled prekograničnih i međusektorskih rizika na razini Unije** kako bi pomogla državama članicama u procjeni rizika i pridonijela sveobuhvatnoj procjeni rizika na razini EU-a. U skladu sa Strategijom za Uniju pripravnosti Komisija će istodobno surađivati s državama članicama kako bi identificirala ostale sektore i usluge koji nisu obuhvaćeni postojećim zakonodavstvom, a u odnosu na koje bi moglo biti potrebno djelovati.

Radna skupina EU-a i NATO-a za otpornost kritične infrastrukture uspostavila je izvrsnu suradnju u razmjeni najbolje prakse i jačanju otpornosti u sektorima energetike, promet, digitalne infrastrukture i svemira. Ta će se suradnja nastaviti u okviru **strukturiranog dijaloga EU-a i NATO-a o otpornosti**. **EU-ov paket instrumenata protiv hibridnih prijetnji** uvelike pomaže državama članicama i partnerima u pripremi na hibridne prijetnje i njihovu suzbijanju. **Timovi za brzi odgovor na hibridne prijetnje**[34] na zahtjev pružaju prilagođenu interventnu pomoć državama članicama i raznim misijama i partnerima EU-a. Nadalje, Komisija će nastaviti suradnju na razini EU-a u borbi protiv sabotaže provedbom stručnih aktivnosti[35], uključujući **namjenski zajednički program rada** za stručnjake kako bi se pojednostavnila razmjena informacija i utvrdile protumjere.

Incidenti na **podmorskim kabelima** u Europi ukazuju na potrebu za strožim mjerama i jasnijim odgovorima. Kao što je navedeno u **Akcijskom planu EU-a za sigurnost kabela**[36], Komisija će zajedno s Visokim predstavnikom surađivati s državama članicama, agencijama EU-a i partnerima kao što je NATO kako bi se spriječilo, otkrilo, odvraćalo i odgovorilo na ugrožavanje podmorskih kabela. Komisija će u stvaranju integrirane slike stanja prijetnji surađivati s državama članicama na razvoju i uvođenju, na dobrovoljnoj osnovi, integriranog mehanizma nadzora nad podmorskim kabelima u svakom morskom bazenu, počevši s regionalnim čvorištem za nordijsku/baltičku regiju.

[31] 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.
[32] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2).
[33] Direktiva obuhvaća sektore energetike, prometa, bankarstva, infrastrukture financijskog tržišta, zdravstva, vode za piće, otpadnih voda, digitalne infrastrukture, javne uprave, svemira te proizvodnje, prerade i distribucije hrane.
[34] Strateški kompas EU-a za sigurnost i obranu iz 2022., str. 22.
[35] EU-ovi Savjetnici za sigurnosnu zaštitu, Europska mreža za uklanjanje neeksplodiranih eksplozivnih sredstava (EEODN), mreža ATLAS, EU-ova mreža za zaštitu visokorizičnih javnih prostora (EU HRSN), Savjetodavna skupina za KBRN sigurnost, Skupina za otpornost kritičnih subjekata (CERG).
[36] JOIN (2025) 9 final.

Kibernetička sigurnost

Stalna prijetnja **zlonamjernih kibernetičkih aktivnosti**, koje su često dio šireg raspona višedimenzionalnih i hibridnih prijetnji, iziskuje stalnu pozornost i djelovanje na europskoj razini. Unija je posljednjih godina donijela niz propisa o kibernetičkoj sigurnosti, čiji je cilj jačanje kibernetičke otpornosti subjekata obuhvaćenih Direktivom NIS 2 koji djeluju u kritičnim sektorima EU-a i subjekata Unije[37], povećanje sigurnosti digitalnih proizvoda (Akt o kibernetičkoj otpornosti) i uspostavljanje okvira za potporu pripravnosti i odgovoru na incidente (Akt o kibernetičkoj solidarnosti). Komisija je u siječnju 2025. donijela **europski akcijski plan za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite**[38] kako bi se poboljšalo otkrivanje prijetnji, pripravnost i odgovor na krize. On se mora u potpunosti provesti. Kako bismo odgovorili na nove prijetnje i kretanja, istovremeno moramo pojačati svoje djelovanje, posebno u područjima razmjene informacija, sigurnosti lanca opskrbe, ucjenjivačkog softvera i kibernetičkih napada, kao i tehnološke suverenosti.

Nadalje, za provedbu je potrebno smanjiti sadašnji manjak od 299 000 stručnjaka u području kibernetičke sigurnosti. Komisija će u okviru unije vještina[39] surađivati s državama članicama na povećavanju radne snage u području kibernetičke sigurnosti, posebno angažmanom nove Akademije za vještine u području kibernetičke sigurnosti. Strateški plan za obrazovanje u području STEM-a[40] poboljšava dostupnost talenata i odgovor Europe na potrebe tržišta rada u području kibernetičke sigurnosti.

Usporedno s jačanjem svoje otpornosti EU će nastaviti u potpunosti koristiti okvir za zajednički diplomatski odgovor EU-a na zlonamjerne kibernetičke aktivnosti **(paket instrumenata za kibernetičku diplomaciju)** kako bi se spriječilo, odvraćalo i odgovorilo na kibernetičke prijetnje koje potječu od državnih i nedržavnih aktera.

Sigurnost lanaca opskrbe IKT-om

Paket instrumenata za sigurnost 5G tehnologije pruža relevantan okvir za zaštitu 5G mreža, ali ga države članice trenutačno nedovoljno primjenjuju. Neprihvatljivi sigurnosni rizici i dalje su prisutni, posebno u pogledu zamjene visokorizičnih dobavljača. Usklađenim pristupom sigurnosti lanca opskrbe IKT-om može se riješiti trenutačna fragmentiranost unutarnjeg tržišta uzrokovana različitim pristupima na nacionalnoj razini, izbjeći kritične ovisnosti i smanjiti rizik u našim lancima opskrbe IKT-om u odnosu na visokorizične dobavljače, čime se štiti naša kritična infrastruktura.

U skladu s tim pristupom u predstojećoj **reviziji Akta o kibernetičkoj sigurnosti** Komisija će šire razmotriti sigurnost i otpornost lanaca opskrbe i infrastrukture IKT-a. Osim toga, Komisija će predložiti poboljšanje **europskog okvira za kibernetičkosigurnosnu certifikaciju** kako bi se budući programi certifikacije mogli donijeti na vrijeme i tako odgovoriti na potrebe politike.

Na temelju dovršenih ili tekućih sektorskih procjena[41] Komisija će zajedno s državama članicama oblikovati **strateško planiranje za koordinirane procjene kibernetičkosigurnosnih rizika**.

[37] Uredba (EU, Euratom) 2023/2841 Europskog parlamenta i Vijeća od 13. prosinca 2023. o utvrđivanju mjera za visoku zajedničku razinu kibernetičke sigurnosti u institucijama, tijelima, uredima i agencijama Unije, SL L, 2023/2841, 18.12.2023.

[38] https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.

[39] COM (2025)90 final.

[40] COM(2025) 89 final.

[41] Kao što su 5G mreže, telekomunikacije, električna energija, energija iz obnovljivih izvora i umrežena vozila.

Usluge računalstva u oblaku i telekomunikacijske usluge postale su glavni element u lancima opskrbe za kritičnu infrastrukturu, poduzeća i javna tijela. Komisija će poduzeti mjere kako bi potaknula kritične subjekte da odabiru **usluge računalstva u oblaku i telekomunikacijske usluge koje nude odgovarajuću razinu kibernetičke sigurnosti**, uzimajući u obzir ne samo tehničke rizike nego i strateške rizike i ovisnosti.

Ucjenjivački softver i kibernetički napadi

Ucjenjivački softver jedan je od trajnih ozbiljnih problema kibernetičke sigurnosti u EU-u i svijetu. U jednom se izvješću procjenjuje se da će do 2031. prouzročiti godišnju štetu u vrijednosti većoj od 250 milijardi EUR na svjetskoj razini[42]. **Direktiva NIS 2** i **Akt o kibernetičkoj otpornosti** znatno će poboljšati sigurnosni položaj subjekata i time mrežama ucjenjivačkog softvera povećati troškove napada. Osim toga, Komisija će blisko surađivati s državama članicama kako bi se osiguralo da se tijelima za izvršavanje zakonodavstva prijavljuje više napada ucjenjivačkim softverom, posebno onih u kojima je riječ o naprednim trajnim prijetnjama, i plaćanja otkupnine, što bi olakšavalo istrage.

Kako bi se spriječili i zaustavili kibernetički napadi, EU treba bolje zaštititi razmjenu informacija između tijela za izvršavanje zakonodavstva, tijela i subjekata za kibernetičku sigurnost i privatnih subjekata, pod okriljem Europola i Agencije EU-a za kibersigurnost (ENISA).

Europol i Eurojust trebali bi nastaviti svoj uspješni rad na gašenju mreža ucjenjivačkog softvera i tako pridonijeti suradnji tijela za izvršavanje zakonodavstva. U tu bi svrhu tijela za izvršavanje zakonodavstva trebala u najvećoj mogućoj mjeri iskorištavati mehanizme suradnje, uključujući **Europolov Međunarodni model odgovora na ucjenjivački softver** i **Međunarodnu inicijativu za suzbijanje napada ucjenjivačkim softverom (CRI)**[43], a ENISA i Europol trebali bi surađivati na proširenju repozitorija alata za dešifriranje za razne tipove ucjenjivačkog softvera[44].

Tehnološka suverenost

Kibernetička sigurnost i tehnološka suverenost usko su povezane, a rješavanje problema tehnološke ovisnosti treba biti prioritet. Unija mora **usmjeravati razvoj i uvođenje novih tehnologija**, pri čemu će Komisija raditi na **poboljšanju kapaciteta u područjima strateških tehnologija** kao što su umjetna inteligencija, kvantna tehnologija, napredna povezivost, računalstvo u oblaku, računalstvo na rubu mreže i internet stvari[45], i to provedbom budućih inicijativa kao što su Akcijski plan za „kontinent umjetne inteligencije", kvantna strategija i druge[46]. Komisija će nastaviti podupirati pravodobno uvođenje najnovijih međunarodno dogovorenih **internetskih protokola** koji su ključni za održavanje prilagodljivog i učinkovitog interneta s povećanom razinom kibernetičke sigurnosti. Za hvatanje ukoštac s **problemima u području radiofrekvencijskog spektra**, na primjer s lažiranjem signala GNSS-a, ometanjem, rizicima i ovisnostima u lancu opskrbe, potrebne su i dodatne mjere kao što su upotreba tehnologija kvantnog opažanja i razvoj kapaciteta za praćenje radijskih frekvencija.

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Dostupno putem projekta „No More Ransom", https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] Npr. zajedničko poduzeće EuropHPC https://eurohpc-ju.europa.eu/index_en, početna stranica vodećeg projekta Quantum | vodeći projekt Quantum, mreže 3C (COM(2024) 81 final) i Akcijski plan EU-a za sigurnost kabela (JOIN(2025) 9 final).

Uvođenje rješenja za **postkvantnu kriptografiju** (PQC) bit će od iznimne važnosti za zaštitu osjetljivih komunikacija, podataka u mirovanju i digitalnih identiteta u novom kvantnom dobu. Na temelju Preporuke o planu koordiniranog prelaska na postkvantnu kriptografiju[47] iz 2024. Komisija surađuje s državama članicama na poticanju te tranzicije. U tom bi pogledu države članice trebale utvrditi visokorizične elemente u kritičnim subjektima i što prije, a najkasnije do kraja 2030., za njih osigurati šifriranje otporno na kvantnu tehnologiju. Komisija surađuje i s državama članicama i Europskom svemirskom agencijom (ESA) na razvoju i uvođenju **europske infrastrukture za kvantnu komunikaciju (EuroQCI)**[48] na temelju distribucije kvantnih ključeva (QKD) u okviru programa EU-a za sigurnu povezivost **IRIS²**. Obje će inicijative u konačnici subjektima omogućiti siguran prijenos podataka i pohranu informacija.

Kvantne tehnologije imat će važnu ulogu i u sigurnosnim primjenama: kao dio **kvantne strategije** izradit će se **plan za kvantno opažanje u sigurnosnim primjenama**. Komisija će ujedno raditi na postizanju otpornosti svojih korporativnih sustava neophodnih za sigurnost, uključujući svoje klasificirane informatičke sustave, na kvantnu tehnologiju.

Okvir za kibernetičku sigurnost prilagođen poslovanju

Predstojeća revizija Akta o kibernetičkoj sigurnosti prilika je za **pojednostavnjenje zakonodavstva EU-a o kibernetičkoj sigurnosti**, u skladu s Kompasom konkurentnosti. Komisija će blisko surađivati s državama članicama kako bi se osigurala brza, dosljedna i poslovanju prilagođena provedba horizontalnog okvira za kibernetičku sigurnost utvrđenog u Direktivi NIS 2, Aktu o kibernetičkoj otpornosti i Aktu o kibernetičkoj solidarnosti, uz promicanje jednostavnosti i usklađenosti i izbjegavanje fragmentacije ili udvostručavanja pravila o kibernetičkoj sigurnosti u zakonodavstvu EU-a i nacionalnim propisima.

Kako bi se omogućio siguran pristup internetskim uslugama i povećala digitalna sigurnost u cijelom EU-u, **europski okvir za digitalni identitet** omogućit će do kraja 2026. svim građanima i stanovnicima EU-a pouzdane lisnice za digitalni identitet. Skorašnje uvođenje **europske poslovne lisnice** olakšat će sigurne prekogranične interakcije između poduzeća i javnih uprava. Oboje je preduvjet za sigurno i učinkovitije funkcioniranje jedinstvenog tržišta temeljenog na podacima s alatima kao što su jedinstveni digitalni pristupnik, elektroničko izdavanje računa, e-nabava i digitalna putovnica za proizvode.

Sigurnost na internetu

Neke od najozbiljnijih hibridnih prijetnji koje ugrožavaju sigurnost i zaštitu ljudi u Europi i koje su usmjerene na demokratsku sferu EU-a pojavljuju se na internetu. Te prijetnje uključuju nezakonite aktivnosti i nezakoniti sadržaj na internetu, manipulaciju informacijama koja uključuje umjetno isticanje, zavaravajuće informacije i inozemno upletanje i manipuliranje informacijama.

Stroga provedba **Akta o digitalnim uslugama (DSA)** ključna je za ostvarivanje sigurnog i pristupačnog internetskog okruženja s odgovornim akterima, koje je ujedno otporno i na hibridne prijetnje. Taj akt obvezuje pružatelje vrlo velikih internetskih platformi i vrlo velikih internetskih tražilica da provode procjene rizika i uvode mjere za smanjenje sistemskih rizika koji proizlaze iz dizajna, funkcioniranja ili korištenja njihovih usluga. Neki su od tih rizika negativni učinci na građanski diskurs i izborne procese, kao i na javnu sigurnost, kao što je dalekosežno uplitanje zlonamjernih stranih državnih aktera, na primjer u izborne procese. Bitno je da se nadležna tijela država članica osposobljavaju o upotrebi pravnih sredstava za brzo uklanjanje nezakonitog sadržaja na internetu, posebno rodno uvjetovanog nasilja. U Aktu o digitalnim uslugama predviđa se mehanizam za odgovor na krizu, koji se može aktivirati ako

[47] Preporuka o planu koordiniranog prelaska na postkvantnu kriptografiju | Izgradnja digitalne budućnosti Europe.
[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

izvanredne okolnosti dovedu do ozbiljne prijetnje javnoj sigurnosti ili javnom zdravlju u Uniji ili u njezinim većim dijelovima. Za dopunu tom mehanizmu Komisija i nacionalna nadležna tijela imenovana koordinatorima za digitalne usluge razvili su i dobrovoljni **okvir za odgovor na incidente u okviru Akta o digitalnim uslugama**. Koordinatori za digitalne usluge poduzeli su i mjere za zaštitu integriteta izbora, primjerice organiziranje okruglih stolova i testiranje otpornosti[49]. Akt o digitalnim uslugama i zajedno s njim Uredba o političkom oglašavanju[50] neke su od sastavnica povezanih sa zaštitom demokracije i integriteta demokratskih procesa, koji su osjetljivi na utjecaj zlonamjernih aktera ostvaren, među ostalim, korištenjem digitalnih alata i djelovanjem na društvenim mrežama.

Provedba paketa instrumenata za borbu protiv **inozemnog upletanja i manipuliranja informacijama** još je jedna važna sastavnica koja nudi potporu na razini EU-a. Potpora digitalnoj i medijskoj pismenosti i kritičkom razmišljanju također su važan element tih nastojanja.[51]

Suzbijanje korištenja migracija kao oružja

Rusija je uz pomoć i odlučnu potporu Bjelarusa namjerno koristila migracije kao oružje i nezakonito poticala migracijske tokove prema vanjskim granicama EU-a s ciljem destabilizacije naših društava i ugrožavanja jedinstva Europske unije. To ugrožava ne samo nacionalnu sigurnost i suverenost država članica, nego i sigurnost i cjelovitost šengenskog područja i sigurnost Unije u cjelini. U zaključcima iz listopada 2024. Europsko vijeće naglasilo je da se Rusiji i Bjelarusu, kao ni bilo kojoj drugoj zemlji, ne smije dopustiti da zlorabe naše vrijednosti, uključujući pravo na azil, i da podrivaju našu demokraciju.

Kako je navedeno u Komunikaciji Komisije iz 2024. o korištenju migracija kao oružja, Unija je, uz snažnu političku potporu, poduzela financijske, operativne i diplomatske mjere, uključujući suradnju sa zemljama podrijetla i tranzitnim zemljama migranata, kako bi djelotvorno odgovorila na te prijetnje[52]. Taj odgovor uključuje korištenje novog okvira koji je uspostavilo Vijeće za sankcioniranje pojedinaca i organizacija uključenih u djelovanja i politike kao što je rusko korištenje migracija kao oružja tako što će im se zamrzavati imovina i zabranjivati putovanja[53]. EU će prema potrebi nastaviti primjenjivati taj okvir i podupirati države članice u suzbijanju te prijetnje.

Prometna sigurnost

Morske i zračne luke i kopnena infrastruktura bitne su ulazne i izlazne točke. Imaju važnu ulogu u gospodarstvu i društvu EU-a i u vojnoj mobilnosti. Međutim, ta prometna čvorišta i prijevozna sredstva ujedno su glavna meta vanjskih prijetnji i kriminalnih aktivnosti. Nedavni incidenti, uključujući povredu sigurnosti zračnog prijevoza tereta i napade na željezničku infrastrukturu, ukazuju na ozbiljne rizike. **Prijevoznici** mogu biti i mete i instrumenti za zlonamjerne aktere. Postojeći pravni instrumenti EU-a unaprijedili su zaštitu zračnog prometa[54], ali zbog visoke razine prijetnje civilnom zrakoplovstvu potrebna su sredstva za predviđanje incidenata i brzo savjetovanje s relevantnim državama članicama. Komisija će surađivati s državama članicama

[49] Paket alata za izbore za koordinatore digitalnih usluga 2025. https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Uredba (EU) 2024/900 Europskog parlamenta i Vijeća od 13. ožujka 2024. o transparentnosti i ciljanju u političkom oglašavanju, SL L, 2024/900, 20.3.2024.
[51] Akcijski plan za digitalno obrazovanje (2021. – 2027.) – europski prostor obrazovanja.
[52] COM(2024) 570 final.
[53] Uredba Vijeća (EU) 2024/2642 od 8. listopada 2024. o mjerama ograničavanja s obzirom na destabilizirajuće aktivnosti Rusije, ST/8744/2024/INIT, SL L, 2024/2642, 9.10.2024.
[54] Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa, SL L 97, 9.4.2008., str. 72.

na izmjeni postojećeg provedbenog zakonodavstva u području zaštite zračnog prometa radi razmjene klasificiranih podataka o **događajima relevantnima za zaštitu zračnog prometa**. Osim toga, Komisija će razmotriti **regulatorne mjere** za suzbijanje novih prijetnji kao što su **incidenti u zračnom prijevozu tereta** i za jačanje standarda zaštite zračnog prometa. To će uključivati i poboljšano **zakonodavstvo o zaštiti zračnog prometa (AVSEC)** radi omogućivanja hitnih reakcija i uz zadržavanje objedinjenog područja zaštite u zračnim lukama EU-a.

Pri izradi predstojeće **strategije EU-a za luke**, oblikovane na temelju **Europskog saveza luka**, Komisija će razmotriti načine za daljnje poboljšanje zakonodavstva o pomorskoj sigurnosti kako bi se djelotvorno odgovorilo na nove prijetnje, osigurale luke i poboljšala sigurnost lanca opskrbe EU-a. Da bi se to postiglo, Komisija će se pobrinuti za strogu provedbu tih pravila i raditi na usklađivanju nacionalne prakse i jačanju sigurnosnih provjera u lukama. Komisija će surađivati s državama članicama i privatnim sektorom na proširenju sigurnosnih protokola za zaštitu zračnog prijevoza tereta na zaštitu pomorskog prijevoznog lanca.

Predloženo carinsko tijelo EU-a analizirat će i procjenjivati rizike na temelju **carinskih informacija** o robi koja ulazi u EU, izlazi iz njega i provozi se kroz njega kako bi se državama članicama pomoglo u sprečavanju zlonamjernih aktera da iskorištavaju međunarodne lance opskrbe. U skladu sa Strategijom pomorske sigurnosti EU-a[55] budući **Europski pakt o oceanima** bit će iznimno važan za jačanje pomorske sigurnosti u morskim bazenima oko EU-a i udaljenima od EU-a, među ostalim zato što će poticati proširenje višenamjenskih pomorskih operacija i vježbi.

Otpornost lanaca opskrbe

Europa se treba manje oslanjati na tehnologije iz trećih zemalja jer to može dovesti do ovisnosti i sigurnosnih rizika. Komisija nastoji ublažiti ovisnosti o samo jednom stranom dobavljaču, smanjiti rizik za naše lance opskrbe od visokorizičnih dobavljača i zaštititi kritičnu infrastrukturu i industrijske kapacitete u EU-u, kako je navedeno u **Kompasu konkurentnosti**[56] i **Planu za čistu industriju**[57]. Komisija će u suradnji s EU-ovim industrijama u ključnim sektorima (npr. prometna čvorišta, kritična infrastruktura) promicati **industrijsku politiku za unutarnju sigurnost** kako bi se proizvela sigurnosna rješenja kao što su oprema za otkrivanje, biometrijske tehnologije i bespilotni zrakoplovi sa značajkama integrirane sigurnosti. Pri **preispitivanju pravila EU-a o javnoj nabavi** Komisija će procijeniti jesu li sigurnosne odredbe iz Direktive o javnoj nabavi u području obrane i sigurnosti iz 2009.[58] dovoljne za ispunjavanje potreba tijela za izvršavanje zakonodavstva i kritičnih subjekata u pogledu otpornosti.

Komisija će podupirati države članice u **provjeri izravnih stranih ulaganja** i nabavi opreme za logistička čvorišta tako što će se pobrinuti za sigurnost kritične infrastrukture i tehnologije.

Nakon što se počne primjenjivati, **Akt o izvanrednim okolnostima i otpornosti na unutarnjem tržištu (IMERA)** pomoći će EU-u u upravljanju krizama koje ometaju ključne lance opskrbe i slobodno kretanje robe, usluga i osoba. Omogućit će brzu koordinaciju u kriznim situacijama, određivanje robe i usluga relevantnih u slučaju krize te pružiti paket instrumenata za osiguravanje njihove dostupnosti. Nadalje, Komisija će u bliskoj suradnji s

[55] JOIN(2023) 8 final.
[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Direktiva 2009/81/EZ o usklađivanju postupaka nabave za određene ugovore o radovima, ugovore o nabavi robe i ugovore o uslugama koje sklapaju javni naručitelji ili naručitelji u području obrane i sigurnosti, SL L 216, 20.8.2009.

državama članicama predložiti uspostavu **višeagencijskog mehanizma upozoravanja o sigurnosti prometa i lanca opskrbe** kako bi se zajamčila sigurna i pravodobna razmjena relevantnih informacija za predviđanje i suzbijanje prijetnji.

Osim toga, uz provedbu Akta o kritičnim sirovinama i akta o industriji s nultom neto stopom emisija povećana primjena kriterija održivosti, otpornosti i europske preferencije u javnoj nabavi EU-a potaknut će razvoj vodećih tržišta. Jače trgovinske veze, primjerice u okviru partnerstava za sirovine i partnerstava za čistu trgovinu i ulaganja, pridonijet će diversifikaciji lanaca opskrbe.

Otpornost i pripravnost na kemijske, biološke, radiološke i nuklearne prijetnje

Agresivni rat Rusije protiv Ukrajine povećao je rizik od **kemijskih, bioloških, radioloških i nuklearnih prijetnji**. Kako bi se riješio problem moguće nabave i korištenja kemijskih, bioloških, radioloških i nuklearnih materijala kao oružja, Komisija će podupirati države članice i partnerske zemlje ciljanim osposobljavanjem i vježbama. Ojačat će kapacitete za pripravnost i odgovor na kemijske, biološke, radiološke i nuklearne prijetnje, utvrditi prioritetne prijetnje, financirati inovacije za protumjere, osigurati kapacitete sustava rescEU i stvoriti zalihe medicinske opreme, i to u okviru novog **akcijskog plana pripravnosti i odgovora na kemijske, biološke, radiološke i nuklearne prijetnje**. Osim toga, **strategija EU-a za medicinske protumjere** poduprijet će razvoj medicinskih protumjera, od istraživanja do proizvodnje i distribucije, kako bi se EU zaštitio od pandemija i kemijskih, bioloških, radioloških i nuklearnih prijetnji.

Nakon iskustva s pandemijom bolesti COVID-19 EU je ojačao okvir za zdravstvenu sigurnost[59]. Komisija određuje referentne laboratorije EU-a u javnom zdravstvu kako bi ojačala kapacitete za nadzor i brzo otkrivanje na razini EU-a i na nacionalnoj razini. Plan Unije za pripravnost, prevenciju i odgovor u području zdravstvene sigurnosti bit će objavljen 2025.

Ključne mjere

Komisija će:

- **u 2025. preispitati Akt o kibernetičkoj sigurnosti,**
- **izraditi mjere za kibernetičku sigurnost pri korištenju usluga računalstva u oblaku,**
- **u 2025. predložiti strategiju EU-a za luke,**
- **u 2026. preispitati pravila EU-a o javnoj nabavi u području obrane i sigurnosti,**
- **u 2026. iznijeti novi akcijski plan pripravnosti i odgovora na kemijske, biološke, radiološke i nuklearne prijetnje.**

Komisija će u suradnji s državama članicama:

- **razviti i uvesti europsku infrastrukturu za kvantnu komunikaciju (EuroQCI),**
- **osigurati djelotvornu provedbu Akta o digitalnim uslugama,**
- **raditi na suzbijanju korištenja migracija kao oružja,**
- **uspostaviti sustav zaštite zračnog prometa u slučaju sigurnosnih incidenata,**
- **raditi na uspostavi višeagencijskog mehanizma upozoravanja o sigurnosti prometa i lanca opskrbe.**

Vijeće se poziva da:

- **donese preporuku Vijeća o Planu EU-a za kibernetičku sigurnost.**

Države članice pozivaju se da:

[59] Posebice Uredbom (EU) 2022/2371 o ozbiljnim prekograničnim prijetnjama zdravlju.

- **prenesu i u potpunosti provode direktive CER i NIS 2.**

5. Intenziviranje borbe protiv teškog i organiziranog kriminala

Iskorjenjivanju organiziranog kriminala pridonijet ćemo predlaganjem strožih pravila za borbu protiv organiziranih kriminalnih skupina, uključujući istrage, smanjenjem izloženosti mladih u EU-u novačenju u kriminal te jačanjem mjera za lišavanje kriminalaca alata i imovine.

Organizirani kriminal iskorištava okruženje koje se mijenja i drastično širi. Koristi napredne tehnologije, djeluje u više jurisdikcija i ima snažne veze izvan granica EU-a. S obzirom na te složene transnacionalne prijetnje iznimno je važna koordinacija i potpora na razini EU-a.

Sprečavanje kriminala

Novačenje mladih u organizirani kriminal sve je veći problem u EU-u. Za suzbijanje organiziranog kriminala potrebno je ukloniti njegove **temeljne uzroke** i pružiti edukaciju i alternative kriminalnom životu kroz pristup koji obuhvaća cijelo društvo. Komisija će podupirati uključivanje sigurnosnih pitanja u politiku obrazovanja, socijalnu politiku, politiku zapošljavanja i regionalnu politiku EU-a. EU će **promicati politike za sprečavanje kriminala utemeljene na dokazima**[60] i prilagođene lokalnim kontekstima.

Kako bi se korisnici internetskih usluga, a posebice maloljetnici, zaštitili, među ostalim, od seksualnih zlostavljača djece, trgovaca ljudima i novačenja na internetu u kriminal ili nasilni ekstremizam, mjerama iz **Akta o digitalnim uslugama** od pružatelja internetskih platformi dostupnih maloljetnicima zahtijeva se da upravljaju rizicima i reagiraju na nezakonit sadržaj, uključujući govor mržnje. Komisija planira izdati **smjernice o zaštiti maloljetnika** kako bi pružateljima internetskih platformi pomogla da osiguraju visoku razinu privatnosti, sigurnosti i zaštite maloljetnika na internetu. Smjernice će sadržavati niz preporuka za bolju zaštitu maloljetnika na internetu za sve digitalne usluge koje se pružaju u Uniji. Komisija 2025. planira izraditi rješenje za **provjeru dobi kojim se štiti privatnost** kao privremenu mjeru do uvođenja europske lisnice za digitalni identitet krajem 2026. Komisija će predstaviti i akcijski plan za borbu protiv zlostavljanja na internetu.

Nadalje, nastavit će podupirati dobrovoljnu suradnju više dionika s internetskim platformama i drugim relevantnim akterima, među ostalim putem internetskog foruma EU-a i ciljanih kodeksa ponašanja u skladu s Aktom o digitalnim uslugama, kao što je Kodeks ponašanja u slučaju nezakonitog govora mržnje na internetu iz 2025. Cilj je informiranje, zajednički odgovor na postojeće i nove prijetnje te izrada i razmjena dobrih primjera iz prakse za mjere ublažavanja.

Utjecaj organiziranog kriminala na lokalnoj razini ukazuje na potrebu za regionalnim rješenjima za smanjenje ranjivosti i privlačnosti nezakonitih aktivnosti. Program EU-a za gradove bavit će se sigurnosnim problemima u gradovima na temelju inicijative „Gradovi EU-a protiv radikalizacije”. Komisija će sredstvima iz Europskog fonda za regionalni razvoj podupirati države članice u poboljšanju urbane i regionalne sigurnosti.

Kvalitetnije obrazovanje i vještine temelj su otpornih i povezanih društava. Zahvaljujući **uniji vještina** i **akcijskom planu za integraciju i uključivanje** Unija će pomoći ljudima da postanu otporniji na pogrešne informacije i dezinformacije, radikalizaciju i novačenje u kriminal.

Zaštita djece od svih oblika nasilja, uključujući kriminal te fizičko ili mentalno nasilje u virtualnom i stvarnom svijetu, temeljni je cilj EU-a. Kako bi se odgovorilo na potrebe posebno ranjivih skupina kao što su djeca, koja su sve izloženija novačenju i radikalizaciji, mamljenju i

[60] https://www.eucpn.org/.

seksualnom zlostavljanju, zlostavljanju na internetu, dezinformacijama i drugim prijetnjama, EU će izraditi **akcijski plan za zaštitu djece od kriminala**, koji će obuhvaćati aktivnosti na internetu i izvan njega. Odredit će se dosljedan i koordiniran pristup koji se temelji na dostupnim okvirima i alatima, uključujući budući EU-ov Centar za sprečavanje i suzbijanje seksualnog zlostavljanja djece i druga tijela i agencije EU-a, te će se predložiti daljnji koraci u područjima u kojima i dalje postoje nedostaci.

Razbijanje kriminalnih mreža i njihovih pomagača

Potrebno je intenzivirati borbu protiv kriminalnih mreža visokog rizika te njihovih vođa i pomagača. Unatoč zamjetnom nedavnom uspjehu[61], zastarjela pravila i nedosljedne definicije kriminalnih mreža otežavaju učinkovit kaznenopravni odgovor i prekograničnu suradnju. Komisija će revidirati zastarjelo zakonodavstvo u tom području i predložiti obnovljeni **pravni okvir o organiziranom kriminalu** radi jačanja odgovora.

Izvršenje upravnih mjera može dopuniti kazneni progon i dovesti do bržeg ostvarenja rezultata, kao što su pokazali EPPO i Europski ured za borbu protiv prijevara (OLAF) u **suzbijanju prekograničnih prijevara i kaznenih djela protiv financijskih interesa EU-a**. Počinitelji prijevara u području subvencija ciljaju na sektore kao što su obnovljiva energija, istraživački programi i poljoprivreda[62]. Komisija će istražiti načine za koordiniranu upotrebu kaznenih i administrativnih instrumenata kako bi se intenzivirala suradnja s Europolom, Eurojustom i EPPO-om. Osim toga, nastavit će podupirati širu primjenu **administrativnog pristupa** kako bi se lokalnim i drugim upravnim tijelima olakšalo sprečavanje infiltracije kriminala[63].

EU radi na jačanju svojeg pravnog okvira za borbu protiv **korupcije**[64]. Europski parlament i Vijeće trebali bi brzo zaključiti pregovore o ažuriranom okviru za borbu protiv korupcije koji je predložila Komisija. Komisija će iznijeti strategiju EU-a za borbu protiv korupcije kako bi povećala integritet i poboljšala koordinaciju među svim relevantnim tijelima i dionicima u tom području.

Vatreno oružje ima važnu ulogu u porastu nasilja organiziranih kriminalnih skupina. Komisija će predložiti zajedničke kaznenopravne standarde o nezakonitoj trgovini vatrenim oružjem. U središtu novog **akcijskog plana EU-a za kontrolu trgovine vatrenim oružjem** bit će zaštita zakonitog tržišta, ograničavanje kriminalnih aktivnosti na temelju boljih obavještajnih podataka i jačanje međunarodne suradnje s posebnim naglaskom na Ukrajinu i zapadni Balkan.

Kad je riječ o pirotehničkim sredstvima kojima se nezakonito trguje i koja se upotrebljavaju u kaznenim djelima, potrebne su mjere za poboljšanje prevencije i sljedivosti. Komisija trenutačno ocjenjuje Direktivu o pirotehničkim sredstvima i razmotrit će **kaznene sankcije za trgovinu pirotehničkim sredstvima**.

Praćenje novca

Praćenje novca ključno je za borbu protiv organiziranog kriminala i terorizma, ali je i dalje vrlo zahtjevno. Kad je riječ o vezi između organiziranog kriminala i novčanih tokova, potreban

[61] Uključujući nedavne slučajeve u okviru EMPACT-a.
[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.
[64] Prijedlog Direktive Europskog parlamenta i Vijeća o borbi protiv korupcije, zamjeni Okvirne odluke Vijeća 2003/568/PUP i Konvencije o borbi protiv korupcije koja uključuje dužnosnike Europskih zajednica ili dužnosnike država članica Europske unije te o izmjeni Direktive (EU) 2017/1371 Europskog parlamenta i Vijeća, COM(2023) 234 final, Bruxelles 3.5.2023.

je intenzivan i udružen rad da se zaustavi pristup kriminalnih mreža izvorima financiranja i bolje zaštite ljudi, poduzeća i javni proračuni.

EU je pojačao svoj angažman novim pravilima o sprečavanju pranja novca, uključujući osnivanje **tijela EU-a za sprečavanje pranja novca (AMLA)**[65]. Suradnja AMLA-e, OLAF-a, EPPO-a, Eurojusta i Europola neophodna je za provedbu djelotvornih financijskih istraga. Komisija će podržati uspostavu **partnerstava**, kako onih koja potiču međuagencijsku suradnju tako i onih koja uključuju privatni sektor.

Kako bi se uklonili financijski motivi koji stoje iza organiziranog kriminala, iznimno je važno zaplijeniti imovinu i oduzeti imovinsku korist stečenu kriminalom. Države članice trebale bi bez odgode prenijeti nedavno donesena stroža pravila o **povratu i oduzimanju imovine**[66] te ih u potpunosti provoditi. U borbi protiv paralelnih financijskih sustava koji zaobilaze EU-ov okvir za sprečavanje pranja novca, uključujući sustave koji se temelje na kriptoimovini, potrebne su inovativne mjere, razmjena najboljih primjera iz prakse među državama članicama i jača potpora Europola i Eurojusta. Komisija će istražiti bi li se mogao uvesti novi sustav na razini EU-a za praćenje dobiti od organiziranog kriminala i financiranja terorizma te će poticati pravovremene i proširene protoke informacija od **financijsko-obavještajnih jedinica** do tijela za izvršavanje zakonodavstva. Komisija će istražiti načine za popunjavanje praznina, poduprijeti države članice u izgradnji kapaciteta te nastaviti raditi na jačanju suradnje s trećim zemljama koje kriminalci zloupotrebljavaju za ilegalno bankarsko poslovanje.

Borba protiv teških kaznenih djela

Osim razbijanja kriminalnih mreža, za borbu protiv teških kaznenih djela potrebne su ciljane mjere. Kako bismo bili u mogućnosti intenzivnije se boriti protiv **internetskih prijevara**, koje uzrokuju veliku financijsku štetu[67], Komisija će podržati preventivne mjere i učinkovitije djelovanje tijela kaznenog progona te će surađivati s državama članicama i dionicima u podupiranju i zaštiti žrtava, uključujući pružanje pomoći za povrat imovine. Ta će se nastojanja formalizirati u **akcijskom planu za borbu protiv prijevara na internetu**.

Nadovezujući se na strategiju EU-a za borbu protiv **seksualnog zlostavljanja djece** za razdoblje 2020. – 2025.[68], Komisija će podupirati rad suzakonodavaca, koji bi trebali dovršiti zakonodavne prijedloge[69] za sprečavanje i suzbijanje seksualnog zlostavljanja djece na internetu te za djelotvorniju provedbu mjera kaznenog progona u slučajevima seksualnog zlostavljanja i iskorištavanja djece. Privremena pravila na snazi su do travnja 2026. pa je iznimno važno uspostaviti trajni pravni okvir. Komisija potiče suzakonodavce da započnu pregovore o nacrtu Uredbe o utvrđivanju pravila za sprečavanje i suzbijanje seksualnog zlostavljanja djece. Suzakonodavci se pozivaju da ostvare napredak i u pregovorima o Direktivi o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i materijala koji sadržava seksualno zlostavljanje djece, u kojoj će se utvrditi minimalna pravila za definiranje kaznenih djela i sankcija u području seksualnog iskorištavanja djece.

Polovina najopasnijih kriminalnih mreža u EU-u uključena je u nasilnu **trgovinu drogom**. Premda je EU nedavno intenzivirao borbu protiv tog oblika kriminala[70], posebice proširenjem mandata **Agencije EU-a za droge,** potrebne su daljnje mjere. Komisija će u bliskoj suradnji s državama članicama predložiti novu **strategiju EU-a u području droga**. Revidirat će **pravni**

[65] https://www.amla.europa.eu/index_hr.
[66] Direktiva (EU) 2024/1260 Europskog parlamenta i Vijeća od 24. travnja 2024. o povratu i oduzimanju imovine, SL L, 2024/1260, 2.5.2024.
[67] Globalno izvješće o borbi protiv prijevara za 2024.
[68] COM(2020) 607 final
[69] COM(2022) 209 final i COM(2024) 60 final.
[70] COM(2023) 641 final.

okvir za prekursore za droge i predložiti **akcijski plan EU-a za borbu protiv trgovine drogom** kako bi se prekinule rute i poslovni modeli. **Javno-privatno partnerstvo Europskog saveza luka** za pojačanu zaštitu luka proširit će se na manje luke i luke unutarnjih plovnih putova te će se osigurati provedba pravila pomorske sigurnosti. Prepoznajući ozbiljne lokalne posljedice trgovine drogom, Komisija će nastaviti podupirati uravnoteženu i multidisciplinarnu politiku o drogama utemeljenu na dokazima, koja je spremna reagirati na iznenadne priljeve droga, posebice sintetičkih opojnih droga.

EU je u borbi protiv iskorištavanja ljudi donio nova pravila[71] i uvest će **obnovljenu strategiju EU-a za suzbijanje trgovine ljudima** (2026. – 2030.), koja će obuhvaćati sve faze, od prevencije do kaznenog progona, a u prvom će planu biti potpora žrtvama na razini EU-a i na međunarodnoj razini.

Komisija će u okviru borbe protiv **krijumčarenja migranata** u suradnji s Europolom, Eurojustom i Frontexom predvoditi rad s ključnim partnerima u okviru novog globalnog saveza za borbu protiv krijumčarenja migranata, uključujući na internetu. Komisijine prijedloge o suzbijanju krijumčarenja[72] trebalo bi što prije donijeti i provesti. Osim toga, Komisija je nakon donošenja **paketa instrumenata za prijevoznike**[73] proširila odnose sa stranim tijelima i prijevoznicima, a nastavit će i surađivati sa zrakoplovnom industrijom i organizacijama civilnog zrakoplovstva[74] na informiranju o krijumčarenju migranata zračnim putem[75].

Kaznena djela protiv okoliša dugoročno ugrožavaju okoliš, javno zdravlje i gospodarstva. Komisija će podupirati države članice u provedbi Direktive o zaštiti okoliša putem kaznenog prava[76] i ojačati operativne mreže i mjere u tom području[77]. Iznimno je važno da provedba bude dosljedna. Osim toga, nedavno donesena Konvencija Vijeća Europe o zaštiti okoliša putem kaznenog prava[78] doprinijet će poduzimanju strogih i usporedivih mjera za borbu protiv kaznenih djela protiv okoliša u Europi i šire.

Kaznenopravni odgovor

Kriminal i terorizam mogu utjecati na svakoga pa je neophodno podupirati **žrtve** i štititi njihova prava kako bi se smanjila šteta i povećala opća sigurnost i povjerenje u vlasti. Komisija će na temelju Direktive o pravima žrtava uvesti novu **strategiju EU-a za prava žrtava**.

Kaznenopravnim sustavima EU-a potrebni su djelotvorni alati za odgovor na nove prijetnje. Kako bi se to postiglo, Komisija je pokrenula **Forum na visokoj razini o budućnosti kaznenog pravosuđa u EU-u**. Taj forum okuplja države članice, Europski parlament, agencije i tijela EU-a i druge relevantne dionike. Cilj mu je raspravljati o tome kako osigurati da naši kaznenopravni sustavi ostanu djelotvorni, pravedni i otporni na nove izazove, a da se

[71] Direktiva (EU) 2024/1712 od 13. lipnja 2024. o izmjeni Direktive 2011/36/EU o sprečavanju i suzbijanju trgovanja ljudima i zaštiti njegovih žrtava, SL L, 2024/1712, 24.6.2024.
[72] COM(2023) 755 final i COM(2023) 754 final.
[73] Paket instrumenata za rješavanje problema korištenja komercijalnih prijevoznih sredstava za nezakonite migracije.
[74] Uključujući Međunarodnu organizaciju civilnog zrakoplovstva (ICAO).
[75] Komisija će također podupirati dovršetak Uredbe o mjerama protiv prijevoznika koji sudjeluju u trgovini ljudima ili krijumčarenju migranata ili ih olakšavaju, COM(2021) 753 final.
[76] Direktiva (EU) 2024/1203 Europskog parlamenta i Vijeća od 11. travnja 2024. o zaštiti okoliša putem kaznenog prava, SL L, 2024/1203, 30.4.2024.
[77] Mreža EU-a za provedbu i izvršenje prava u području okoliša (IMPEL), Europska mreža državnih odvjetnika u području okoliša (ENPE), EnviCrimeNet i Forum sudaca EU-a u području okoliša (EUFJE).
[78] Odbor stručnjaka za zaštitu okoliša putem kaznenog prava (PC-ENV) – Europski odbor za probleme povezane s kriminalom.

istovremeno ojačaju pravosudna suradnja i uzajamno povjerenje, među ostalim digitalizacijom[79].

Ključne mjere

Komisija će:

- **u 2026. iznijeti zakonodavni prijedlog za modernizirana pravila o organiziranom kriminalu,**
- **u 2025. predstaviti zakonodavni prijedlog za reviziju pravnog okvira o prekursorima za droge,**
- **u 2025. iznijeti zakonodavni prijedlog za zajedničke kaznenopravne standarde o nezakonitoj trgovini vatrenim oružjem,**
- **procijeniti potrebu za revizijom Direktive o pirotehničkim sredstvima i Direktive o eksplozivima za civilnu upotrebu,**
- **procijeniti potrebu za daljnjim jačanjem Europskog istražnog naloga i europskog uhidbenog naloga,**
- **u 2026.predstaviti novu strategiju EU-a za borbu protiv trgovine ljudima,**
- **u 2026. predstaviti novu strategiju EU-a za prava žrtava,**
- **do 2027.iznijeti akcijski plan EU-a za zaštitu djece od kriminala,**
- **u 2025. iznijeti akcijski plan EU-a za borbu protiv trgovine drogom,**
- **u 2026. predstaviti akcijski plan EU-a za kontrolu trgovine oružjem,**
- **od 2025. širiti Europski savez luka,**
- **u 2026. donijeti smjernice za zaštitu maloljetnika na temelju Akta o digitalnim uslugama,**
- **u 2026. predstaviti akcijski plan EU-a za borbu protiv zlostavljanja na internetu.**

Države članice pozivaju se da:

- **do kraja 2026. u potpunosti prenesu nova pravila o povratu i oduzimanju imovine i u potpunosti ih provode,**
- **primjenjuju administrativni pristup u borbi protiv infiltracije kriminala,**
- **uspostave javno-privatna partnerstva za borbu protiv pranja novca,**
- **prenesu i u potpunosti provode Direktivu o sprečavanju i borbi protiv nasilja nad ženama i nasilja u obitelji.**

Europski parlament i Vijeće pozivaju se da:

- **nastave rad na pregovorima o Uredbi o utvrđivanju pravila za sprečavanje i suzbijanje seksualnog zlostavljanja djece i Direktivi o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i materijala koji sadržava seksualno zlostavljanje djece,**
- **zaključe pregovore o Direktivi o borbi protiv korupcije.**

6. Borba protiv terorizma i nasilnog ekstremizma

Uvest ćemo sveobuhvatni program borbe protiv terorizma kako bismo spriječili radikalizaciju, osigurali internetske i javne prostore, ograničili pristup izvorima financiranja i odgovorili na moguće napade.

[79] Posebice uspostavom Sustava za komunikaciju u okviru e-pravosuđa s pomoću internetske razmjene podataka (eCODEX) i Europskog informacijskog sustava kaznene evidencije za državljane trećih zemalja (ECRIS-TCN).

Rizik od terorizma u EU-u i dalje je visok. Usko je povezan s posljedicama geopolitičkih događaja, novih tehnologija i novih načina financiranja terorizma. Moramo se pobrinuti da EU bude dobro opremljen za predviđanje prijetnji, sprečavanje radikalizacije (na internetu i izvan njega), zaštitu građana i javnih prostora od napada i djelotvoran odgovor na moguće napade. **Novi program EU-a za sprečavanje i suzbijanje terorizma i nasilnog ekstremizma**, u kojem će se utvrditi buduće mjere EU-a, iznijet će se 2025. EU će prema novom programu 2025. sa zapadnim Balkanom potpisati novi **zajednički akcijski plan** za sprečavanje i suzbijanje terorizma i nasilnog ekstremizma.

Sprečavanje radikalizacije i zaštita ljudi na internetu

Kao i borba protiv organiziranog kriminala, borba protiv terorizma i nasilnog ekstremizma počinje **uklanjanjem njegovih temeljnih uzroka**. **Centar znanja EU-a za sprečavanje radikalizacije** pojačat će potporu stručnjacima i oblikovateljima politika novim **sveobuhvatnim paketom instrumenata za prevenciju**. Taj će paket omogućiti ranu identifikaciju i intervencije usmjerene na ranjive pojedince, posebice maloljetnike. Radikalizacija se često događa u zatvorima pa će Komisija izdati nove preporuke kako bi pomogla državama članicama u rješavanju tog problema.

Teroristi i nasilni ekstremisti koriste internetske platforme za širenje terorističkih i štetnih sadržaja, prikupljanje sredstava i vrbovanje. Ranjivi korisnici, a posebno maloljetnici, na internetu se radikaliziraju zabrinjavajućom brzinom. **Uredba o terorističkom sadržaju na internetu** bila je ključna u borbi protiv širenja terorističkih sadržaja na internetu jer je omogućila brzo uklanjanje najokrutnijih i najopasnijih materijala[80]. Komisija trenutačno ocjenjuje njezino funkcioniranje i analizira kako najbolje ojačati taj okvir.

Protokol EU-a za krizne situacije za zajednički i brz odgovor tijela za izvršavanje zakonodavstva i tehnološke industrije na teroristički napad izmijenit će se kako bi se omogućila prilagodljivost i fleksibilnost u odgovoru na sve raširenije terorističke napade na internetu. Internetski forum EU-a i dalje će biti glavni kanal za dobrovoljnu suradnju s tehnološkom industrijom u borbi protiv terorističkih i štetnih sadržaja na internetu. Usto, Komisija sudjeluje u međunarodnim inicijativama kao što su zaklada Christchurch Call i globalni internetski forum za borbu protiv terorizma (GIFCT).

Borba protiv financiranja terorizma

Teroristi svoje aktivnosti financiraju kampanjama skupnog financiranja, kriptoimovinom, neobankama ili internetskim platformama za plaćanje. Tijela kaznenog progona moraju te financijske tokove otkriti i istražiti, a za to su potrebna sredstva, alati i stručno znanje. Ključnu ulogu u tome ima **mreža financijskih istražitelja za borbu protiv terorizma**. Komisija će razmotriti uspostavu **novog sustava na razini EU-a za praćenje financiranja terorizma**, koji će obuhvaćati transakcije unutar EU-a i SEPA-e, prijenose kriptoimovine i internetska i elektronička plaćanja. Time će se dopuniti Sporazum o programu za praćenje financiranja terorizma (TFTP) između EU-a i SAD-a.

Proračun EU-a mora se **zaštititi od zlouporabe za poticanje radikalnih/ekstremističkih stajališta** u državama članicama. Revidirana **Financijska uredba** sad uključuje osudu za „poticanje na diskriminaciju, mržnju ili nasilje” kao osnovu za isključenje iz financiranja sredstvima EU-a. Komisija će nastaviti istraživati najbolji način za potpuno iskorištavanje paketa instrumenata, među ostalim za odabir potencijalnih korisnika. Zaštita proračuna EU-a

[80] Do 31. prosinca 2024. izdano je 1426 naloga za uklanjanje terorističkog sadržaja ili blokiranje pristupa tom sadržaju. Velika većina tih naloga bila je usmjerena na džihadistički teroristički sadržaj, ali i na desničarski teroristički sadržaj.

temelji se i na bliskoj suradnji i razmjeni informacija s nacionalnim tijelima te agencijama i tijelima EU-a.

Zaštita od napada

Osim ulaganja u sprečavanje radikalizacije, važna komponenta zaštite građana ograničavanje je načina na koji teroristi i kriminalci mogu izvršiti napade. Potrebno je djelovati i u odnosu na alate koje teroristi upotrebljavaju i poduzimati mjere za zaštitu meta kojima prijeti napad.

Osim mjera koje se odnose na vatreno oružje, Komisija će **preispitati i pravila** o **prekursorima eksploziva** kako bi se obuhvatile visokorizične kemikalije. **Javni prostori** i dalje su najčešće mete terorističkih napada, posebice za individualne napade. U cilju zaštite građana od ozljeda ojačat će se **EU-ov savjetodavni program sigurnosne zaštite** i na zahtjev država članica provodit će se procjene ranjivosti javnih prostora, kritične infrastrukture i visokorizičnih događaja, uz financiranje iz proračuna EU-a u okviru Fonda za unutarnju sigurnost. EU će nastojati povećati dostupna sredstva za zaštitu javnog prostora. Komisija za pomoć tijelima država članica i privatnim subjektima pruža posebne smjernice i alate, kao što je centar znanja o zaštiti javnih prostora[81], a za zaštitu javnih prostora od 2020. je na raspolaganje stavljeno već 70 milijuna EUR.

Komisija će razmotriti i uvođenje zahtjeva za organizacije da uzmu u obzir ili primjenjuju sigurnosne mjere na javno dostupnim mjestima u suradnji s lokalnim tijelima i privatnim partnerima.

S obzirom na očite ranjivosti, nastavit će provoditi mjere za zaštitu židovske zajednice vodeći se **Strategijom EU-a za suzbijanje antisemitizma i njegovanje židovskog načina života (2021. – 2030.)**. Komisija će se isto tako pobrinuti da se uvedu odgovarajući alati za potporu državama članicama u borbi protiv **mržnje prema muslimanima**.

Upotreba **bespilotnih zrakoplova** za špijunažu i napade sve je veći sigurnosni problem. Komisija će izraditi **usklađenu metodologiju ispitivanja sustava za obranu od bespilotnih zrakoplova**, uspostaviti **centar izvrsnosti za obranu od bespilotnih zrakoplova** i procijeniti potrebu za usklađivanjem propisa i postupaka država članica[82].

Strani teroristički borci

Za identifikaciju stranih terorističkih boraca koji se vraćaju ili ulaze na vanjskim granicama EU-a potrebni su podaci o pojedincima koji predstavljaju terorističku prijetnju. U tu će svrhu Komisija zajedno s Europolom intenzivnije **surađivati s ključnim trećim zemljama kako bi se prikupili biografski i biometrijski podaci o pojedincima koji bi mogli predstavljati terorističku prijetnju**, uključujući strane terorističke borce, koji se zatim mogu unijeti u Šengenski informacijski sustav (SIS) u skladu s primjenjivim pravnim okvirima EU-a i nacionalnim pravnim okvirima. Stoga je ključno da države članice iskoriste sve postojeće alate. To uključuje unošenje svih relevantnih informacija u **SIS**, poboljšanje biometrijskih provjera i provođenje obveznih sustavnih provjera svih osoba na vanjskim granicama EU-a[83]. Osim toga, **zajednički pokazatelji rizika** koje je izradio Frontex i dalje će tijelima država članica nadležnima za nadzor državne granice pomagati u prepoznavanju i procjeni rizika od sumnjivih kretanja potencijalnih stranih terorističkih boraca.

Kako bi države članice mogle zadržati pristup **dokazima s bojišta** koje je prikupio istražni tim UN-a za promicanje odgovornosti za kaznena djela koja je počinio Daiš/ISIL (UNITAD) radi kaznenog progona stranih terorističkih boraca, Komisija će zajedno s Eurojustom procijeniti

[81] Centar znanja o zaštiti javnih prostora.
[82] Na temelju skupa ključnih mjera iz Komunikacije o obrani od dronova iz 2023., COM(2023) 659 final.
[83] U potpunosti u skladu sa Zakonikom o šengenskim granicama i Uredbom o dubinskim provjerama.

mogućnost pohrane tih dokaza u Eurojustovoj središnjoj bazi podataka s dokazima o najtežim međunarodnim zločinima. Uz to, novi **europski pravosudni registar za borbu protiv terorizma** pravosudnim će tijelima država članica i dalje pomagati u brzom prepoznavanju prekograničnih veza u predmetima povezanima s terorizmom.

Ključne mjere

Komisija će:

- **u 2025. donijeti novi program EU-a za sprečavanje i suzbijanje terorizma i nasilnog ekstremizma,**
- **u 2025. sa zapadnim Balkanom potpisati novi zajednički akcijski plan za sprečavanje i suzbijanje terorizma i nasilnog ekstremizma,**
- **pripremiti novi sveobuhvatni paket instrumenata za prevenciju u suradnji s Centrom znanja EU-a,**
- **u 2026. ocijeniti primjenu Uredbe o terorističkom sadržaju na internetu,**
- **u 2025. izmijeniti Protokol EU-a za krizne situacije,**
- **u 2026. iznijeti zakonodavni prijedlog za reviziju Uredbe o stavljanju na tržište i uporabi prekursora eksploziva,**
- **istražiti izvedivost novog sustava na razini EU-a za praćenje financiranja terorizma.**

Države članice pozivaju se da:

- **unaprijede biometrijske provjere i provode obvezne sustavne provjere na vanjskim granicama EU-a,**
- **potpuno iskoriste Europski pravosudni registar za borbu protiv terorizma.**

7. EU kao snažan globalni akter u području sigurnosti

U cilju jačanja sigurnosti EU-a intenzivirat ćemo operativnu suradnju kroz partnerstva s ključnim regijama kao što su naši partneri u procesu proširenja i partneri iz susjedstva, Latinska Amerika i mediteranska regija. Sigurnosni interesi EU-a uzet će se u obzir u međunarodnoj suradnji, među ostalim iskorištavanjem EU-ovih alata i instrumenata.

Posljednjih su godina postale evidentne neraskidive veze između EU-ove vanjske i unutarnje sigurnosti. Ruski agresivni rat protiv Ukrajine, sukob u Gazi, stanje u Siriji i novi sukobi drugdje u svijetu ozbiljno utječu na EU-ovu unutarnju sigurnost. U cilju suzbijanja utjecaja globalne nestabilnosti na unutarnju sigurnost **EU treba aktivno braniti svoje sigurnosne interese** uklanjanjem vanjskih prijetnji, prekidanjem krijumčarskih ruta i zaštitom koridora od strateškog interesa kao što su trgovinske rute. S druge strane nastavit će biti snažan saveznik partnerskim zemljama i surađivat će s njima na jačanju globalne sigurnosti i uzajamne otpornosti na prijetnje.

Posljednjih je godina poduzeo važne korake kako bi poboljšao suradnju u području sigurnosti. Sklopio je sporazume o operativnoj suradnji tijela za izvršavanje zakonodavstva i pravosudnoj suradnji, kao i druge vrste dogovora s partnerskim zemljama. Aktivno radi na dodatnim međunarodnim sporazumima u skladu s pregovaračkim smjernicama Vijeća i inicijativama za izgradnju kapaciteta, uz potporu agencija i tijela EU-a. Globalna Europa – NDICI također je važna za jačanje sigurnosti u suradnji s partnerskim zemljama.

Međunarodni poredak utemeljen na pravilima preduvjet je za unapređenje globalne sigurnosti. Dijalozi o sigurnosti, pa i tematski, presudni su u tim nastojanjima. Provedba

Strateškog kompasa za sigurnost i obranu, kao i bilateralni i multilateralni okviri suradnje kao što su sporazumi o stabilizaciji i pridruživanju i sporazumi o pridruživanju te suradnja s organizacijama kao što su UN i NATO, omogućuju razvoj učinkovitih sigurnosnih rješenja. EU će nastaviti djelovati u multilateralnim forumima[84] i poboljšat će suradnju s relevantnim međunarodnim i regionalnim organizacijama i okvirima, uključujući NATO, Ujedinjene narode, Vijeće Europe, Interpol, skupinu G-7, OESS i civilno društvo.

Regionalna suradnja

Nastavak EU-ove nepokolebljive potpore **Ukrajini** i jačanje sigurnosti i otpornosti **zemalja proširenja EU-a** politički su i geostrateški imperativi. Potpora sigurnosti EU-a trebala bi ići ruku pod ruku s **ubrzanom integracijom zemalja kandidatkinja u sigurnosnu strukturu EU-a**, paralelno s konsolidacijom njihove regionalne suradnje. Komisija će zahvaljujući EU-ovoj politici proširenja podržati kapacitete zemalja kandidatkinja i potencijalnih kandidata za odgovor na prijetnje, povećati operativnu suradnju i razmjenu informacija te osigurati usklađenost s EU-ovim načelima, zakonodavstvom i instrumentima. Instrument pretpristupne pomoći (IPA III) te instrumenti za Ukrajinu, Moldovu i zapadni Balkan neophodni su za jačanje sigurnosti i u zemljama kandidatkinjama i potencijalnim kandidatima.

EU će također dodatno integrirati **partnere iz susjedstva** u sigurnosnu strukturu EU-a. Na temelju **novog pakta za Sredozemlje** i predstojećeg **strateškog pristupa Crnome moru** Unija će nastojati dalje graditi regionalnu suradnju i bilateralna sveobuhvatna strateška partnerstva sa sigurnosnom dimenzijom, prema potrebi u okviru redovitih dijaloga o sigurnosti na visokoj razini. Ojačat će se operativna suradnja sa Sjevernom Afrikom, **Bliskim istokom i Zaljevom**, posebice u područjuborbe protiv terorizma, sprečavanja pranja novca, trgovine vatrenim oružjem i proizvodnje i trgovine drogom, osobito kaptagonom**.**

Kako bi se riješio problem porasta terorističkih i kriminalnih aktivnosti i njihovih posljedica u **supsaharskoj Africi**, **posebice u Sahelu, na Rogu Afrike i u zapadnoj Africi**, EU će pojačati potporu Afričkoj uniji, regionalnim gospodarskim zajednicama i zemljama u regiji. U skladu sa Strategijom pomorske sigurnosti[85] EU će unaprijediti suradnju u **Gvinejskom zaljevu, na Crvenom moru i na Indijskom oceanu** u borbi protiv trgovine ljudima i piratstva, i to poticanjem suradnje unutar Afrike i regionalne suradnje i uz potporu EU-ove koordinirane mornaričke prisutnosti i Centra za pomorske analize i operacije (narkotici) (MAOC-N).

EU će intenzivirati operativnu suradnju s **Latinskom Amerikom i Karibima** radi razbijanja i kaznenog progona kriminalnih mreža visokog rizika te prekidanja nezakonitih aktivnosti i krijumčarskih ruta, uz jačanje okvira suradnje, kao što su EU-CLASI (Latinskoamerički odbor za unutarnju sigurnost) i Mehanizam koordinacije i suradnje EU-a i CELAC-a u vezi s drogama. Među prioritetima su otpornost i partnerstva logističkih čvorišta te pristupi praćenja novca. EU će podupirati razvoj Policijske zajednice Sjeverne i Južne Amerike (AMERIPOL), koja će postati regionalni ekvivalent Europola i ojačati pravosudnu suradnju između država članica i te regije. Surađivat će i s **južnom i središnjom Azijom** na zajedničkim sigurnosnim problemima povezanima s terorizmom, trgovinom nezakonitom robom, uključujući droge, trgovinom ljudima i krijumčarenjem migranata.

Osim toga, EU će podupirati okvire regionalne suradnje u trećim zemljama kako bi im dodatno pomogao u zaustavljanju nezakonite trgovine na izvoru, u skladu s načelom zajedničke odgovornosti za cijeli kriminalni lanac opskrbe. Nadalje, EU će doprinijeti jačanju sigurnosti

[84] Globalni forum za borbu protiv terorizma, globalna koalicija za borbu protiv Daiša, globalni internetski forum za borbu protiv terorizma (GIFCT), zaklada Christchurch Call, globalna koalicija za suzbijanje prijetnji povezanih sa sintetičkim drogama.
[85] JOIN(2023) 8 final.

logističkih čvorišta u inozemstvu tako što će koordinirati **zajedničke inspekcije u lukama trećih zemalja**.

Operativna suradnja

Global Gateway poduprijet će održive i visokokvalitetne infrastrukturne projekte u digitalnom, klimatskom, energetskom, prometnom, zdravstvenom, obrazovnom i istraživačkom sektoru. Komisija će, prema potrebi, u buduća ulaganja u okviru strategije Global Gateway uključivati sigurnosna pitanja. To će obuhvaćati inicijative ključne za stratešku autonomiju EU-a i njegovih partnerskih zemalja, kao što su infrastrukturni projekti sa sigurnosnim procjenama i mjerama za ublažavanje rizika.

Komisija će nastaviti raditi na daljnjim **sporazumima između EU-a i trećih zemalja o suradnji s Europolom i Eurojustom**, posebice sa zemljama Latinske Amerike.

Osim toga, proaktivno sudjelovanje trećih zemalja u **EMPACT-u** jedno je od najdjelotvornijih načina za jačanje operativne suradnje. EU će dodatno poticati uključivanje trećih zemalja, osobito zapadnog Balkana, istočnog susjedstva, supsaharske Afrike, sjeverne Afrike, Bliskog istoka, Latinske Amerike i Kariba, u taj okvir. Još jedan način da se intenzivira suradnja s trećim zemljama u borbi protiv kriminala jesu operativne radne skupine država članica koje koordinira Europol i u kojima mogu sudjelovati treće zemlje. Komisija namjerava dovršiti pregovore o međunarodnom sporazumu između **EU-a i Interpola**[86] kako bi se osigurao ujednačeniji pristup globalnim sigurnosnim prijetnjama i suzbijanje transnacionalnih kaznenih djela.

Unija mora biti prisutna na terenu u skladu s pristupom Tima Europa. Specijalizirano osoblje Unije i država članica znatno doprinosi tome da vanjsko djelovanje Unije bude dobro informirano, usklađeno i prilagodljivo okolnostima. Kako bi se taj pristup dodatno unaprijedio, Komisija će, uz potporu Visokog predstavnika za vanjske poslove i sigurnosnu politiku, ojačati **mreže za vezu** i olakšati raspoređivanje regionalnih **časnika za vezu Europola i Eurojusta** u skladu s operativnim potrebama država članica.

EU će nastojati ostvariti bližu operativnu suradnju tijela za izvršavanje zakonodavstva i pravosudnu suradnju i poticati razmjenu informacija u stvarnom vremenu i zajedničke operacije **zajedničkih istražnih timova** u trećim zemljama uz potporu Europola i Eurojusta. Komisija će podupirati države članice u uspostavi **zajedničkih centara za povezivanje**, u kojima će se okupljati stručnjaci i lokalna tijela za izvršavanje zakonodavstva u strateškim trećim zemljama.

Alati zajedničke vanjske i sigurnosne politike (ZVSP)

Misije zajedničke sigurnosne i obrambene politike (ZSOP) u potpunosti će se iskoristiti za bolje prepoznavanje i suzbijanje vanjskih prijetnji unutarnjoj sigurnosti EU-a, u skladu s njihovim mandatima, koje je utvrdilo Vijeće. U cilju izgradnje kapaciteta trećih zemalja, Visoki predstavnik za vanjske poslove i sigurnosnu politiku podupirat će, zajedno s Komisijom, aktivnosti ZSOP-a posebnim instrumentima financiranja i istražiti sve primjerene načine financiranja.

EU-ove mjere ograničavanja uhodan su alat ZVSP-a koji se upotrebljava i za borbu protiv terorizma. Vijeće može na temelju prijedloga Visokog predstavnika za vanjske poslove i sigurnosnu politiku, država članica ili Komisije procijeniti kako EU-ove postojeće samostalne mjere ograničavanja (EU-ov popis terorista) učiniti učinkovitijima, operativnijima i fleksibilnijima. Nadalje, mogu se, u skladu s ciljevima ZVSP-a, razmotriti dodatne mjere ograničavanja usmjerene na kriminalne mreže.

[86] Odluka Vijeća (EU) 2021/1312 od 19. srpnja 2021. i Odluka Vijeća (EU) 2021/1313 od 19. srpnja 2021.

Vizna politika i razmjena informacija

Vizna politika EU-a važan je alat za suradnju s trećim zemljama i zaštitu naših granica kontroliranjem i definiranjem uvjeta za ulazak u EU. Komisija će u novom strategijom za viznu politiku EU-a u potpunosti integrirati **sigurnosna pitanja u viznu politiku EU-a**. Surađivat će sa suzakonodavcima na donošenju prijedloga za reviziju i pojednostavnjenje mehanizma suspenzije viza, posebice u posebnim slučajevima zlouporabe bezviznog režima[87]. Treće zemlje poticat će se na razmjenu informacija o pojedincima koji mogu predstavljati sigurnosnu prijetnju i te će se informacije unositi u informacijske sustave i baze podataka EU-a.

Kako bi se ostvarila koordinacija politika i poduzelo mjere za učinkovitiju, bržu i neometanu suradnju, Komisija će nastojati postići **dogovore o protoku podataka** i istražiti načine da se **poboljša razmjena informacija** za potrebe izvršavanja zakonodavstva i upravljanja granicama s pouzdanim trećim zemljama, poštujući pritom temeljna prava i pravila o zaštiti podataka.

Ključne mjere

Komisija će:

- **sklopiti međunarodne sporazume između EU-a i prioritetnih trećih zemalja o suradnji s Europolom i Eurojustom,**
- **poticati sudjelovanje partnerskih zemalja u EMPACT-u radi suzbijanja organiziranog kriminala i terorizma,**
- **podupirati agencije i tijela EU-a u postizanju i intenziviranju radnih dogovora s partnerskim zemljama,**
- **uključiti sigurnosna pitanja u viznu politiku EU-a u okviru nove vizne strategije,**
- **poboljšati razmjenu informacija s pouzdanim trećim zemljama za potrebe izvršavanja zakonodavstva i upravljanja granicama.**

Komisija će u suradnji s Visokim predstavnikom za vanjske poslove:

- **potpuno iskoristiti civilne misije zajedničke sigurnosne i obrambene politike (ZSOP),**
- **koordinirati zajedničke inspekcije u lukama trećih zemalja do 2027.**

Komisija će u suradnji s Visokim predstavnikom za vanjske poslove i državama članicama:

- **jačati mreže za vezu i suradnju u skladu s pristupom Tima Europa,**
- **od 2025. uspostavljati zajedničke operativne timove i centre za povezivanje u trećim zemljama.**

Europski parlament i Vijeće pozivaju se da:

- **zaključe pregovore o reviziji mehanizma suspenzije viza.**

8. Zaključak

Budući da u svijetu vlada nesigurnost, potrebno je povećati sposobnost Unije za predviđanje, sprečavanje i reagiranje na sigurnosne prijetnje.

Nije dovoljno samo odgovarati na krize nakon što se dogode. Moramo imati cjelovit pregled prijetnji i njihova razvoja i pobrinuti se da naši alati i kapaciteti budu na visini zadatka.

[87] COM(2023) 642.

Sveobuhvatan skup mjera opisanih u ovoj strategiji pridonijet će povećanju autonomije Unije u svijetu: da može predviđati, planirati i zadovoljavati vlastite sigurnosne potrebe, djelotvorno reagirati na prijetnje unutarnjoj sigurnosti, privoditi počinitelje pravdi i štititi svoja otvorena, slobodna i prosperitetna društva i demokracije.

Zato moramo promijeniti svoju percepciju o unutarnjoj sigurnosti. Promicat ćemo novu kulturu sigurnosti EU-a, tako da se pitanja sigurnosti uključuju u sve naše propise, politike i programe, od njihova predlaganja do provedbe, a suradnja raznih područja politike omogućava da postavimo nove temelje.

To nije zadatak samo jedne institucije, vlade ili aktera, nego cijele Europe.