EVROPSKA
KOMISIJA

Strasbourg, 1.4.2025
COM(2025) 148 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

ProtectEU: evropska strategija notranje varnosti

1. ProtectEU: evropska strategija notranje varnosti

Varnost je temelj, na katerem gradijo vse naše svoboščine. Demokracija, pravna država, temeljne pravice, blaginja Evropejcev, konkurenčnost in blaginja – vse to je odvisno od naše sposobnosti, da zagotovimo osnovno varnostno jamstvo. V novem obdobju varnostnih groženj, v katerem živimo zdaj, je zmožnost držav članic EU, da svojim državljanom in državljankam zagotovijo varnost, bolj kot kdaj koli prej odvisna od **enotnega evropskega pristopa k zaščiti naše notranje varnosti**. V razvijajočem se geopolitičnem okolju mora Evropa še naprej izpolnjevati svojo trajno obljubo miru.

Prvi koraki k oblikovanju evropskega varnostnega aparata so že bili narejeni. V zadnjem desetletju smo poskrbeli, da ima Unija izboljšane skupne mehanizme za ukrepanje na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodnega sodelovanja, varnosti meja, boja proti hudim kaznivim dejanjem in organiziranemu kriminalu, boja proti terorizmu in nasilnemu ekstremizmu ter zaščite svoje fizične in digitalne kritične infrastrukture. Ustrezno izvajanje predhodno sprejete zakonodaje in predhodno razvitih politik ostaja ključnega pomena.

Zaradi narave današnjih groženj in neločljive povezanosti notranje in zunanje varnosti EU moramo iti še korak dlje.

Obzorje krajine groženj je temno. Meje med **hibridnimi grožnjami** in odprto vojno so zabrisane. Rusija vodi spletno in nespletno hibridno kampanjo proti EU in njenim partnerjem, da bi pretresla in spodkopala družbeno kohezijo in demokratične procese ter preizkušala solidarnost EU z Ukrajino. Sovražne tuje države in akterji, ki jih podpirajo države, si prizadevajo, da bi se infiltrirali v naše kritične infrastrukture in dobavne verige ter povzročili motnje v njih, kradli občutljive podatke in se postavili v položaj, ki bi jim omogočal povzročanje čim več motenj v prihodnosti. Kriminal izkoriščajo kot storitev, storilce kaznivih dejanj pa kot posrednike. Poleg tega smo zaradi naše odvisnosti od tretjih držav, na katere se zanašajo dobavne verige, bolj ranljivi za hibridne kampanje sovražnih držav.

Kot je poudarjeno v oceni ogroženosti zaradi hudih kaznivih dejanj in organiziranega kriminala (SOCTA)[1], ki jo je nedavno predstavil Europol, se v Evropi širijo močne **organizirane kriminalne združbe**, ki se razvijajo na spletu in se širijo v naše gospodarstvo ter vplivajo na našo družbo. Ko se organizirani kriminal zasidra v skupnosti ali gospodarskem sektorju, postane boj proti njemu težka bitka: tretjina najnevarnejših kriminalnih mrež deluje že več kot deset let. Kriptovalute in vzporedni finančni sistemi jim pomagajo pri pranju in prikrivanju premoženjskih koristi, pridobljenih s kaznivimi dejanji.

Stopnja ogroženosti zaradi terorizma v Evropi ostaja visoka. Regionalne krize zunaj EU ustvarjajo verižni učinek, saj terorističnim akterjem na celotnem ideološkem spektru dajejo novo motivacijo za novačenje, mobilizacijo ali krepitev njihovih zmogljivosti. Svoja prizadevanja v zvezi z radikalizacijo in novačenjem usmerjajo predvsem v najranljivejše dele naših družb, zlasti nekatere mlade. Navdihujejo napade storilcev, ki delujejo sami, in porast protisistemskega ekstremizma, katerega cilj je razbiti demokratični pravni red.

Skokovit **tehnološki napredek** ponuja ključna orodja za izboljšanje našega varnostnega aparata. Vendar so kibernetski napadi in tuje manipuliranje z informacijami vse pogostejši, saj izkoriščajo nove tehnologije, kot je umetna inteligenca. Otroci, mladi in starejši so še posebej izpostavljeni tveganjem na spletu, širjenje sovraštva na spletu pa ogroža svobodo izražanja in socialno kohezijo.

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

Naša življenja so postala manj varna, kar Evropejci vse bolj občutijo, saj je njihovo **dojemanje varnosti in zaščite v EU** načeto do te mere, da je 64 % anketiranih na vprašanje o prihodnosti odgovorilo, da so zaskrbljeni zaradi varnosti EU[2]. Vse bolj zaskrbljena so tudi podjetja; napačne informacije in dezinformacije, kriminal in nezakonite dejavnosti ter kibernetsko vohunjenje so med desetimi največjimi tveganji, opredeljenimi v poročilu Svetovnega gospodarskega foruma o svetovnih tveganjih za leto 2025[3].

Evropejci bi **morali imeti možnost, da živijo brez strahu**, pa naj je to na ulicah, doma, na javnih mestih, na podzemni železnici ali na internetu. Zaščita ljudi, zlasti tistih, ki so najbolj izpostavljeni napadom, ki običajno nesorazmerno prizadenejo otroke, ženske in manjšine, vključno z judovskimi in muslimanskimi skupnostmi, je v središču prizadevanj EU na področju varnosti. To je bistveno za izgradnjo odpornih in kohezivnih družb.

Komisija pripravlja **evropsko strategijo notranje varnosti** za boljše preprečevanje groženj v prihodnosti. Z bolje izdelanim naborom pravnih orodij, tesnejšim sodelovanjem in obsežnejšo izmenjavo informacij bomo okrepili našo odpornost in kolektivno sposobnost napovedovanja, preprečevanja in odkrivanja varnostnih groženj ter učinkovitega odzivanja nanje. Enoten pristop k notranji varnosti lahko države članice podpre, da izkoristijo moč tehnologije za krepitev varnosti, ne njeno oslabitev, hkrati pa spodbujajo varen digitalni prostor za vse. Poleg tega podpira skupni odziv držav članic na svetovne politične in gospodarske spremembe, ki vplivajo na notranjo varnost Unije.

Ta strategija temelji na **treh načelih** in v svojem jedru nosi spoštovanje pravne države in temeljnih pravic.

Prvič, določa ambicije za spremembo kulture na področju varnosti. Potrebujemo **vsedružbeni pristop**, ki bo vključeval vse državljanke in državljane ter deležnike, vključno s civilno družbo, raziskovalci, akademskimi krogi in zasebnimi subjekti. Ukrepi v okviru strategije zato temeljijo na celostnem, večdeležniškem pristopu, kadar je to mogoče.

Drugič, **varnostne vidike je treba vključiti v vso zakonodajo, politike in programe EU**, vključno z zunanjimi ukrepi EU. Zakonodajo, politike in programe bo treba pripraviti, pregledati in izvajati z varnostnim vidikom v mislih, pri čemer je treba zagotoviti, da se upoštevajo potrebna varnostna vprašanja, da se spodbudi skladen in celovit pristop k varnosti.

Na koncu so za varno, zaščiteno in odporno Evropo potrebne **resne naložbe EU, njenih držav članic in zasebnega sektorja**. Prednostne naloge in ukrepi iz te strategije zahtevajo zadostne človeške in finančne vire, da se zagotovi njihovo izvajanje. Kot je določeno v sporočilu o poti do naslednjega večletnega finančnega okvira[4], bo morala Evropa povečati javno porabo za varnost ter spodbujati raziskave in naložbe na področju varnosti, s čimer bo okrepila svojo strateško avtonomijo.

Ta strategija dopolnjuje **strategijo za unijo pripravljenosti**[5], ki določa celovit pristop, ki zajema vse nevarnosti, za pripravljenost na konflikte, nesreče, ki jih povzroči človek, naravne nesreče in krize, ter **belo knjigo o prihodnosti evropske obrambe – Pripravljenost 2030**[6], ki podpira razvoj in pridobivanje obrambnih zmogljivosti po vsej EU za odvračanje tujih nasprotnikov. Komisija bo predlagala tudi **evropski ščit za demokracijo**, da bi okrepila

[2] Raziskava Flash Eurobarometer FL550: Izzivi in prednostne naloge 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.

demokratično odpornost v EU. Te pobude skupaj določajo vizijo za varno, zaščiteno in odporno EU.

Novo upravljanje evropske notranje varnosti

Komisija bo tesno sodelovala z državami članicami in agencijami EU, da bi nadgradila pristop EU k notranji varnosti na strateški in operativni ravni.

To bomo dosegli z:

- **dosledno opredelitvijo potencialnih posledic novih in revidiranih pobud Komisije za varnost in pripravljenost že na začetku pogajalskega procesa in med njim;**
- **rednimi srečanji projektne skupine Komisije za evropsko notranjo varnost, podprtimi s strateškim medsektorskim sodelovanjem znotraj Komisije;**
- **predstavitvami analiz groženj, povezanih z notranjo varnostjo, v podporo delu kolegija za varnost;**
- **razpravami z državami članicami v Svetu o spreminjajočih se izzivih na področju notranje varnosti na podlagi analize groženj in izmenjav o ključnih prednostnih nalogah politike;**
- **rednim poročanjem Evropskemu parlamentu in Svetu za spremljanje in podporo izvajanju ključnih pobud na področju varnosti.**

2. Celostno situacijsko zavedanje in analiza ogroženosti

EU bomo opremili z novimi načini izmenjave in združevanja informacij ter zagotavljali redne analize groženj za notranjo varnost EU, kar bo prispevalo k celoviti oceni tveganj in ogroženosti.

Varnost se začne z **učinkovitim napovedovanjem**. EU se mora zanašati na celovito, dovolj avtonomno in posodobljeno situacijsko zavedanje in analizo ogroženosti. Obveščevalni podatki, na podlagi katerih je mogoče ukrepati in za katere se države članice spodbuja, naj jih dodatno okrepijo z enotno zmogljivostjo za analizo obveščevalnih podatkov (SIAC) kot enotno vstopno točko za obveščevalne podatke držav članic, so ključnega pomena za ocenjevanje groženj in boj proti njim, kar je navsezadnje podlaga za politične in zakonodajne ukrepe[7]. Na ravni EU moramo učinkoviteje in sodelovalno uporabljati **analize na podlagi obveščevalnih podatkov** in **ocene ogroženosti**.

Komisija bo na podlagi različnih ocen tveganj in ogroženosti, pripravljenih na ravni EU in za posamezne sektorje[8], pripravljala **redne analize groženj za notranjo varnost EU**, da bi opredelila glavne varnostne izzive, z namenom prispevati k prednostnim nalogam politike. To bo pripomoglo k razvoju prožne in odzivne notranje varnostne politike, ki učinkovito obravnava spreminjajoče se grožnje, bolje ščiti ljudi in podjetja pred napadi ter omogoča pravočasne ciljno usmerjene intervencije politike. Te analize groženj za notranjo varnost EU bodo prispevale tudi k **celoviti (medsektorski) oceni tveganj in ogroženosti za EU (ki zajema vse nevarnosti)**, ki jo pripravita Komisija in visoki predstavnik, kot je določeno v strategiji za unijo pripravljenosti.

[7] Varnejši skupaj – Krepitev civilne in vojaške pripravljenosti Evrope, str. 23.

[8] Sektorske ocene ogroženosti, ki bodo prispevale k tej analizi groženj, vključujejo oceno ogroženosti zaradi hudih kaznivih dejanj in organiziranega kriminala v EU (SOCTA), poročilo o stanju in trendih na področju terorizma v EU (TE-SAT), skupno poročilo o oceni kibernetske varnosti (JCAR) ter prihodnje ocene groženj, tveganj in metod pranja denarja in financiranja terorizma, ki jih bosta izvedla Komisija in organ za preprečevanje pranja denarja.

Zaupanje in varna obdelava sta bistvena za deljenje informacij, za kar je potrebna zanesljiva in varna infrastruktura. Institucije, organi, in agencije EU morajo zagotoviti, da lahko uporabljajo **varne komunikacijske kanale** za izmenjavo občutljivih in tajnih podatkov med seboj in z državami članicami. Naložbe v **interoperabilne varne sisteme** in zanesljivo tehnologijo bodo okrepile avtonomijo EU ter sposobnost EU za obvladovanje kriz in zagotavljanje operativne odpornosti. V zvezi s tem Komisija poziva sozakonodajalca, naj zaključita pogajanja o **predlagani uredbi o informacijski varnosti v institucijah, organih, uradih in agencijah Unije**, zlasti za zagotovitev skupnega okvira za obravnavanje občutljivih netajnih in tajnih podatkov[9].

Da bi zagotovila lastno operativno varnost in situacijsko zavedanje, bo Komisija revidirala svoj okvir korporativnega upravljanja varnosti in ustanovila **Center za povezane varnostne operacije (ISOC)** za zaščito ljudi, materialnih sredstev in operacij na vseh lokacijah Komisije. Komisija bo okrepila tudi svoje operativne in analitične zmogljivosti za prepoznavanje in blaženje hibridnih groženj.

V skladu s strategijo za unijo pripravljenosti bodo vidiki pripravljenosti in varnosti vključeni v zakonodajo, politike in programe EU. Komisija bo pri pripravi ali pregledu zakonodaje, politik ali programov imela v mislih vidik pripravljenosti in varnosti v mislih ter dosledno opredelila morebitne učinke prednostne možnosti politike na pripravljenost in varnost. To bo podprto z rednim usposabljanjem oblikovalcev politik v Komisiji.

V podporo državam članicam bo Komisija s Svetom razpravljala o spreminjajočih se izzivih na področju notranje varnosti in ključnih prednostnih nalogah politike ter ga redno obveščala o izvajanju strategije. Komisija bo obveščala tudi Evropski parlament in ustrezne deležnike ter poskrbela za njihovo udeležbo pri vseh zadevnih ukrepih.

Ključni ukrepi

Komisija bo:

- **pripravljala in predstavljala redne analize groženj za izzive notranje varnosti EU.**

Države članice se poziva, naj:

- **izboljšajo izmenjavo obveščevalnih podatkov s SIAC ter zagotovijo boljšo izmenjavo informacij z agencijami in organi EU.**

Evropski parlament in Svet sta pozvana:

- **da zaključita pogajanja o predlagani uredbi o informacijski varnosti v institucijah, organih, uradih in agencijah Unije.**

3. Okrepljene varnostne zmogljivosti EU

Razvili bomo nova orodja za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, kot je prenovljen Europol, ter boljša sredstva za usklajevanje in zagotavljanje varne izmenjave podatkov in zakonitega dostopa do njih.

Za učinkovit boj proti spreminjajočim se grožnjam mora EU okrepiti svoje varnostne zmogljivosti in spodbujati inovacije. Organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodni organi kot glavni akterji proti grožnjam za notranjo varnost potrebujejo ustrezna operativna orodja in zmogljivosti za hitro in učinkovito ukrepanje. Za učinkovito

[9] COM(2022) 119 final.

preprečevanje, odkrivanje, preiskovanje in pregon je pomembno, da lahko ti organi komunicirajo ter se usklajujejo prek meja in med službami.

Agencije in organi EU za notranjo varnost

Agencije in organi EU na področju pravosodja, notranjih zadev in kibernetske varnosti imajo ključno vlogo v varnostni arhitekturi EU – vlogo, ki s širitvijo njihovih pristojnosti stalno raste.

Danes, 25 let po ustanovitvi, je **Europol** bolj kot kdaj koli prej osrednjega pomena za varnostni okvir EU. Podpira zapletene čezmejne preiskave, olajšuje izmenjavo informacij, razvija inovativna orodja za policijsko delo in zagotavlja napredno strokovno znanje za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Vendar pa mu več dejavnikov preprečuje, da bi v celoti dosegel svoj operativni potencial pri podpiranju preiskovalnih in operativnih dejavnosti za boj proti čezmejnemu kriminalu: ti segajo vse od nezadostne ravni virov do dejstva, da njegov sedanji mandat ne zajema novih varnostnih groženj, kot so sabotaže, hibridne grožnje ali manipuliranje z informacijami. Zato bo Komisija predlagala **ambiciozno prenovo mandata Europola**, da bi ta postal resnično operativna policijska agencija, ki bi bolje podpirala države članice. Cilj je okrepiti Europolovo tehnološko usposobljenost in zmogljivosti za podporo nacionalnim organom preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, izboljšati usklajevanje z drugimi agencijami in organi ter državami članicami, okrepiti strateška partnerstva s partnerskimi državami in zasebnim sektorjem ter zagotoviti okrepljen nadzor nad Europolom.

Poleg tega si bo Komisija prizadevala za nadaljnje **izboljšanje učinkovitosti in dopolnjevanja agencij in organov EU za notranjo varnost ter okrepitev nemotenega sodelovanja** med njimi.

Mandat **Eurojusta** bo ocenjen in okrepljen za učinkovitejše pravosodno sodelovanje, kar bo okrepilo dopolnjevanje in sodelovanje z Europolom. To vključuje izboljšanje učinkovitosti Eurojusta ter njegove zmogljivosti za zagotavljanje proaktivne podpore in analiz pravosodnim organom držav članic. Poleg tega bo Komisija glede na edinstveno pristojnost **Evropskega javnega tožilstva (EJT)** za preiskovanje in pregon kaznivih dejanj, ki škodijo finančnim interesom Unije, preučila, kako najbolje izboljšati zmogljivost EJT za zaščito sredstev Unije. To bo vključevalo krepitev sodelovanja med EJT in Europolom.

Učinkovita in varna izmenjava informacij med agencijami je ključna za sodelovanje. Na podlagi skupne izjave iz januarja 2024[10] Europol in Frontex potrebujeta hitro medsebojno izmenjavo informacij, tudi za operativne namene. Agencija **eu-LISA** ima osrednjo vlogo pri zagotavljanju varne hrambe in razpoložljivosti podatkov za boljše usklajevanje in učinkovitejšo izmenjavo informacij med agencijami. **Agencija EU za temeljne pravice** zagotavlja strokovno znanje o varstvu temeljnih pravic pri razvoju in izvajanju varnostnih politik.

Organ EU za preprečevanje pranja denarja (AMLA) je pooblaščen za navzkrižno preverjanje informacij na podlagi sistema, ali obstaja zadetek ali ne med informacijami, ki jih dajo na voljo Europol, EJT, Eurojust in Urad EU za boj proti goljufijam za izvajanje skupnih analiz čezmejnih primerov.

ENISA ima osrednjo vlogo pri izvajanju evropske zakonodaje o kibernetski varnosti. Komisija bo v prihodnji **reviziji akta o kibernetski varnosti** ocenila njen mandat in predlagala njegovo posodobitev, da bi povečala njeno dodano vrednost EU.

Sodelovanje med carinskimi organi in drugimi organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj se bo okrepilo s predlagano ustanovitvijo **carinskega organa EU** in **EU vozlišča**

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

carinskih podatkov v okviru svežnja carinskih reform EU. Informacije prihodnjega vozlišča in povezani podatki Europola, Eurojusta, EJT, OLAF, AMLA in Frontexa v okviru njihovih pristojnosti bodo okrepili skupno analizo in prispevali k bolj usklajenim operativnim dejavnostim, zlasti na zunanjih mejah. Komisija spodbuja sozakonodajalca, naj hitro zaključita pogajanja o carinski reformi EU, in jima bo v ta namen še naprej pomagala.

Izboljšanje dopolnjevanja med EJT, OLAF, Europolom, Eurojustom, AMLA in predlaganim carinskim organom EU bo temeljilo tudi na rezultatih tekočega pregleda **strukture EU za boj proti goljufijam**. Tak celosten pristop, ki se osredotoča na boljšo uporabo kazenskih in upravnih sredstev, interoperabilnost informacijskih sistemov in boljše sodelovanje, lahko koristi notranji varnosti.

Kritične komunikacije

Kritični komunikacijski sistemi[11] danes večinoma delujejo ločeno na nacionalni ravni. To pomeni, da prvi reševalci pogosto ne morejo komunicirati s sorodnimi organi, ko prestopijo mejo v druge države članice. V nekaterih državah članicah obstajajo tudi omejitve glede komunikacije med različnimi vrstami reševalcev (npr. policijo in reševalnimi vozili). Standardi večine sistemov ne izpolnjujejo današnjih zahtev glede funkcionalnosti in odpornosti, kar znatno omejuje odzivno zmogljivost prvih reševalcev, zlasti čezmejno.

Za izboljšanje zmogljivosti EU za odzivanje na krize bo Komisija predlagala zakonodajo za vzpostavitev **evropskega kritičnega komunikacijskega sistema (EUCCS)**, ki bo povezal kritične komunikacijske sisteme naslednje generacije držav članic v EU. Cilj je, da EUCCS temelji na treh strateških stebrih: operativni mobilnosti, močni odpornosti in strateški avtonomiji. Pobuda EUCCS bo določila harmonizirane zahteve in pomagala posodobiti kritične komunikacijske sisteme držav članic, kar jim bo omogočilo nemoteno delovanje. Razširila bo tudi pokritost sistema, in sicer s prihodnjim multiorbitalnim sistemom IRIS[2] [12]. S projekti, ki jih financira EU, bodo zgrajene tehnične zmogljivosti za EUCCS, pri čemer se bodo projekti opirali predvsem na evropske ponudnike tehnologije, da bi spodbudili strateško avtonomijo EU v tem občutljivem sektorju.

Zakonit dostop do podatkov

Organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodni organi morajo biti sposobni preiskovati kriminal in ukrepati proti njemu. Danes imajo skoraj vse oblike hudih kaznivih dejanj in organiziranega kriminala digitalni odtis[13]. Približno 85 % kazenskih preiskav se danes zanaša na zmožnost organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, da dostopajo do digitalnih informacij[14].

Skupina na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon je v svojem sklepnem poročilu[15] poudarila, da so organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter sodstvo v zadnjem desetletju zaostali za storilci kaznivih dejanj, saj se ti poslužujejo orodij in izdelkov iz drugih jurisdikcij, ki jim jih zagotavljajo ponudniki, ki so uvedli ukrepe, ki jim onemogočajo, da bi se odzvali na zakonite zahteve v posameznih kazenskih zadevah. Sistematično sodelovanje med organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter zasebnimi strankami, vključno s ponudniki storitev, je zato

[11] To so mreže, ki jih uporabljajo organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, mejni policisti, carinski organi, civilna zaščita, gasilci, reševalci in drugi ključni akterji na področju javne varnosti.
[12] Infrastruktura EU za odpornost, medsebojno povezljivost in varnost po satelitu.
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex:52019PC0070.
[15] Sklepno poročilo skupine na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon – 15. november 2024, 4802e306-c364-4154-835b-e986a9a49281_en.

bistveno v prihodnjih prizadevanjih za razbitje najnevarnejših kriminalnih mrež in posameznikov v Uniji in zunaj nje.

Ker je digitalizacija vse bolj prevladujoča in storilcem kaznivih dejanj zagotavlja vse večji vir novih orodij, je okvir za dostop do podatkov, ki ustreza potrebam po izvrševanju naše zakonodaje in zaščiti naših vrednot, bistvenega pomena. Hkrati je zagotavljanje, da digitalni sistemi ostanejo varni pred nepooblaščenim dostopom, enako bistveno za ohranitev kibernetske varnosti in zaščito pred nastajajočimi varnostnimi grožnjami. Taki okviri za dostop morajo spoštovati tudi temeljne pravice in med drugim zagotavljati ustrezno varstvo zasebnosti in osebnih podatkov.

EU je v zadnjih letih sprejela ukrepe tako za boj proti **spletnemu kriminalu kot tudi za olajšanje dostopa do digitalnih dokazov za vsa kazniva dejanja**, in sicer s sprejetjem pravil o elektronskih dokazih, ki se bodo v celoti uporabljala od avgusta 2026[16]. Dopolnjevali jih bodo mednarodni instrumenti za izmenjavo informacij in dokazov. Komisija bo kmalu predlagala podpis in sklenitev nove **Konvencije ZN proti kibernetski kriminaliteti**.

Za ukrepanje na podlagi priporočil skupine na visoki ravni[17], bo Komisija v prvi polovici leta 2025 predstavila **kažipot, v katerem bodo določeni pravni in praktični ukrepi**, ki jih predlaga za **zagotovitev zakonitega in učinkovitega dostopa do podatkov**. Komisija bo v okviru nadaljnjega ukrepanja na podlagi tega kažipota dala prednost oceni učinka **pravil o hrambi podatkov** na ravni EU in pripravi **tehnološkega kažipota za šifriranje**, da bi opredelila in ocenila tehnološke rešitve, ki bi organom preprečevanja, odkrivanja in preiskovanja kaznivih dejanj omogočile zakonit dostop do šifriranih podatkov ter zaščitile kibernetsko varnost in temeljne pravice.

Operativno sodelovanje

Komisija bo sodelovala z državami članicami, agencijami in organi EU ter partnerskimi državami, da bi okrepila operativno sodelovanje, ki je bistveno za učinkovitejši pristop k boju proti mednarodnemu organiziranemu kriminalu in terorizmu.

Evropska večdisciplinarna platforma proti grožnjam kriminala (EMPACT) je kot glavni okvir EU za skupno ukrepanje proti hudim kaznivim dejanjem in organiziranemu kriminalu dosegla znatne operativne rezultate. Naslednji cikel EMPACT 2026–2029 je priložnost za nadaljnjo okrepitev tega okvira. Da bi razbili najnevarnejše kriminalne mreže in posameznike, mora Unija racionalizirati svoja prizadevanja in se osredotočiti na najnujnejše prednostne naloge, s krepitvijo zavez držav članic in zagotavljanjem učinkovite rabe virov.

V ta namen bo Komisija sodelovala s predsedstvi Sveta in državami članicami, da bi **čim bolje izkoristila potencial EMPACT in obravnavala ključne prednostne naloge za naslednji cikel EMPACT 2026–2029**. Na teh prednostnih področjih so potrebni obveščevalni podatki o najnevarnejših kriminalnih mrežah, skupne preiskave in operativne projektne skupine ter odločen pravosodni odziv, vključno s pristopom sledenja denarju. Poleg tega se mora Unija boriti proti novačenju v kriminal in infiltraciji kriminala ter okrepiti sodelovanje in usposabljanje na področju večagencijskega in mednarodnega preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

Komisija bo podpirala tudi druge oblike **čezmejnega operativnega sodelovanja na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj med državami članicami in**

[16] Uredba (EU) 2023/1543 Evropskega parlamenta in Sveta z dne 12. julija 2023 o evropskem nalogu za posredovanje in evropskem nalogu za zavarovanje elektronskih dokazov v kazenskih postopkih ter za izvrševanje zapornih kazni po kazenskem postopku (UL L 191, 28.7.2023).

[17] Sklepi Sveta o dostopu do podatkov za učinkovito odkrivanje in pregon (12. december 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/en/pdf.

pridruženimi schengenskimi državami. Schengensko območje brez nadzora na notranjih mejah zahteva tesno sodelovanje in izmenjavo informacij med organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj držav članic, da se zagotovi visoka raven notranje varnosti. Uradniki organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj se danes še vedno soočajo z izzivi pri nadzoru ali izvajanju nujnih čezmejnih posredovanj[18], preprečevanje hibridnih groženj pa zahteva tudi okrepljeno čezmejno sodelovanje. Ustanoviti bi bilo treba **skupino na visoki ravni za prihodnost operativnega sodelovanja na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj**, da bi razvili skupno strateško vizijo.

Učinkovita izmenjava podatkov med organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj je bistvena tudi za učinkovito čezmejno sodelovanje. Ko bo **arhitektura interoperabilnosti** vzpostavljena, bo organom preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter Europolu zagotovila učinkovit dostop do ključnih informacij. Hkrati bi morale EU in njene države članice dati prednost dvostranski in večstranski izmenjavi informacij s pravnim in tehničnim izvajanjem **uredbe Prüm II**[19] v sodelovanju z eu-LISA in Europolom. To bo omogočilo varno avtomatizirano izmenjavo prstnih odtisov, profilov DNK, podatkov iz registrov vozil, podob obraza in policijskih evidenc prek usmerjevalnikov EU. Na nacionalni ravni morajo države članice izvajati **direktivo o izmenjavi informacij**[20], ki izboljšuje kanale za izmenjavo informacij za nemoten čezmejni pretok informacij, hkrati pa zagotavlja njihovo povezovanje s sistemi na ravni Unije, kot je SIENA[21].

Učinkovito čezmejno sodelovanje temelji tudi na spodbujanju **skupne kulture preprečevanja, odkrivanja in preiskovanja kaznivih dejanj v EU**. Za dosego tega cilja so bistvenega pomena skupno usposabljanje, centri odličnosti in programi mobilnosti. Komisija bo preučila, kako lahko EU najbolje podpre usposabljanje za organe držav članic, pri čemer se bo oprla na **CEPOL** kot agencijo EU za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

Krepitev varnosti meja

Krepitev odpornosti in varnosti zunanjih meja je ključna za preprečevanje hibridnih groženj, kot je instrumentalizacija migracij, za preprečevanje vstopa akterjev groženj in blaga v EU ter za učinkovit boj proti čezmejnemu kriminalu in terorizmu. **Schengenski informacijski sistem (SIS) bo po načrtih okrepljen** leta 2026, da bodo lahko države članice na podlagi podatkov, ki jih tretje države delijo z Europolom, vanj vnesle razpise ukrepov v zvezi z državljani tretjih držav, vpletenimi v terorizem, vključno s tujimi terorističnimi bojevniki, in druga huda kazniva dejanja.

Izboljšana **interoperabilnost** obsežnih informacijskih sistemov EU bo državam članicam zagotovila bistvene informacije o posameznikih iz tretjih držav, ki prečkajo ali nameravajo prečkati zunanje meje, kar bo organom pomagalo oceniti pogoje za odobritev vstopa na ozemlje

[18] Kot je navedeno v oceni Komisije o učinku Priporočila Sveta (EU) 2022/915 z dne 9. junija 2022 o operativnem sodelovanju na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (5909/25) s strani držav članic.

[19] Uredba (EU) 2024/982 Evropskega parlamenta in Sveta z dne 13. marca 2024 o avtomatiziranem iskanju in izmenjavi podatkov za policijsko sodelovanje ter spremembi sklepov Sveta 2008/615/PNZ in 2008/616/PNZ ter uredb (EU) 2018/1726, (EU) 2019/817 in (EU) 2019/818 Evropskega parlamenta in Sveta (Uredba Prüm II) (UL L 2024/982, 5.4.2024).

[20] Direktiva (EU) 2023/977 Evropskega parlamenta in Sveta z dne 10. maja 2023 o izmenjavi informacij med organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj držav članic ter razveljavitvi Okvirnega sklepa Sveta 2006/960/PNZ (UL L 134, 22.5.2023, str. 1).

[21] Secure Information Exchange Network Application (mrežna aplikacija za varno izmenjavo informacij).

držav članic[22]. Komisija bo še naprej tesno sodelovala z državami članicami in eu-LISA za hitro izvajanje teh sistemov, zlasti **vstopno-izstopnega sistema (SVI), evropskega sistema za potovalne odobritve (ETIAS) in revidiranega vizumskega informacijskega sistema (VIS)**, da bi zagotovila njihovo nemoteno delovanje in koristi za varnost.

Za nadaljnje izboljšanje varnosti meja in okrepitev sodelovanja EU glede na spreminjajoče se grožnje bo **Komisija predlagala okrepitev agencije Frontex**. Število mejnih policistov Evropske mejne in obalne straže bi se moralo sčasoma potrojiti na 30 000. Agencija bi morala biti opremljena z napredno tehnologijo za nadzor in situacijsko zavedanje, vključno z obveščevalnimi podatki, pomembnimi za evropsko integrirano upravljanje meja, in dostopom do zanesljivih vladnih storitev EU za opazovanje Zemlje za nadzor meja, ki se bodo uvedle do leta 2027. To bi moralo dodatno izboljšati zmožnost odkrivanja in preprečevanja čezmejnega kriminala na zunanjih mejah in boja proti njemu ter okrepiti podporo državam članicam pri izvajanju vračanja, zlasti državljanov tretjih držav, ki predstavljajo varnostno tveganje.

Ponarejanje listin in identitetne prevare olajšujejo tihotapljenje migrantov, trgovino z ljudmi, prikrita kriminalna gibanja in trgovino z nedovoljenim blagom. **Detektor več identitet (MID)**[23] bo, ko bo začel delovati, izboljšal sposobnost nacionalnih organov za identifikacijo posameznikov, ki uporabljajo več identitet, in boj proti identitetnim prevaram. Komisija bo preučila načine za izboljšanje varnosti potnih listin in dokumentov za prebivanje, izdanih državljanom EU in državljanom tretjih držav. Poleg tega bo Komisija ocenila, kako lahko denarnice EU za digitalno identiteto, ki bodo uvedene v okviru evropskega okvira za digitalno identiteto do konca leta 2026, prispevajo k izboljšanju varnosti potnih listin in preverjanja identitete. To bo dopolnilo predloga o digitalnih potovalnih dokumentih in digitalni potovalni aplikaciji EU[24].

Potovalne informacije so ključne za organe pri odkrivanju in preiskovanju gibanja storilcev kaznivih dejanj, teroristov in drugih oseb, ki predstavljajo varnostne grožnje. Čeprav obstaja okvir EU za informacije o komercialnem zračnem prometu[25], je obdelava podatkov iz drugih načinov prevoza za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj razdrobljena. Posledično lahko storilci kaznivih dejanj in teroristi izkoriščajo različne načine prevoza za nezakonite dejavnosti, ne da bi jih pri tem odkrili. Komisija bo sodelovala z državami članicami in prometnim sektorjem, da bi **okrepila okvir za potovalne informacije**, in sicer s preučitvijo sheme Unije, ki od operaterjev zasebnih letov zahteva zbiranje in prenos podatkov o potnikih, oceno pravil za obdelavo evidenc podatkov o potnikih in oceno načinov za racionalizacijo obdelave potovalnih informacij o pomorskem prevozu. Za cestni promet bo Komisija ocenila razširjeno uporabo sistemov za **samodejno prepoznavanje registrskih tablic (ANPR)** in povečala možnosti za sinergije s SIS.

Predvidevanje, inovacije in pristop, ki temelji na zmogljivostih

Komisija bo razvila **celovit pristop predvidevanja na področju notranje varnosti na ravni EU**, ki bo temeljil na dobrih praksah, opredeljenih na nacionalni ravni. Ta pristop bo podpiral

[22] Vstopno-izstopni sistem (SVI) bo državam članicam zlasti omogočil identifikacijo državljanov tretjih držav na zunanjih mejah schengenskega območja ter evidentiranje njihovih vstopov in izstopov, kar bo omogočilo sistematično identifikacijo oseb, ki so prekoračile obdobje dovoljenega bivanja. Evropski sistem za potovalne informacije in odobritve (ETIAS) in vizumski informacijski sistem (VIS) bosta pred prihodom državljana tretje države na zunanje meje državam članicam omogočila, da predhodno ocenijo, ali bi prisotnost državljana tretje države na ozemlju EU pomenila varnostno tveganje.

[23] MID je eden od sestavnih delov interoperabilnosti, uvedenih z Uredbo (EU) 2019/818 in Uredbo 2019/817.

[24] https://ec.europa.eu/commission/presscorner/detail/sl/ip_24_5047.

[25] Okvira za evidenco podatkov o potnikih (PNR) in za predhodne informacije o potnikih (API), vzpostavljena z Direktivo (EU) 2016/681 (direktiva o PNR) ter Uredbo (EU) 2025/12 in Uredbo (EU) 2025/13 (uredbi o API).

oblikovanje politik in usmerjal naložbe v ustrezne raziskave in inovacije na področju varnosti, ki jih financira EU.

Raziskave in inovacije imajo ključno vlogo na področju notranje varnosti, saj ustvarjajo rešitve za boj proti nastajajočim grožnjam, vključno z zlorabo tehnologije[26]. EU mora prek raziskav in inovacij na področju varnosti, ki jih financira EU[27], še naprej vlagati v razvoj inovativnih orodij in rešitev za obravnavanje varnostnih groženj ob spoštovanju pravil EU in temeljnih pravic. Komisija bi morala podpirati prehod z raziskav na uvajanje, da bi zagotovila učinkovito uporabo teh sodobnih zmogljivosti, pri čemer bi morala dati prednost **sodobnim tehnologijam**, kot je umetna inteligenca. Ta pristop bi moral vključevati usposabljanje za izboljšanje uporabe umetnointeligenčnih sistemov in drugih tehničnih zmogljivosti s strani organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodnih organov. Poleg tega bi bilo treba potencial tehnologij z dvojno rabo izkoristiti v obeh smereh (od civilne do obrambne in od obrambne do civilne rabe)[28], kadar je ustrezno.

Inovacijsko vozlišče EU za notranjo varnost[29], mreža laboratorijev za inovacije, ki zagotavlja najnovejše posodobitve inovacij in učinkovite rešitve v podporo delu akterjev na področju notranje varnosti v EU in državah članicah, bo pripomoglo k vključevanju raziskav v prakso in politiko. Za povečanje učinkovitosti Europola je treba okrepiti Europolovo odložišče orodij (ETR), kar mu bo omogočilo operativna opredelitev, razvoj, skupno naročanje in uporaba naprednih tehnologij. Poleg tega bo Komisija v svojem skupnem raziskovalnem središču ustanovila **kampus za raziskave in inovacije na področju varnosti**, ki bo združeval raziskovalce, da bi skrajšali cikel od rezultatov raziskav do inovacij, razvoja in uspešnega izvajanja, hkrati pa zmanjšali stroške razvoja, preskušanja in potrjevanja.

Naš **evropski raziskovalni prostor** je že po svoji naravi sodelovalen in je zato občutljiv na tuje vmešavanje in dezinformacije. Po sprejetju priporočila Sveta o varnosti raziskav[30] Komisija in države članice sprejemajo ukrepe za opolnomočenje zadevnih akterjev, med drugim z ustanovitvijo strokovnega centra za varnost raziskav.

Ključni ukrepi

Komisija bo sprejela:

- **zakonodajni predlog za preoblikovanje Europola v resnično operativno agencijo za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v letu 2026;**
- **zakonodajni predlog za okrepitev Eurojusta v letu 2026;**
- **zakonodajni predlog za okrepitev vloge in nalog agencije Frontex v letu 2026;**
- **zakonodajni predlog za vzpostavitev evropskega kritičnega komunikacijskega sistema v letu 2026.**

Komisija bo:

- **v letu 2025 predstavila kažipot, ki določa nadaljnje korake v zvezi z zakonitim in učinkovitim dostopom do podatkov za organe preprečevanja, odkrivanja in preiskovanja kaznivih dejanj;**

[26] Glej poročilo Skupnega raziskovalnega središča Komisije „Nastajajoča tveganja in priložnosti za notranjo varnost EU, ki izhajajo iz novih tehnologij“, https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] Študija o krepitvi raziskav in inovacij na področju varnosti, ki jih financira EU – 20 let raziskav in inovacij na področju civilne varnosti, ki jih financira EU – 2025, https://data.europa.eu/doi/10.2837/0004501.
[28] Kot je navedeno v Niinistöjevem poročilu.
[29] Inovacijsko vozlišče EU za notranjo varnost | Europol.
[30] UL C/2024/3510, 30.5.2024.

- **v letu 2025 pripravila oceno učinka z namenom posodobitve pravil o hrambi podatkov na ravni EU, kot je ustrezno;**
- **v letu 2026 predstavila tehnološki kažipot za šifriranje, da bi opredelili in ocenili tehnološke rešitve, da bi organom preprečevanja, odkrivanja in preiskovanja kaznivih dejanj omogočili zakonit dostop do podatkov;**
- **si prizadevala za ustanovitev skupine na visoki ravni za okrepitev operativnega sodelovanja na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj;**
- **v letu 2026 ustanovila kampus za raziskave in inovacije na področju varnosti v Skupnem raziskovalnem središču.**

Komisija bo v sodelovanju z državami članicami in ustreznimi agencijami EU:

- **okrepila strukturo EMPACT;**
- **si prizadevala za hitro uvedbo arhitekture interoperabilnosti in izvajanje uredbe Prüm II;**
- **okrepila okvir za potovalne informacije.**

Države članice se poziva, naj:

- **prenesejo in v celoti izvajajo direktivo o izmenjavi informacij.**

4. Odpornost proti hibridnim grožnjam in drugim sovražnim dejanjem

Odpornost proti hibridnim grožnjam bomo okrepili z izboljšanjem zaščite kritične infrastrukture, krepitvijo kibernetske varnosti, varovanjem prometnih vozlišč in pristanišč ter bojem proti spletnim grožnjam.

Pogostost in izpopolnjenost sovražnih dejanj, ki ogrožajo varnost EU, sta se povečali, zlonamerni akterji pa so močno razširili svoj nabor orožij. Hibridne kampanje, usmerjene proti EU, njenim državam članicam in partnerjem, so se okrepile in vključujejo dejanja, kot so sabotaža, usmerjena v kritično infrastrukturo, požigi, kibernetski napadi, vmešavanje v volitve, tuje vmešavanje in manipuliranje z informacijami, vključno z dezinformacijami, ter instrumentalizacija migracij. Institucijam, organom, uradom in agencijam Unije (subjektom Unije) zaradi njihove politične in operativne vloge ter narave informacij, ki jih obdelujejo, ni prizaneseno.

EU mora **okrepiti svojo odpornost**, učinkovito uporabljati obstoječa orodja in razviti nove načine za soočanje s temi spreminjajočimi se grožnjami, ki izhajajo iz državnih in nedržavnih akterjev, tako zdaj kot v prihodnosti.

Kritična infrastruktura

Grožnje **kritični infrastrukturi**, vključno s hibridnimi grožnjami, kot sta sabotaža in zlonamerna kibernetska dejavnost, so zelo zaskrbljujoče, zlasti za infrastrukturo, ki povezuje države članice – pa naj gre za povezovalne daljnovode ali čezmejne komunikacijske kable in promet. Od ruske vojne agresije proti Ukrajini se je število sabotaž, usmerjenih v kritično infrastrukturo, povečalo, zlasti leta 2024, kar je prizadelo številne države članice. Sodelovanje med organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, varnostnimi službami in službami za kibernetsko varnost, vojaško in civilno zaščito ter zasebnimi izvajalci je bistveno za učinkovito napovedovanje, odkrivanje in preprečevanje takih dejanj ter odzivanje nanje.

Zmanjšanje ranljivosti in krepitev odpornosti kritičnih subjektov sta nujna za zagotovitev neprekinjenega zagotavljanja bistvenih storitev za gospodarstvo in družbo. Ključna za doseganje tega sta pravočasen prenos in pravilno izvajanje **direktive o odpornosti kritičnih**

subjektov (CER)[31] in **direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (NIS2)**[32] s strani vseh držav članic.

Za zagotovitev hitrega napredka bo Komisija v sodelovanju s **skupino za odpornost kritičnih subjektov in skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov** podpirala države članice pri opredelitvi kritičnih subjektov[33] in izmenjavi dobrih praks v zvezi z nacionalnimi strategijami in ocenami tveganja v zvezi z bistvenimi storitvami. Če bi prišlo do motenj kritične infrastrukture s pomembnimi čezmejnimi vplivi, bi se odziv na ravni EU usklajeval na podlagi **načrta EU za kritično infrastrukturo**. Komisija poziva Svet, naj hitro sprejme **kibernetski načrt EU**, ki bo dodatno okrepil usklajevanje v okviru kriznega upravljanja in olajšal tesnejše sodelovanje med organi na področju fizične in digitalne odpornosti. Po uspešnih stresnih testih v energetskem sektorju leta 2023 bo Komisija spodbujala **prostovoljne stresne teste** v drugih ključnih sektorjih za notranjo varnost. Poleg tega bo Komisija zagotovila **pregled čezmejnih in medsektorskih tveganj** za bistvene storitve **na ravni Unije**, da bi podprla ocene tveganja držav članic in prispevala k celoviti oceni tveganja na ravni EU. V skladu s strategijo za unijo pripravljenosti bo Komisija sodelovala z državami članicami, da bi opredelila nadaljnje sektorje in storitve, ki niso zajeti v veljavni zakonodaji in v zvezi s katerimi je morda potrebno ukrepati.

Projektna skupina EU-NATO za odpornost kritične infrastrukture je spodbujala odlično sodelovanje pri izmenjavi dobrih praks in krepitvi odpornosti v energetskem, prometnem, digitalnem in vesoljskem sektorju. To delo se bo nadaljevalo v okviru **strukturiranega dialoga med EU in Natom o odpornosti**. **Nabor orodij EU za odzivanje na hibridne grožnje** zagotavlja trdno podporo državam članicam in partnerjem pri pripravah na hibridne grožnje in njihovem preprečevanju. **Skupine za hitro odzivanje na hibridne grožnje**[34] državam članicam, različnim misijam in partnerjem EU na zahtevo zagotavljajo prilagojeno kratkoročno pomoč. Poleg tega bo Komisija nadaljevala sodelovanje EU v boju proti sabotaži s strokovnimi dejavnostmi[35], vključno z **namenskim skupnim delovnim programom** za strokovnjake za racionalizacijo izmenjave informacij in opredelitev protiukrepov.

Incidenti, ki vplivajo na **podvodne kable** v Evropi, kažejo, da so potrebni strožji ukrepi in jasnejši odzivi. Kot je navedeno v **akcijskem načrtu EU za varnost kablov**[36], bo Komisija skupaj z visokim predstavnikom sodelovala z državami članicami, agencijami EU in partnerji, kot je Nato, pri preprečevanju in odkrivanju groženj za podmorske kable, odzivanju nanje in odvračanju od njih. Za pridobitev celovite slike stanja glede groženj bo Komisija sodelovala z državami članicami pri razvoju in prostovoljnem uvajanju integriranega mehanizma nadzora za podvodne kable po morskih bazenih, začenši s severnomorskim/baltskim regionalnim vozliščem.

[31] Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES.
[32] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2).
[33] Sektorji, ki jih zajema Direktiva, so energetika, promet, bančništvo, infrastruktura finančnega trga, zdravje, pitna voda, odpadne vode, digitalna infrastruktura, javna uprava, vesolje, proizvodnja, predelava in distribucija hrane.
[34] Strateški kompas EU za varnost in obrambo 2022, str. 22.
[35] Svetovalci EU za zaščito in varnost, Evropska mreža za odstranjevanje neeksplodiranih ubojnih sredstev (EEODN), mreža ATLAS, varnostna mreža EU za visoka tveganja (EU HRSN), svetovalna skupina za KBRJ varnost, skupina za odpornost kritičnih subjektov (CERG).
[36] JOIN(2025) 9 final.

Kibernetska varnost

Vztrajnost **zlonamernih kibernetskih dejavnosti**, ki so pogosto del širšega spektra večdimenzionalnih in hibridnih groženj, zahteva stalno pozornost in ukrepanje na evropski ravni. Unija je v zadnjih letih sprejela vrsto zakonov o kibernetski varnosti, ki krepijo kibernetsko odpornost subjektov, zajetih v direktivi NIS2, ki delujejo v kritičnih sektorjih EU, in subjektov Unije[37], izboljšujejo varnost digitalnih proizvodov (akt o kibernetski odpornosti) ter vzpostavljajo okvir za pripravljenost in podporo odzivanju na incidente (akt o kibernetski solidarnosti). Komisija je januarja 2025 sprejela **evropski akcijski načrt za kibernetsko varnost bolnišnic in izvajalcev zdravstvenih dejavnosti**[38] za izboljšanje odkrivanja groženj ter pripravljenosti in odzivanja na krize. Ključno je, da se izvaja v celoti. Hkrati moramo za obravnavanje novih groženj in razvoja okrepiti naše ukrepe, zlasti na področju izmenjave informacij, varnosti dobavne verige, izsiljevalskega programja in kibernetskih napadov ter tehnološke suverenosti.

Poleg tega je za izvajanje treba zapolniti sedanjo vrzel v veščinah na področju kibernetske varnosti, saj manjka 299 000 ljudi. Komisija bo sodelovala z državami članicami v okviru unije spretnosti[39], da bi povečala delovno silo na področju kibernetske varnosti, zlasti s pomočjo nove akademije za kibernetske veščine. Strateški načrt za izobraževanje na področju naravoslovja, tehnologije, inženirstva in matematike[40] prispeva k izboljšanju nabora talentov in odziva Evrope na potrebe trga dela na področju kibernetske varnosti.

EU bo vzporedno s krepitvijo svoje odpornosti še naprej v celoti uporabljala okvir za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti (**zbirka orodij za kibernetsko diplomacijo**) za preprečevanje kibernetskih groženj, ki izhajajo iz državnih in nedržavnih akterjev, odvračanje od njih in odzivanje nanje.

Varnost dobavnih verig IKT

Zbirka orodij za varnost 5G zagotavlja ustrezen okvir za zaščito omrežij 5G, vendar jo države članice trenutno premalo izvajajo. Še vedno so prisotna nesprejemljiva varnostna tveganja, zlasti v zvezi z nadomestitvijo ponudnikov z visokim tveganjem. Usklajen pristop k varnosti dobavne verige IKT lahko odpravi sedanjo razdrobljenost notranjega trga, ki jo povzročajo različni pristopi na nacionalni ravni, prepreči kritične odvisnosti in zmanjša tveganje naših dobavnih verig IKT, ki izhaja iz dobaviteljev z visokim tveganjem, s čimer se zavaruje naša kritična infrastruktura.

V skladu s tem pristopom bo Komisija pri prihodnji **reviziji akta o kibernetski varnosti** širše obravnavala varnost in odpornost dobavnih verig in infrastrukture IKT. Poleg tega bo Komisija predlagala izboljšanje **evropskega certifikacijskega okvira za kibernetsko varnost**, da se zagotovi pravočasno sprejetje prihodnjih certifikacijskih shem in odzivanje na potrebe politike.

Komisija bo na podlagi obstoječih sektorskih ocen ali sektorskih ocen v pripravi[41] skupaj z državami članicami pripravila **strateško načrtovanje za usklajene ocene tveganj za kibernetsko varnost**.

---

[37] Uredba (EU, Euratom) 2023/2841 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije (UL L, 2023/2841, 18.12.2023.

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

[39] COM(2025) 90 final.

[40] COM(2025) 89 final.

[41] Na primer v zvezi z omrežji 5G, telekomunikacijami, električno energijo, energijo iz obnovljivih virov in povezanimi vozili.

Storitve v oblaku in telekomunikacijske storitve so postale osnova dobavnih verig kritične infrastrukture, podjetij in javnih organov. Komisija bo sprejela ukrepe za spodbujanje kritičnih subjektov, da se odločijo izbrati **storitve v oblaku in telekomunikacijske storitve, ki zagotavljajo ustrezno raven kibernetske varnosti**, pri čemer se bodo upoštevala ne samo tehnična tveganja, ampak tudi strateška tveganja in odvisnosti.

Izsiljevalsko programje in kibernetski napadi

Trdovraten velik izziv v EU in po svetu je **izsiljevalsko programje**, za katerega je v enem od poročil ocenjeno, da bodo skupni letni stroški do leta 2031 znašali več kot 250 milijard EUR[42]. **Direktiva NIS2** in **akt o kibernetski odpornosti** bosta znatno izboljšala varnostno stanje subjektov, zaradi česar bo izvajanje napadov za kriminalna omrežja, ki uporabljajo izsiljevalsko programje, postalo dražje. Poleg tega bo Komisija tesno sodelovala z državami članicami, da bi zagotovila, da se napadi z izsiljevalskim programjem, zlasti kadar gre za napredne trajne grožnje, in plačila odkupnine, pogosteje prijavljajo organom preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kar bo olajšalo preiskave.

Za preprečevanje in zaustavitev kibernetskih napadov mora EU okrepiti izmenjavo informacij med organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, organi in subjekti za kibernetsko varnost ter zasebnimi strankami pod okriljem Europola in Agencije EU za kibernetsko varnost (ENISA).

Europol in Eurojust bi morala še naprej graditi na dosežkih, ki sta jih dosegla pri razbijanju operacij izsiljevalskega programja, pri čemer bi morala podpirati sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. V ta namen bi morali organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj čim bolj povečati uporabo mehanizmov sodelovanja, vključno z **Europolovim mednarodnim modelom odzivanja na izsiljevalsko programje** in **mednarodno pobudo za boj proti izsiljevalskemu programju (CRI)**[43], ENISA in Europol pa bi morala sodelovati pri razširitvi odložišča orodij za dešifriranje različic izsiljevalskega programja[44].

Tehnološka suverenost

Kibernetska varnost in tehnološka suverenost sta tesno povezani, tehnološke odvisnosti pa je treba obravnavati prednostno. Unija mora **usmerjati razvoj in uvajanje novih tehnologij**, pri čemer si mora Komisija prizadevati za **krepitev zmogljivosti na področju strateških tehnologij**, kot so umetna inteligenca, kvantno računalništvo, napredna povezljivost, storitve v oblaku, storitve na robu in internet stvari[45], in sicer s prihodnjimi pobudami, kot so akcijski načrt za celino umetne inteligence, strategija za kvantno tehnologijo in druge[46]. Komisija bo še naprej podpirala pravočasno uvedbo najnovejših razpoložljivih mednarodno dogovorjenih **internetnih protokolov**, ki so bistveni za vzdrževanje nadgradljivega in učinkovitega interneta z višjo ravnjo kibernetske varnosti. Potrebni so tudi nadaljnji ukrepi za reševanje **izzivov, povezanih z radijskim spektrom**, na primer v zvezi s slepljenjem GNSS, motenjem, tveganji in odvisnostmi v dobavni verigi, kot je uporaba tehnologij kvantnega zaznavanja in raziskovanje razvoja zmogljivosti za spremljanje radijskih frekvenc.

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Na voljo v okviru projekta No More Ransom, https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] npr. EuropHPC JU https://eurohpc-ju.europa.eu/index_en, kvantna pobuda Domača stran kvantne pobude | kvantna pobuda, omrežja 3C (COM(2024) 81 final) in akcijski načrt EU za kabelsko varnost (JOIN(2025) 9 final).

Uvedba rešitev za **postkvantno kriptografijo** (PQC) bo ključna za zaščito občutljivih komunikacij, podatkov v mirovanju in zaščito digitalnih identitet v novi kvantni dobi. Komisija na podlagi priporočila iz leta 2024 o časovnem načrtu usklajenega izvajanja za prehod na postkvantno kriptografijo[47] sodeluje z državami članicami pri spodbujanju tega prehoda. V zvezi s tem bi morale države članice čim prej, najpozneje pa do konca leta 2030, opredeliti primere z visokim tveganjem pri kritičnih subjektih in zagotoviti kvantno varno šifriranje za te primere z visokim tveganjem. Komisija sodeluje tudi z državami članicami in Evropsko vesoljsko agencijo (ESA) pri razvoju in uvedbi **evropske infrastrukture za kvantno komunikacijo (EuroQCI)**[48] na podlagi kvantnega razdeljevanja ključa (QKD) v okviru programa EU za varno povezljivost **IRIS²**. Obe pobudi bosta subjektom omogočili varen prenos podatkov in shranjevanje informacij.

Kvantne tehnologije bodo imele ključno vlogo tudi pri varnostnih aplikacijah: v okviru **strategije za kvantno tehnologijo** bo pripravljen **kažipot za kvantno zaznavanje v varnostnih aplikacijah**. Podobno si Komisija prizadeva za kvantno odpornost svojih korporativnih varnostnih sistemov, vključno s tajnimi informacijskimi sistemi.

Podjetjem prijazen okvir za kibernetsko varnost

Prihodnja revizija akta o kibernetski varnosti je priložnost za **poenostavitev zakonodaje EU o kibernetski varnosti** v skladu s kompasom za konkurenčnost. Komisija bo tesno sodelovala z državami članicami, da bi zagotovila hitro, skladno in podjetjem prijazno izvajanje horizontalnega okvira za kibernetsko varnost iz direktive NIS2, akta o kibernetski odpornosti in akta o kibernetski solidarnosti, da bi spodbujala enostavnost in skladnost ter preprečila razdrobljenost ali podvajanje pravil o kibernetski varnosti v zakonodaji EU in nacionalni zakonodaji.

Da bi omogočili varen dostop do spletnih storitev in okrepili digitalno varnost po vsej EU, bo **evropski okvir za digitalno identiteto** pred koncem leta 2026 vsem državljanom in prebivalcem EU ponudil zaupanja vredne denarnice za digitalno identiteto. Prihodnja **evropska podjetniška denarnica** bo olajšala varno čezmejno interakcijo med podjetji in javnimi upravami. Oboje je pogoj za varno in učinkovitejše delovanje podatkovno vodenega enotnega trga z orodji, kot so enotno digitalno vstopno mesto, izdajanje elektronskih računov, e-javna naročila in digitalni potni list izdelkov.

Spletna varnost

Nekatere najresnejše hibridne grožnje, ki ogrožajo varnost in zaščito ljudi v Evropi ter so usmerjene v demokratično okolje EU, se odvijajo na spletu. Te grožnje vključujejo nezakonite dejavnosti in nezakonite spletne vsebine, manipulacijo z informacijami, ki vključuje umetno ojačevanje, zavajajoče informacije ter tuje manipuliranje z informacijami in vmešavanje (FIMI).

Dosledno izvrševanje **akta o digitalnih storitvah** je bistvenega pomena za zagotovitev varnega in dostopnega spletnega okolja z odgovornimi akterji, ki je odporno tudi na hibridne grožnje. Akt o digitalnih storitvah od ponudnikov zelo velikih spletnih platform in zelo velikih spletnih iskalnikov zahteva, da izvedejo ocene tveganja in uvedejo ukrepe za blaženje sistemskih tveganj, ki izhajajo iz zasnove, delovanja ali uporabe njihovih storitev. Taka tveganja lahko vključujejo negativne učinke na državljansko razpravo in volilne procese ter na javno varnost, kot je daljnosežno vmešavanje zlonamernih tujih državnih akterjev, na primer v volilne procese. Pomembno je usposabljanje pristojnih organov držav članic o uporabi pravnih orodij za

[47] Priporočilo o časovnem načrtu usklajenega izvajanja za prehod na postkvantno kriptografijo | Oblikovanje digitalne prihodnosti Evrope.
[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

takojšnjo odstranitev nezakonitih spletnih vsebin, zlasti v zvezi s kibernetskim nasiljem na podlagi spola. Akt o digitalnih storitvah določa mehanizem za odzivanje na krize, ki se lahko aktivira, kadar izredne razmere povzročijo resno grožnjo javni varnosti ali javnemu zdravju v Uniji ali njenem znatnem delu. Za dopolnitev tega mehanizma so Komisija in pristojni nacionalni organi, imenovani za koordinatorje digitalnih storitev, razvili tudi prostovoljni **okvir za odzivanje na incidente v okviru akta o digitalnih storitvah**. Koordinatorji digitalnih storitev so sprejeli tudi ukrepe za zaščito integritete volitev, na primer z organizacijo volilnih okroglih miz in stresnih testov[49]. Akt o digitalnih storitvah skupaj z uredbo o političnem oglaševanju[50] zagotavlja enega od več sklopov, povezanih z varovanjem demokracije in integritete demokratičnih procesov, ki so lahko tarča sovražnih akterjev, tudi z digitalnimi orodji in v družbenih medijih.

Izvajanje nabora orodij za preprečevanje **tujega manipuliranja z informacijami in vmešavanja** je še en pomemben element, ki zagotavlja ključno podporo na ravni EU. V središču teh prizadevanj je tudi podpiranje digitalne in medijske pismenosti ter kritičnega razmišljanja[51].

Preprečevanje instrumentalizacije migracij

Rusija je s pomočjo in odločno podporo Belorusije migracije namenoma uporabila kot orožje in nezakonito omogočala migracijske tokove proti zunanjim mejam EU, da bi destabilizirala naše družbe in spodkopala enotnost Evropske unije. To ne ogroža le nacionalne varnosti in suverenosti držav članic, temveč tudi varnost in celovitost schengenskega območja ter varnost Unije kot celote. Evropski svet je v sklepih iz oktobra 2024 poudaril, da Rusiji, Belorusiji oziroma kateri koli drugi državi ne smemo dovoliti, da bi zlorabljala naše vrednote, vključno s pravico do azila, in spodkopavala našo demokracijo.

Kot je navedeno v sporočilu Komisije iz leta 2024 o instrumentalizaciji migracij, je Unija poleg močne politične podpore sprejela finančne, operativne in diplomatske ukrepe, vključno s sodelovanjem z državami izvora in tranzita, da bi učinkovito obravnavala te grožnje[52]. Ta odziv vključuje uporabo novega okvira, ki ga je vzpostavil Svet, za sankcioniranje posameznikov in organizacij, ki sodelujejo pri ukrepih in politikah, kot je ruska instrumentalizacija migracij, z zamrznitvijo sredstev in prepovedjo potovanja[53]. EU bo po potrebi še naprej uporabljala ta okvir in podpirala države članice pri boju proti tej grožnji.

Varnost prometa

Morska pristanišča, letališča in kopenska infrastruktura so ključne vstopne in izstopne točke. Imajo ključno vlogo v gospodarstvu in družbi EU ter so bistvenega pomena za vojaško mobilnost. Vendar so ta prometna vozlišča in sredstva tudi glavna tarča zunanjih groženj in kriminalnih dejavnosti. Nedavni incidenti, vključno s kršitvami varnosti letalskega tovora in napadi na železniško infrastrukturo, kažejo na resna tveganja. **Prevozniki** so lahko tako cilji kot orodje za zlonamerne akterje. Obstoječi pravni instrumenti EU so izboljšali varovanje v letalstvu[54], vendar zaradi visoke stopnje ogroženosti civilnega letalstva potrebujemo način za

[49] Zbirka orodij za volitve za koordinatorje digitalnih storitev v okviru akta o digitalnih storitvah za leto 2025 https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Uredba (EU) 2024/900 Evropskega parlamenta in Sveta z dne 13. marca 2024 o preglednosti in ciljanju v političnem oglaševanju (UL L, 2024/900, 20.3.2024).
[51] Akcijski načrt za digitalno izobraževanje (2021–2027) – Evropski izobraževalni prostor.
[52] COM(2024) 570 final.
[53] Uredba Sveta (EU) 2024/2642 z dne 8. oktobra 2024 o omejevalnih ukrepih zaradi destabilizirajočih dejavnosti Rusije (ST/8744/2024/INIT) (UL L, 2024/2642, 9.10.2024).
[54] Uredba (ES) št. 300/2008 Evropskega parlamenta in Sveta z dne 11. marca 2008 o skupnih pravilih na področju varovanja civilnega letalstva (UL L 97, 9.4.2008, str. 72).

predvidevanje incidentov in hitro posvetovanje z zadevnimi državami članicami. Komisija bo sodelovala z državami članicami, da bi spremenila obstoječo izvedbeno zakonodajo na področju varovanja v letalstvu za izmenjavo tajnih podatkov o **dogodkih na področju varovanja v letalstvu**. Poleg tega bo Komisija razmislila o **regulativnih ukrepih** za obravnavanje novih groženj, kot so **incidenti v letalskem tovornem prometu**, in za okrepitev standardov varovanja v letalstvu. To bo vključevalo tudi okrepitev **zakonodaje o varovanju v letalstvu (AVSEC)**, da se omogočijo takojšnji odzivni ukrepi ob hkratnem ohranjanju območja enkratnega varnostnega pregleda na letališčih EU.

Komisija bo pri razvoju prihodnje **pristaniške strategije EU** na podlagi **zavezništva evropskih pristanišč** preučila načine za nadaljnjo krepitev zakonodaje o pomorski varnosti, da bi učinkovito obravnavala nastajajoče grožnje, zavarovala pristanišča in okrepila varnost dobavne verige EU. V ta namen bo Komisija zagotovila dosledno izvajanje zakonodaje ter si prizadevala za harmonizacijo nacionalnih praks in okrepitev preverjanja preteklosti v pristaniščih. Poleg varnostnih protokolov, vzpostavljenih za letalski tovor, bo Komisija sodelovala z državami članicami in zasebnim sektorjem pri razširitvi teh protokolov za zaščito verig pomorskega prometa.

Predlagani carinski organ EU bo analiziral in ocenil tveganja na podlagi **carinskih informacij** v zvezi z blagom, ki vstopa v EU, izstopa iz nje in je v tranzitu preko nje, da bi državam članicam pomagal preprečevati izkoriščanje mednarodnih dobavnih verig s strani zlonamernih akterjev. V skladu s strategijo EU za pomorsko varnost[55] bo imel prihodnji **evropski pakt za oceane** ključno vlogo pri krepitvi pomorske varnosti v morskih bazenih v EU in zunaj nje, tudi s spodbujanjem krepitve večnamenskih pomorskih operacij in vaj.

Odpornost oskrbovalnih verig

Evropa mora zmanjšati svojo odvisnost od tehnologij tretjih držav, ki lahko privede do odvisnosti in varnostnih tveganj. Komisija namerava zmanjšati odvisnosti od posameznih tujih dobaviteljev, zmanjšati tveganje naših dobavnih verig, ki izhaja iz dobaviteljev z visokim tveganjem, ter zaščititi zmogljivosti kritične infrastrukture in industrijske zmogljivosti na ozemlju EU, kot je določeno v **kompasu za konkurenčnost**[56] in **dogovoru o čisti industriji**[57] Komisija bo spodbujala **industrijsko politiko za notranjo varnost** s sodelovanjem z industrijo EU v ključnih sektorjih (npr. prometna vozlišča, kritična infrastruktura) za oblikovanje varnostnih rešitev, kot so oprema za odkrivanje, biometrične tehnologije in droni, pri katerih je varnost vključena v zasnovi. Komisija bo pri **ponovnem pregledu pravil EU o javnem naročanju** ocenila, ali varnostni vidiki iz direktive o javnih naročilih na področju obrambe in varnosti iz leta 2009[58] zadostujejo za obravnavanje potreb organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter kritičnih subjektov po odpornosti.

Komisija bo podpirala države članice pri **pregledu neposrednih tujih naložb** in javnih naročil opreme za logistična vozlišča, s čimer bo zagotovila, da kritična infrastruktura in tehnologija ostaneta varni.

Ko bo začel veljati **akt o izrednih razmerah na notranjem trgu in njegovi odpornosti (IMERA)**, bo EU pomagal pri obvladovanju kriz, ki povzročajo motnje kritičnih dobavnih verig ter prostega pretoka blaga, storitev in ljudi. Omogočil bo hitro krizno usklajevanje, opredelitev v krizi pomembnega blaga in storitev ter zagotovil nabor orodij za zagotovitev

[55] JOIN(2023) 8 final.
[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Direktiva 2009/81/ES o usklajevanju postopkov za oddajo nekaterih naročil gradenj, blaga in storitev, ki jih oddajo naročniki na področju obrambe in varnosti (UL L 216, 20.8.2009).

njihove razpoložljivosti. Poleg tega bo Komisija v tesnem sodelovanju z državami članicami predlagala vzpostavitev **večagencijskega mehanizma opozarjanja na področju varnosti prometa in dobavne verige**, da se zagotovi varna in pravočasna izmenjava ustreznih informacij, potrebnih za predvidevanje groženj in boj proti njim.

Poleg tega bo z izvajanjem akta o kritičnih surovinah in akta o neto ničelni industriji večja uporaba trajnostnih, odpornih in evropskih prednostnih meril pri javnih naročilih EU spodbujala razvoj vodilnih trgov. Okrepljene trgovinske vezi, na primer prek partnerstev za surovine ter partnerstev za čisto trgovino in naložbe, bodo prispevale k diverzifikaciji dobavnih verig.

Odpornost in pripravljenost na kemične, biološke, radiološke in jedrske grožnje

Ruska vojna agresija proti Ukrajini je povečala tveganje **kemičnih, bioloških, radioloških in jedrskih (KBRJ) groženj**. Da bi obravnavala morebitno nabavo in instrumentalizacijo KBRJ materialov, bo Komisija podpirala države članice in partnerske države z namenskim usposabljanjem in vajami. Komisija bo v okviru novega **akcijskega načrta za pripravljenost in odzivanje na KBRJ grožnje** okrepila tudi zmogljivosti za pripravljenost in odzivanje na področju KBRJ, in sicer s prednostno razvrstitvijo groženj, financiranjem inovacij za protiukrepe, zmogljivostmi rescEU in ustvarjanjem zalog medicinske opreme. Poleg tega bo **strategija EU za zdravstvene protiukrepe** podpirala razvoj zdravstvenih protiukrepov od raziskav do proizvodnje in distribucije za zaščito EU pred pandemijami in KBRJ grožnjami.

EU je na podlagi izkušenj s pandemijo COVID-19 okrepila okvir za zdravstveno varnost[59]. Komisija imenuje referenčne laboratorije EU na področju javnega zdravja, da bi okrepila zmogljivosti za nadzor in hitro odkrivanje na ravni EU in nacionalni ravni. Načrt Unije za pripravljenost, preprečevanje in odzivanje na področju zdravstvene varnosti bo objavljen leta 2025.

Ključni ukrepi

Komisija bo:

- **v letu 2025 pregledala in revidirala akt o kibernetski varnosti;**
- **razvila ukrepe za zagotavljanje kibernetske varnosti pri uporabi storitev v oblaku;**
- **v letu 2025 predlagala pristaniško strategijo EU;**
- **v letu 2026 revidirala pravila EU o javnem naročanju za obrambo in varnost;**
- **v letu 2026 predstavila nov akcijski načrt za pripravljenost in odzivanje na področju KBRJ.**

Komisija bo v sodelovanju z državami članicami:

- **razvila in uvedla evropsko infrastrukturo za kvantno komunikacijo (EuroQCI);**
- **zagotovila učinkovito izvrševanje akta o digitalnih storitvah;**
- **si prizadevala za boj proti instrumentalizaciji migracij;**
- **vzpostavila sistem za dogodke na področju varovanja v letalstvu;**
- **si prizadevala za vzpostavitev večagencijskega mehanizma opozarjanja na področju prometa in dobavne verige.**

Svet poziva, naj:

- **sprejme priporočilo Sveta o kibernetskem načrtu EU.**

Države članice se poziva, naj:

[59] Zlasti z Uredbo (EU) 2022/2371 o resnih čezmejnih grožnjah za zdravje.

- **v celoti prenesejo in izvajajo direktivo o odpornosti kritičnih subjektov ter direktivo o varnosti omrežij in informacijskih sistemov.**

5. Zategovanje zanke okoli hudih kaznivih dejanj in organiziranega kriminala

Pomagali bomo izkoreniniti organizirani kriminal, tako da bomo predlagali strožja pravila za boj proti organiziranim kriminalnim združbam, vključno s preiskavami, zmanjšali ranljivost mladih v EU za novačenje v kriminal ter okrepili ukrepe za prekinitev dostopa do orodij za kazniva dejanja in s kriminalom pridobljenega premoženja.

Organizirani kriminal izkorišča razvijajoče se okolje in se eksponentno širi. Izkorišča napredne tehnologije, deluje v več jurisdikcijah in ima močne povezave zunaj meja EU. Glede na te kompleksne nadnacionalne grožnje sta usklajevanje in podpora na ravni EU ključnega pomena.

Preprečevanje kriminala

Novačenje mladih v organizirani kriminal je v EU vse bolj zaskrbljujoč pojav. V boju proti organiziranemu kriminalu je treba obravnavati njegove **temeljne vzroke** z zagotavljanjem izobraževanja in alternativ kriminalnemu življenju z vsedružbenim pristopom. Komisija bo podprla vključevanje varnostnih vidikov v izobraževalne, socialne in regionalne politike EU ter v politike zaposlovanja EU. EU bo **spodbujala politike za preprečevanje kriminala**[60], ki temeljijo na dokazih in so prilagojene lokalnim razmeram.

Da bi zaščitili prejemnike spletnih storitev, zlasti mladoletnike, med drugim pred storilci spolnih zlorab otrok, trgovci z ljudmi in spletnim novačenjem za kazniva dejanja ali nasilni ekstremizem, ukrepi na podlagi **akta o digitalnih storitvah** od ponudnikov spletnih platform, dostopnih mladoletnikom, zahtevajo, da obvladujejo tveganja in ukrepajo v zvezi z nezakonitimi vsebinami, vključno s sovražnim govorom. Komisija namerava izdati **smernice o zaščiti mladoletnikov**, da bi ponudnikom spletnih platform pomagala pri zagotavljanju visoke ravni zasebnosti, varnosti in zaščite mladoletnikov na spletu. Smernice bodo vsebovale sklop priporočil za izboljšanje zaščite mladoletnikov na spletu za vse digitalne storitve, ki se izvajajo v Uniji. Komisija namerava leta 2025 omogočiti tudi rešitev EU za **preverjanje starosti, ki varuje zasebnost**, s katero bo zapolnila vrzel, preden bo konec leta 2026 na voljo evropska denarnica za digitalno identiteto. Komisija bo predstavila tudi akcijski načrt proti kibernetskemu ustrahovanju.

Poleg tega bo Komisija še naprej podpirala prostovoljno sodelovanje več deležnikov s spletnimi platformami in drugimi ustreznimi akterji, tudi prek internetnega foruma EU in ciljno usmerjenih kodeksov ravnanja na podlagi akta o digitalnih storitvah, kot je kodeks ravnanja za odpravo nezakonitega sovražnega govora na spletu v letu 2025. Cilj je povečati ozaveščenost, se skupaj odzvati na trenutne in nastajajoče grožnje ter pripraviti in izmenjevati dobre prakse za blažitvene ukrepe.

Na lokalni ravni vpliv organiziranega kriminala poudarja potrebo po regionalnih rešitvah za zmanjšanje ranljivosti in privlačnosti nezakonitih dejavnosti. Agenda EU za mesta bo obravnavala varnostne izzive v mestih na podlagi pobude Mesta v EU proti radikalizaciji. Komisija bo države članice podpirala pri krepitvi mestne in regionalne varnosti prek Evropskega sklada za regionalni razvoj.

Odporne in kohezivne družbe so podprte z močnejšimi izobraževalnimi temelji in spretnostmi. Unija si bo z **unijo spretnosti** ter **akcijskim načrtom za integracijo in vključevanje**

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

prizadevala pomagati ljudem, da postanejo odpornejši proti napačnim informacijam in dezinformacijam, radikalizaciji in novačenju v kriminal.

Zaščita otrok pred vsemi oblikami nasilja, vključno s kaznivimi dejanji, fizičnim ali psihičnim nasiljem, tako na spletu kot zunaj njega, je osrednji cilj EU. Za obravnavanje posebnih potreb posebej ranljivih skupin, kot so otroci, ki so vse bolj izpostavljeni novačenju in radikalizaciji, pridobivanju za spolne namene in spolni zlorabi, kibernetskemu ustrahovanju, dezinformacijam in drugim grožnjam, bo EU pripravila **akcijski načrt za zaščito otrok pred kriminalom**, ki bo vključeval spletno in nespletno razsežnost. V njem bo določen skladen in usklajen pristop, ki bo temeljil na razpoložljivih okvirih in orodjih, vključno s prihodnjim evropskim centrom za preprečevanje spolne zlorabe otrok in boj proti njej ter drugimi organi in agencijami EU, ter predlagani nadaljnji ukrepi na področjih, kjer ostajajo vrzeli.

Razbitje kriminalnih mrež in njihovih spodbujevalcev

Okrepiti je treba boj proti kriminalnim mrežam z visokim tveganjem, vodjem organiziranih kriminalnih združb in spodbujevalcem. Čeprav so nedavni uspehi opazni[61], zastarela pravila in nedosledne opredelitve kriminalnih mrež ovirajo učinkovit odziv kazenskega pravosodja in čezmejno sodelovanje. Komisija bo pregledala zastarelo zakonodajo na tem področju in predlagala prenovljen **pravni okvir za organizirani kriminal**, da bi okrepila odziv.

Upravno izvrševanje lahko dopolnjuje preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za hitrejše rezultate, kot sta pokazala Evropsko javno tožilstvo in Evropski urad za boj proti goljufijam (OLAF) pri obravnavanju **čezmejnih goljufij in kaznivih dejanj, ki škodijo finančnim interesom EU**. Osebe, ki goljufajo pri pridobivanju subvencij, se osredotočajo na sektorje, kot so energija iz obnovljivih virov, raziskovalni programi in kmetijstvo[62]. Komisija bo preučila načine za usklajevanje uporabe kazenskih in upravnih orodij ter okrepila sodelovanje z Europolom, Eurojustom in EJT. Komisija bo tudi še naprej podpirala širšo uporabo **upravnega pristopa** za opolnomočenje lokalnih in drugih upravnih organov za onemogočanje infiltracije kriminala[63].

EU si prizadeva za okrepitev svojega pravnega okvira za boj proti **korupciji**[64]. Evropski parlament in Svet bi morala hitro zaključiti pogajanja o posodobljenem protikorupcijskem okviru, ki ga je predlagala Komisija. Komisija bo predstavila protikorupcijsko strategijo EU za spodbujanje integritete in okrepitev usklajevanja med vsemi ustreznimi organi in deležniki na tem področju.

Strelno orožje je ključni dejavnik, ki omogoča vse več nasilja organiziranih kriminalnih združb. Komisija bo predlagala skupne kazenskopravne standarde za nedovoljeno trgovino s strelnim orožjem. Novi **akcijski načrt EU za boj proti nedovoljeni trgovini s strelnim orožjem** bo osredotočen na zaščito zakonitega trga, omejevanje kriminalnih dejavnosti na podlagi boljših obveščevalnih podatkov in krepitev mednarodnega sodelovanja s posebnim poudarkom na Ukrajini in Zahodnem Balkanu.

Za pirotehnične izdelke, s katerimi se nezakonito trguje in se uporabljajo pri kaznivih dejanjih, so potrebni ukrepi za izboljšanje preprečevanja in sledljivosti. Komisija trenutno ocenjuje

[61] Vključno z nedavnimi zadevami EMPACT.
[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] Predlog direktive Evropskega parlamenta in Sveta o boju proti korupciji, nadomestitvi Okvirnega sklepa Sveta 2003/568/PNZ in Konvencije o boju proti korupciji uradnikov Evropskih skupnosti ali uradnikov držav članic Evropske unije ter spremembi Direktive (EU) 2017/1371 Evropskega parlamenta in Sveta, COM(2023) 234 final, Bruselj, 3.5.2023.

direktivo o pirotehničnih izdelkih in bo razmislila tudi o **kazenskih sankcijah za nezakonito trgovino s pirotehničnimi izdelki**.

Sledenje denarju

Sledenje denarju je ključnega pomena v boju proti organiziranemu kriminalu in terorizmu, vendar ostaja zelo zahtevno. Povezava med organiziranim kriminalom in denarnimi tokovi zahteva intenzivna in skupna prizadevanja za zaustavitev dostopa kriminalnih mrež do virov financiranja ter boljšo zaščito ljudi, podjetij in javnih proračunov.

EU je okrepila svoja prizadevanja z novimi pravili za preprečevanje pranja denarja, vključno z ustanovitvijo organa **EU za preprečevanje pranja denarja (AMLA)**[65]. Sodelovanje med AMLA, uradom OLAF, EJT, Eurojustom in Europolom je bistveno za izvajanje učinkovitih finančnih preiskav. Komisija bo podprla sklepanje **partnerstev**, tako tistih, ki spodbujajo sodelovanje med agencijami, kot tistih, ki vključujejo zasebni sektor.

Za odpravo finančnih motivov v ozadju organiziranega kriminala je bistvenega pomena, da se zasežejo sredstva in odvzamejo premoženjske koristi, pridobljene s kaznivim dejanjem. Nedavno sprejeta strožja pravila o **povrnitvi in odvzemu premoženja**[66] bi države članice morale nemudoma prenesti v nacionalno zakonodajo in v celoti izkoristiti njihov potencial. Za boj proti vzporednim finančnim sistemom, ki se izogibajo okviru EU za preprečevanje pranja denarja, vključno s sistemi, ki temeljijo na kriptosredstvih, so potrebni tudi inovativni ukrepi, izmenjava najboljših praks med državami članicami ter večja podpora Europola in Eurojusta. Komisija bo preučila izvedljivost novega vseevropskega sistema za sledenje dobičkom iz organiziranega kriminala in financiranju terorizma ter spodbujala pravočasen in razširjen pretok informacij od **finančnoobveščevalnih enot** do organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Komisija bo preučila načine za zapolnitev vrzeli, podpirala države članice pri krepitvi zmogljivosti in si še naprej prizadevala za krepitev sodelovanja s tretjimi državami, ki jih storilci kaznivih dejanj zlorabljajo za dejavnosti podzemnega bančništva.

Boj proti hudim kaznivim dejanjem

Poleg razbijanja kriminalnih mrež so za boj proti hudim kaznivim dejanjem potrebna ciljno usmerjena prizadevanja. Za okrepitev naše sposobnosti za **boj proti spletnim goljufijam**, ki povzročajo zelo veliko finančno škodo[67], bo Komisija podprla preventivne ukrepe in učinkovitejše ukrepe za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter bo sodelovala z državami članicami in deležniki pri podpori in zaščiti žrtev, tudi s pomočjo pri povrnitvi njihovega premoženja. Ta prizadevanja bodo formalizirana v **akcijskem načrtu za boj proti spletnim goljufijam**.

Komisija bo na podlagi strategije EU za boj proti **spolni zlorabi otrok 2020–2025**[68] podprla sozakonodajalca pri dokončanju dveh zakonodajnih predlogov[69] za preprečevanje spolne zlorabe otrok na spletu in boj proti njej ter za izboljšanje učinkovitosti ukrepov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj zoper spolno zlorabo in izkoriščanje otrok. Ker začasna pravila veljajo do aprila 2026, je bistveno vzpostaviti stalni pravni okvir, Komisija pa spodbuja sozakonodajalca, naj začneta pogajanja o osnutku uredbe o določitvi pravil za preprečevanje spolne zlorabe otrok in boj proti njej. Sozakonodajalca sta tudi pozvana,

[65] https://www.amla.europa.eu/index_sl.
[66] Direktiva (EU) 2024/1260 Evropskega parlamenta in Sveta z dne 24. aprila 2024 o povrnitvi in odvzemu premoženja, UL L, 2024/1260, 2.5.2024.
[67] Global Anti-Scam Report 2024 (Svetovno poročilo o boju proti spletnim goljufijam za leto 2024).
[68] COM(2020) 607 final.
[69] COM(2022) 209 final in COM(2024) 60 final.

naj nadaljujeta z delom za pogajanja o direktivi o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter gradivu spolne zlorabe otrok, v kateri bodo določena minimalna pravila o opredelitvi kaznivih dejanj in sankcij na področju spolnega izkoriščanja otrok.

Polovica najnevarnejših kriminalnih mrež v EU je vpletena v nasilen **nedovoljen promet s prepovedanimi drogami**. Čeprav je EU nedavno okrepila boj proti tovrstnemu kriminalu[70], zlasti z razširitvijo pristojnosti **Agencije EU za droge**, so potrebni nadaljnji ukrepi. Komisija bo v tesnem sodelovanju z državami članicami predlagala novo **strategijo EU na področju drog**. Prav tako bo pregledala **pravni okvir o predhodnih sestavinah za prepovedane droge** in predlagala **akcijski načrt EU za boj proti nedovoljenemu prometu s prepovedanimi drogami**, da bi prekinila poti in poslovne modele. **Javno-zasebno partnerstvo zavezništva evropskih pristanišč** za okrepljeno zaščito pristanišč se bo razširilo na manjša pristanišča in pristanišča na celinskih vodah ter zagotovilo izvajanje pravil o pomorski varnosti. Komisija bo ob priznavanju resnih lokalnih učinkov nedovoljenega prometa s prepovedanimi drogami še naprej podpirala uravnoteženo, na dokazih temelječo in večdisciplinarno politiko na področju drog, ki bo pripravljena na nenaden pritok drog, zlasti sintetičnih opioidov.

Za boj proti izkoriščanju ljudi je EU sprejela nova pravila[71] in bo uvedla **prenovljeno strategijo EU za boj proti trgovini z ljudmi** (2026–2030), ki bo zajemala vse faze od preprečevanja do pregona s poudarkom na podpori žrtvam tako na ravni EU kot na mednarodni ravni.

V boju proti **tihotapljenju migrantov** bo Komisija v sodelovanju z Europolom, Eurojustom in Frontexom vodila prizadevanja s ključnimi partnerji prek novega svetovnega zavezništva za boj proti tihotapljenju migrantov, ki bo vključevalo tudi spletno razsežnost. Predloge Komisije o boju proti tihotapljenju[72] bi bilo treba nemudoma sprejeti in začeti izvajati. Poleg tega je Komisija po sprejetju **nabora orodij za prevoznike**[73] povečala stike s tujimi organi in prevozniki ter bo še naprej sodelovala z letalsko industrijo in organizacijami civilnega letalstva[74], da bi povečala ozaveščenost o tihotapljenju migrantov po zraku[75].

Okoljska kriminaliteta dolgoročno ogroža okolje, javno zdravje in gospodarstvo. Komisija bo podpirala države članice pri izvajanju direktive o okoljski kriminaliteti[76] ter okrepila operativne mreže in ukrepe na tem področju[77]. Dosledno izvrševanje je bistvenega pomena. Poleg tega bo nedavno sprejeta Konvencija Sveta Evrope o kazenskopravni zaščiti okolja[78] pomagala zagotoviti močna in primerljiva prizadevanja za boj proti okoljski kriminaliteti tako v Evropi kot zunaj nje.

Odziv kazenskega pravosodja

Kriminal in terorizem lahko vplivata na vse, zato je bistveno podpirati in varovati pravice **žrtev**, da se zmanjša škoda ter poveča splošna varnost in zaupanje v organe. Komisija bo na podlagi direktive o pravicah žrtev uvedla novo **strategijo EU o pravicah žrtev**.

[70] COM(2023) 641 final.
[71] Direktiva (EU) 2024/1712 z dne 13. junija 2024 o spremembi Direktive 2011/36/EU o preprečevanju trgovine z ljudmi in boju proti njej ter zaščiti njenih žrtev, UL L, 2024/1712, 24.6.2024.
[72] COM(2023) 755 final in COM(2023) 754 final.
[73] Nabor orodij za obravnavo uporabe komercialnih prevoznih sredstev za olajšanje nedovoljenih migracij v EU.
[74] Vključno z Mednarodno organizacijo civilnega letalstva (ICAO).
[75] Komisija bo podprla tudi dokončanje uredbe o ukrepih zoper prevoznike, ki omogočajo trgovino z ljudmi ali tihotapljenje migrantov v povezavi z nezakonitim vstopom na ozemlje Evropske unije ali pri tem sodelujejo, COM(2021) 753 final.
[76] Direktiva (EU) 2024/1203 Evropskega parlamenta in Sveta z dne 11. aprila 2024 o kazenskopravnem varstvu okolja, UL L, 2024/1203, 30.4.2024.
[77] Mreža Evropske unije za izvajanje in uveljavljanje okoljskega prava (IMPEL), Evropska mreža tožilcev za okolje (ENPE), EnviCrimeNet in Forum sodnikov Evropske unije za okolje (EUFJE).
[78] Odbor strokovnjakov za kazenskopravno zaščito okolja (PC-ENV) – Evropski odbor za vprašanja kriminalitete.

Kazenskopravni sistemi EU potrebujejo učinkovita orodja za obravnavanje nastajajočih groženj. Da bi to dosegla, je Komisija ustanovila **forum na visoki ravni o prihodnosti kazenskega pravosodja EU**. Ta forum združuje države članice, Evropski parlament, agencije in organe EU ter druge ustrezne deležnike. Njegov cilj je omogočiti razprave o načinih za zagotovitev, da naši kazenskopravni sistemi ostanejo učinkoviti, pravični in odporni ob spreminjajočih se izzivih, hkrati pa okrepiti pravosodno sodelovanje in medsebojno zaupanje, tudi z digitalizacijo[79].

Ključni ukrepi

Komisija bo:

- **v letu 2026 predstavila zakonodajni predlog za posodobljena pravila o organiziranem kriminalu;**
- **v letu 2025 predstavila zakonodajni predlog za revizijo pravnega okvira o predhodnih sestavinah za prepovedane droge;**
- **v letu 2025 predstavila zakonodajni predlog za skupne kazenskopravne standarde za nedovoljeno trgovino s strelnim orožjem;**
- **ocenila potrebo po reviziji direktiv o pirotehniki in eksplozivih za civilno uporabo;**
- **ocenila potrebo po nadaljnji krepitvi evropskega preiskovalnega naloga in evropskega naloga za prijetje;**
- **v letu 2026 predstavila novo strategijo EU za boj proti trgovini z ljudmi;**
- **v letu 2026 predstavila novo strategijo EU o pravicah žrtev;**
- **do leta 2027 predstavila akcijski načrt EU za zaščito otrok pred kriminalom;**
- **v letu 2025 predstavila akcijski načrt EU za boj proti nedovoljenemu prometu s prepovedanimi drogami;**
- **v letu 2026 predstavila akcijski načrt EU glede trgovine s strelnim orožjem;**
- **od leta 2025 naprej eno za drugim razširila zavezništvo evropskih pristanišč;**
- **v letu 2026 sprejela smernice akta o digitalnih storitvah o zaščiti mladoletnikov;**
- **v letu 2026 predstavila akcijski načrt EU za boj proti kibernetskemu nadlegovanju.**

Države članice se poziva, naj:

- **do konca leta 2026 v celoti prenesejo nova pravila o povrnitvi in odvzemu premoženja ter jih v celoti izvajajo;**
- **izvajajo upravni pristop v boju proti infiltraciji kriminala;**
- **vzpostavijo javno-zasebna partnerstva za boj proti pranju denarja;**
- **prenesejo in v celoti izvajajo direktivo o preprečevanju nasilja nad ženskami in nasilja v družini ter boju proti njima.**

Evropski parlament in Svet sta pozvana, naj:

- **nadaljujeta z delom za pogajanja o uredbi o določitvi pravil za preprečevanje spolne zlorabe otrok in boj proti njej ter direktivi o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter gradivu spolne zlorabe otrok;**
- **zaključita pogajanja o direktivi o boju proti korupciji.**

[79] Zlasti z vzpostavitvijo sistema za obveščanje v okviru e-pravosodja prek spletne izmenjave podatkov (eCODEX) in evropskega informacijskega sistema kazenskih evidenc – državljani tretjih držav (ECRIS-TCN).

6. Boj proti terorizmu in nasilnemu ekstremizmu

Uvedli bomo celovito agendo za boj proti terorizmu za preprečevanje radikalizacije, varovanje spletnih in javnih prostorov ter odzivanje na izvršene napade.

Stopnja teroristične ogroženosti v EU ostaja visoka. Tesno je povezana z vplivi prelivanja geopolitičnih dogodkov, novih tehnologij in novih načinov financiranja terorizma. Zagotoviti moramo, da bo EU dobro opremljena za napovedovanje groženj, preprečevanje radikalizacije (na spletu in zunaj njega), zaščito državljanov in javnih prostorov pred napadi ter učinkovito odzivanje na napade, ko se zgodijo. Leta 2025 bo predstavljena **nova agenda EU za preprečevanje terorizma in nasilnega ekstremizma ter boj proti njima**, v kateri bodo določeni prihodnji ukrepi EU. V skladu z novo agendo bosta EU in Zahodni Balkan v letu 2025 podpisala novi **skupni akcijski načrt** za preprečevanje terorizma in nasilnega ekstremizma ter boj proti njima.

Preprečevanje radikalizacije in zaščita ljudi na spletu

Podobno kot boj proti organiziranemu kriminalu se tudi boj proti terorizmu in nasilnemu ekstremizmu začne z **odpravljanjem njunih temeljnih vzrokov**. **Vozlišče znanja EU o preprečevanju radikalizacije** bo okrepilo podporo strokovnim delavcem in oblikovalcem politik z novim **celovitim naborom orodij za preprečevanje**, ki bo omogočil zgodnje prepoznavanje in ukrepanje, osredotočeno na ranljive posameznike, zlasti mladoletnike. Radikalizacija se pogosto pojavlja v zaporih, zato bo Komisija izdala nova priporočila za podporo državam članicam pri reševanju te težave.

Teroristični in nasilni skrajneži uporabljajo spletne platforme za širjenje terorističnih in škodljivih vsebin, zbiranje sredstev in novačenje. Ranljivi uporabniki, zlasti mladoletniki, se na spletu radikalizirajo z zaskrbljujočo hitrostjo. **Uredba o terorističnih spletnih vsebinah** je bila ključna v boju proti širjenju terorističnih vsebin na spletu, saj je omogočila hitro odstranitev najbolj sprevrženega in najnevarnejšega gradiva[80]. Komisija trenutno ocenjuje njeno delovanje in bo ocenila, kako najbolje okrepiti ta okvir.

Krizni protokol EU za skupen in hiter odziv organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter tehnološke industrije na teroristične napade bo spremenjen, da se zagotovita nadgradljivost in prožnost pri odzivanju na vse večjo spletno razsežnost terorističnih napadov. Internetni forum EU bo še naprej glavna pot za prostovoljno sodelovanje s tehnološko industrijo v boju proti terorističnim in škodljivim spletnim vsebinam. Poleg tega Komisija sodeluje v mednarodnih pobudah, kot sta fundacija Christchurch Call in Svetovni internetni forum za boj proti terorizmu (GIFCT).

Boj proti financiranju terorizma

Teroristi financirajo svoje dejavnosti s kampanjami množičnega financiranja, kriptosredstvi, neobankami ali spletnimi plačilnimi platformami. Organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj morajo odkrivati in preiskovati te finančne tokove. Za to so potrebna sredstva, orodja in strokovno znanje. Ključno vlogo ima **mreža finančnih preiskovalcev za boj proti terorizmu**. Komisija bo preučila vzpostavitev **novega vseevropskega sistema za sledenje financiranju terorizma**, ki bi zajemal transakcije znotraj EU in SEPA, prenose kriptosredstev ter spletna in elektronska plačila ter dopolnjeval sporazum o programu za sledenje financiranja terorističnih dejavnosti (TFTP) med EU in ZDA.

[80] Do 31. decembra 2024 je bilo izdanih 1 426 odredb o odstranitvi za odstranitev terorističnih vsebin ali blokiranje dostopa do njih, od katerih je velika večina usmerjena proti džihadističnim terorističnim vsebinam, pa tudi desničarskim terorističnim vsebinam.

Proračun EU je treba **zaščititi pred zlorabo za spodbujanje radikalnih/ekstremističnih stališč** v državah članicah. Revidirana **finančna uredba** zdaj vključuje obsodbo za „spodbujanje k diskriminaciji, sovraštvu ali nasilju“ kot razlog za izključitev iz financiranja EU. Komisija bo še naprej preučevala najboljši način za polno uporabo nabora orodij, tudi pri izbiri potencialnih upravičencev. Zaščita proračuna EU je odvisna tudi od tesnega sodelovanja in izmenjave informacij z nacionalnimi organi, agencijami in organi EU.

Zaščita pred napadi

Poleg naložb v preprečevanje radikalizacije je pomemben element zaščite državljanov omejevanje sredstev, s katerimi lahko teroristi in storilci kaznivih dejanj izvedejo napade. Ukrepati je treba tako v zvezi z orodji, ki jih teroristi uporabljajo, kot tudi za zaščito tarč, ki jim grozi napad.

Komisija bo poleg ukrepov v zvezi s strelnim orožjem **pregledala tudi pravila** o **predhodnih sestavinah za eksplozive**, da bi vključila kemikalije z visokim tveganjem. **Javni prostori** so še vedno najpogostejša tarča terorističnih napadov, zlasti za storilce, ki delujejo sami. Za zaščito državljanov pred nevarnostmi bo **svetovalni program EU za varnost in zaščito** okrepljen, da se na zahtevo držav članic izvedejo ocene ranljivosti javnih prostorov, kritične infrastrukture in dogodkov z visokim tveganjem, financira pa se iz proračuna EU v okviru Sklada za notranjo varnost. EU si bo prizadevala povečati razpoložljiva sredstva za varovanju javnih prostorov. Komisija organom držav članic in zasebnim subjektom zagotavlja podporo z namenskimi smernicami in orodji, kot je vozlišče znanja o varovanju javnih prostorov[81], 70 milijonov EUR pa je že na voljo za podporo varovanju javnih prostorov od leta 2020.

Komisija bo preučila tudi uvedbo zahtev za organizacije, da razmislijo o varnostnih ukrepih na javno dostopnih mestih ali jih uvedejo, in sicer s sodelovanjem z lokalnimi organi in zasebnimi partnerji.

Glede na očitne ranljivosti bo **strategija EU za boj proti antisemitizmu in negovanje judovskega življenja (2021–2030)** še naprej usmerjala ukrepe Komisije za zaščito judovske skupnosti. Komisija bo prav tako zagotovila, da bodo na voljo ustrezna orodja za podporo državam članicam v boju **proti sovraštvu do muslimanov**.

Uporaba **dronov** za vohunjenje in napade predstavlja vse večji varnostni izziv. Komisija bo razvila **usklajeno metodologijo preskušanja za protidronske sisteme**, vzpostavila **protidronski center odličnosti** ter ocenila potrebo po uskladitvi zakonov in postopkov držav članic[82].

Tuji teroristični bojevniki

Za identifikacijo tujih terorističnih bojevnikov, ki se vračajo ali vstopajo prek zunanjih meja EU, so potrebni podatki o posameznikih, ki predstavljajo teroristično grožnjo. V ta namen bo Komisija skupaj z Europolom okrepila **sodelovanje s ključnimi tretjimi državami, da bi pridobila biografske in biometrične podatke o posameznikih, ki bi lahko predstavljali teroristično grožnjo**, vključno s tujimi terorističnimi bojevniki, ki jih je nato mogoče vnesti v schengenski informacijski sistem v skladu z veljavnimi pravnimi okviri EU in nacionalnimi pravnimi okviri. Zato je ključnega pomena, da države članice uporabljajo vsa obstoječa orodja. To vključuje vnos vseh ustreznih informacij v **SIS**, izboljšanje biometričnih preverjanj in izvajanje obveznih sistematičnih preverjanj vseh oseb na zunanjih mejah EU[83]. Poleg tega bodo **skupni kazalniki tveganja**, ki jih je razvila agencija Frontex, še naprej podpirali organe držav

[81] Vozlišče znanja o varovanju javnih prostorov.
[82] Na podlagi sklopa ključnih ukrepov iz sporočila o preprečevanju morebitnih groženj zaradi dronov iz leta 2023, COM(2023) 659 final.
[83] Popolnoma v skladu z zakonikom o schengenskih mejah in uredbo o preverjanju.

članic za nadzor meje pri prepoznavanju in ocenjevanju tveganja sumljivih potovanj morebitnih tujih terorističnih bojevnikov.

Da bi zagotovili, da bodo države članice ohranile dostop do **dokazov z bojišč**, ki jih je zbrala preiskovalna enota ZN za spodbujanje prevzemanja odgovornosti za kazniva dejanja, ki jih je zagrešil Daiš/ISIL (UNITAD), za pregon tujih terorističnih borcev, bo Komisija skupaj z Eurojustom ocenila možnost shranjevanja teh dokazov v Eurojustovi zbirki podatkov o dokazih o najhujših mednarodnih kaznivih dejanjih. Poleg tega bo nova evropska **pravosodna protiteroristična evidenca** še naprej podpirala pravosodne organe držav članic pri hitrem odkrivanju čezmejnih povezav v primerih terorizma.

Ključni ukrepi

Komisija bo:

- **v letu 2025 sprejela novo agendo EU za preprečevanje terorizma in nasilnega ekstremizma ter boj proti njima;**
- **v letu 2025 z državami Zahodnega Balkana podpisala nov skupni akcijski načrt za preprečevanje terorizma in nasilnega ekstremizma ter boj proti njima;**
- **v sodelovanju z vozliščem znanja EU razvila nov celovit nabor orodij za preprečevanje;**
- **v letu 2026 ocenila izvajanje uredbe o terorističnih spletnih vsebinah;**
- **v letu 2025 spremenila krizni protokol EU;**
- **v letu 2026 predstavila zakonodajni predlog za revizijo uredbe o trženju in uporabi predhodnih sestavin za eksplozive;**
- **preučila izvedljivost novega vseevropskega sistema za sledenje financiranju terorizma.**

Države članice se poziva, naj:

- **okrepijo biometrična preverjanja in izvajajo obvezna sistematična preverjanja na zunanjih mejah EU;**
- **v celoti uporabljajo evropsko pravosodno protiteroristično evidenco.**

7. EU kot močna svetovna akterka na področju varnosti

Da bi izboljšali varnost EU, bomo okrepili operativno sodelovanje prek partnerstev s ključnimi regijami, kot so partnerice v okviru širitvene politike in sosedske politike, Latinska Amerika in sredozemska regija. Varnostni interesi EU se bodo upoštevali pri mednarodnem sodelovanju, tudi z uporabo orodij in instrumentov EU.

V zadnjih letih so se pokazale neločljive povezave med zunanjo in notranjo varnostjo EU. Ruska vojna agresija proti Ukrajini, konflikt v Gazi, razmere v Siriji in nastajajoči konflikti po svetu so imeli resne učinke prelivanja na notranjo varnost EU. Da bi preprečila vpliv svetovne nestabilnosti na svojo notranjo varnost, **mora EU dejavno braniti svoje varnostne interese** z obravnavanjem zunanjih groženj, prekinitvijo tihotapskih poti in varovanjem koridorjev strateškega interesa, kot so trgovinske poti. Hkrati bo EU še naprej močna zaveznica partnerskih držav, s čimer bo sodelovala pri krepitvi svetovne varnosti in izgradnji vzajemne odpornosti proti grožnjam.

EU je v zadnjih letih sprejela pomembne ukrepe za okrepitev sodelovanja na področju varnosti. S partnerskimi državami je sklenila sporazume o operativnem sodelovanju na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodja in druge

vrste dogovorov. Dejavno si prizadeva za dodatne mednarodne sporazume v skladu s pogajalskimi smernicami Sveta in pobude za krepitev zmogljivosti, ki jih podpirajo agencije in organi EU. NDICI – Globalna Evropa je ključnega pomena tudi za krepitev varnosti s partnerskimi državami.

Na pravilih temelječ mednarodni red je temelj za krepitev svetovne varnosti. Varnostni dialogi, vključno s tematskimi, so ključnega pomena za okrepitev teh prizadevanj. Izvajanje **strateškega kompasa za varnost in obrambo** je skupaj z dvostranskimi in večstranskimi okviri sodelovanja, kot so stabilizacijsko-pridružitveni sporazumi in pridružitveni sporazumi, ter sodelovanjem z organizacijami, kot sta ZN in NATO, ključnega pomena za razvoj učinkovitih varnostnih rešitev. EU bo še naprej sodelovala v večstranskih forumih[84] ter bo okrepila sodelovanje z ustreznimi mednarodnimi in regionalnimi organizacijami in okviri, vključno z Natom, Združenimi narodi, Svetom Evrope, Interpolom, G7, OVSE in civilno družbo.

Regionalno sodelovanje

Nadaljevanje neomajne podpore EU **Ukrajini** ter krepitev varnosti in odpornosti **držav širitve EU** je nujna prednostna naloga s političnega in geostrateškega vidika. Podpora varnosti EU bi morala biti tesno povezana s **pospešenim vključevanjem držav kandidatk** v **varnostno strukturo EU**, vzporedno s krepitvijo njihovega regionalnega sodelovanja. Komisija bo uporabila širitveno politiko EU, da bi podprla zmogljivosti držav kandidatk in potencialnih kandidatk EU za odzivanje na grožnje, povečala operativno sodelovanje in izmenjavo informacij ter zagotovila usklajenost z načeli, zakonodajo in orodji EU. Instrument za predpristopno pomoč (IPA III) ter instrumenti za Ukrajino, Moldavijo in Zahodni Balkan so ključni za krepitev varnosti v državah kandidatkah in potencialnih kandidatkah.

EU bo v varnostno strukturo EU vključila tudi **partnerice v okviru sosedske politike**. Unija si bo z **novim paktom za Sredozemlje** in prihodnjim **strateškim pristopom k Črnemu morju** prizadevala za nadaljnje vzpostavljanje regionalnega sodelovanja in dvostranskih celovitih strateških partnerstev z varnostno razsežnostjo, kadar je ustrezno, z rednimi dialogi na visoki ravni o varnosti. Okrepilo se bo operativno sodelovanje s Severno Afriko, **Bližnjim vzhodom in Zalivom,** predvsem v boju proti terorizmu, pranju denarja, nedovoljeni trgovini s strelnim orožjem, proizvodnji prepovedanih drog in trgovini z njimi, zlasti captagona**.**

EU bo okrepila podporo Afriški uniji, regionalnim gospodarskim skupnostim in državam v regiji, da bi obravnavala porast terorističnih in kriminalnih dejavnosti ter njihove morebitne učinke prelivanja v **podsaharski Afriki, zlasti Sahelu, Afriškem rogu in Zahodni Afriki.** EU bo v skladu s strategijo EU za pomorsko varnost[85] okrepila sodelovanje v **Gvinejskem zalivu, Rdečem morju in Indijskem oceanu** za boj proti nezakoniti trgovini in piratstvu, in sicer s podpiranjem sodelovanja znotraj Afrike in regionalnega sodelovanja ter s podporo koordinirane prisotnosti EU na morju in Pomorskega analitičnega in operacijskega centra za narkotike (MAOC-N).

EU bo z **Latinsko Ameriko in Karibi** okrepila operativno sodelovanje za razbitje in pregon kriminalnih mrež z visokim tveganjem ter prekinitev nezakonitih dejavnosti in tihotapskih poti, pri čemer bo okrepila okvire sodelovanja, kot sta EU-CLASI (Odbor Latinske Amerike za notranjo varnost) ter mehanizem za usklajevanje in sodelovanje na področju boja proti drogam (EU-CELAC). Med prednostnimi nalogami bodo odpornost logističnih vozlišč, partnerstva in

[84] Globalni forum za boj proti terorizmu, svetovna koalicija za boj proti Daišu, Svetovni internetni forum za boj proti terorizmu (GIFCT), fundacija Christchurch Call, svetovna koalicija za obravnavanje nevarnosti sintetičnih drog.
[85] JOIN(2023) 8 final.

pristop sledenja denarju. EU bo še naprej podpirala razvoj policijske skupnosti Amerik (AMERIPOL), da bi ta postala regionalni ekvivalent Europola in okrepila pravosodno sodelovanje med državami članicami in regijo. EU bo sodelovala tudi z **Južno in srednjo Azijo** pri skupnih varnostnih izzivih, povezanih s terorizmom, trgovino z nedovoljenim blagom, vključno s prepovedanimi drogami, trgovino z ljudmi in tihotapljenjem migrantov.

Poleg tega bo EU podpirala okvire regionalnega sodelovanja v tretjih državah, da bi jim dodatno pomagala pri preprečevanju nedovoljene trgovine pri viru v skladu z načelom deljene odgovornosti za celotno kriminalno dobavno verigo. Poleg tega bo EU prispevala h krepitvi varnosti logističnih vozlišč v tujini z usklajevanjem **skupnih inšpekcijskih pregledov v pristaniščih tretjih držav**.

Operativno sodelovanje

Strategija **Global Gateway** bo podpirala trajnostne in visokokakovostne infrastrukturne projekte v digitalnem, podnebnem in energetskem, prometnem, zdravstvenem, izobraževalnem in raziskovalnem sektorju. Komisija bo varnostne vidike sedaj po potrebi vključila v prihodnje naložbe strategije Global Gateway. To bo vključevalo pobude, ki so ključne za strateško avtonomijo EU in njenih partnerskih držav, kot so infrastrukturni projekti, ki vključujejo varnostne ocene in ukrepe za blaženje tveganja.

Komisija si bo prizadevala za nadaljnje **sporazume med EU in tretjimi državami o sodelovanju z Europolom in Eurojustom**, zlasti z državami Latinske Amerike.

Poleg tega je proaktivna udeležba držav, ki niso članice EU, v **EMPACT** eden najučinkovitejših načinov za krepitev operativnega sodelovanja. EU bo še naprej spodbujala vključevanje tretjih držav, zlasti Zahodnega Balkana, vzhodnega sosedstva, podsaharske Afrike, Severne Afrike, Bližnjega vzhoda, Latinske Amerike in Karibov, v okvir. Drugo orodje za okrepitev sodelovanja s tretjimi državami na področju boja proti kriminalu so operativne projektne skupine med državami članicami, ki jih koordinira Europol, kadar lahko v njih sodelujejo tretje države. Komisija namerava tudi zaključiti pogajanja o mednarodnem sporazumu med **EU in Interpolom**[86], da bi zagotovila enotnejši pristop k svetovnim varnostnim grožnjam in boju proti mednarodnim kaznivim dejanjem.

Unija mora biti prisotna na terenu v okviru pristopa Ekipe Evropa. Strokovno osebje Unije in držav članic ima ključno vlogo pri zagotavljanju, da je zunanje delovanje Unije dobro informirano, usklajeno in odzivno. Da bi ta pristop dvignili na naslednjo raven, bo Komisija ob podpori visokega predstavnika za zunanje zadeve in varnostno politiko okrepila **mreže za zvezo** in olajšala napotitev regionalnih **uradnikov za zvezo Europola in Eurojusta** v skladu z operativnimi potrebami držav članic.

EU si bo prizadevala za tesnejše operativno sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodja, spodbujala izmenjavo informacij v realnem času in skupne operacije prek **skupnih preiskovalnih skupin** v tretjih državah ob podpori Europola in Eurojusta. Komisija bo države članice podpirala tudi pri vzpostavitvi **skupnih zbirnih centrov**, ki bodo združevali strokovnjake in lokalne organe za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v strateških tretjih državah.

Orodja skupne zunanje in varnostne politike (SZVP)

Misije skupne varnostne in obrambne politike (SVOP) se bodo prav tako v celoti izkoristile za boljše prepoznavanje in obravnavanje zunanjih groženj notranji varnosti EU v skladu z njihovimi mandati, ki jih je določil Svet. Za krepitev zmogljivosti tretjih držav bosta visoki

[86] Sklep Sveta (EU) 2021/1312 z dne 19. julija 2021 in Sklep Sveta (EU) 2021/1313 z dne 19. julija 2021.

predstavnik za zunanje zadeve in varnostno politiko ter Komisija podprla ukrepe SVOP z namenskimi instrumenti financiranja in preučila vse ustrezne možnosti financiranja.

Omejevalni ukrepi EU so uveljavljeno orodje SZVP, ki se uporablja tudi za boj proti terorizmu. Svet bi lahko na podlagi predlogov visokega predstavnika za zunanje zadeve in varnostno politiko, držav članic ali Komisije ocenil, kako bi lahko obstoječi avtonomni omejevalni ukrepi EU (seznam EU za področje terorizma) postali učinkovitejši, bolj operativni in prilagodljivi. Poleg tega bi lahko preučili dodatne omejevalne ukrepe proti kriminalnim mrežam v skladu s cilji SZVP.

Vizumska politika in izmenjava informacij

Vizumska politika EU je ključno orodje za sodelovanje s tretjimi državami in varovanje naših meja z nadzorom vstopa v EU in določanjem pogojev zanj. Komisija bo **varnostne vidike** v celoti vključila **v vizumsko politiko EU** v okviru prihodnje strategije za vizumsko politiko EU. Komisija bo sodelovala s sozakonodajalcema pri sprejetju predloga za revizijo in racionalizacijo mehanizma za zadržanje izvzetja iz vizumske obveznosti, zlasti v posebnih primerih zlorabe brezvizumskega režima[87]. Tretje države bodo spodbujene k izmenjavi informacij o posameznikih, ki bi lahko pomenili varnostne grožnje, ki bodo vnesene v informacijske sisteme in podatkovne zbirke EU.

Da bi dosegla usklajevanje politike in že prej ukrepala za preprečevanje ter omogočila učinkovitejše, hitrejše in nemoteno sodelovanje, si bo Komisija prizadevala za vzpostavitev **ureditev pretoka podatkov** in preučila načine za **izboljšanje izmenjave informacij** za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter upravljanja meja z zaupanja vrednimi tretjimi državami v skladu s temeljnimi pravicami in pravili o varstvu podatkov.

Ključni ukrepi

Komisija bo:

- **sklenila mednarodne sporazume med EU in prednostnimi tretjimi državami o sodelovanju z Europolom in Eurojustom;**
- **spodbujala sodelovanje partnerskih držav v EMPACT za boj proti organiziranemu kriminalu in terorizmu;**
- **podpirala agencije in organe EU pri vzpostavljanju in krepitvi delovnih dogovorov s partnerskimi državami;**
- **nadaljnje upoštevala varnostne vidike v vizumski politiki EU v prihodnji vizumski strategiji;**
- **krepila izmenjave informacij z zaupanja vrednimi tretjimi državami za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter upravljanja meja.**

Komisija bo v sodelovanju z visokim predstavnikom za zunanje zadeve:

- **v celoti izkoristila civilne misije skupne varnostne in obrambne politike (SVOP);**
- **usklajevala skupne inšpekcijske preglede v pristaniščih tretjih držav do leta 2027.**

Komisija bo v sodelovanju z visokim predstavnikom za zunanje zadeve in državami članicami:

- **okrepila povezovalne mreže in sodelovanja v okviru pristopa Ekipe Evropa;**
- **vzpostavila skupne operativne skupine in zbirne centre v tretjih državah od leta 2025 naprej.**

[87] COM(2023) 642.

Evropski parlament in Svet sta pozvana, naj:

- **zaključita pogajanja o reviziji mehanizma zadržanja izvzetja iz vizumske obveznosti.**

8. Zaključek

V svetu negotovosti je treba okrepiti zmogljivost Unije za napovedovanje in preprečevanje varnostnih groženj ter odzivanje nanje.

Ni dovolj, da se na krize odzovemo le takrat, ko se pojavijo. Okrepiti moramo svojo ozaveščenost s celovito sliko o grožnjah, kot se razvijajo. Poleg tega moramo zagotoviti, da bodo naša orodja in zmogljivosti ustrezali tej nalogi.

Celovit sklop ukrepov, podrobno opisanih v tej strategiji, bo pomagal ustvariti močnejšo Unijo v svetu: Unijo, ki je sposobna napovedati, načrtovati in zadovoljiti lastne varnostne potrebe, da se lahko učinkovito odzove na grožnje notranji varnosti in zahteva, da storilci odgovarjajo za svoja dejanja, ter varuje svoje odprte, svobodne in uspešne družbe in demokracije.

Zato moramo spremeniti našo miselnost glede notranje varnosti. Prizadevali si bomo za spodbujanje nove varnostne kulture EU, pri kateri se varnostni vidiki upoštevajo v vsej naši zakonodaji, politikah in programih – od zasnove do izvajanja. In kjer nam sodelovanje med področji politike omogoča, da postavimo nove temelje.

To ni naloga ene same institucije, vlade ali akterja. To je skupna naloga Evrope.