Rada
Európskej únie

V Bruseli 3. apríla 2025
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	2. apríla 2025
Komu:	Thérèse BLANCHETOVÁ, generálna tajomníčka Rady Európskej únie
Č. dok. Kom.:	COM(2025) 148 final
Predmet:	OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV ProtectEU: európska stratégia vnútornej bezpečnosti

Delegáciám v prílohe zasielame dokument COM(2025) 148 final.

Príloha: COM(2025) 148 final

EURÓPSKA
KOMISIA

V Štrasburgu 1. 4. 2025
COM(2025) 148 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV

ProtectEU: európska stratégia vnútornej bezpečnosti

1. ProtectEU: európska stratégia vnútornej bezpečnosti

Bezpečnosť je základom, na ktorom stoja všetky naše slobody. Demokracia, právny štát, základné práva, blahobyt Európanov, konkurencieschopnosť a prosperita – to všetko závisí od našej schopnosti zaistiť základnú bezpečnosť. Aby mohli členské štáty EÚ zaručiť bezpečnosť svojich občanov v novej ére bezpečnostných hrozieb, v ktorej v súčasnosti žijeme, je viac ako kedykoľvek predtým potrebné zaujať k **ochrane našej vnútornej bezpečnosti jednotný európsky prístup**. Európa musí v meniacom sa geopolitickom prostredí naďalej plniť svoj trvalý prísľub mieru.

Prvé kroky smerom k vybudovaniu európskeho bezpečnostného aparátu už boli prijaté. V poslednom desaťročí sme sa postarali o to, aby v Únii fungovali lepšie kolektívne mechanizmy prijímania opatrení v oblasti presadzovania práva a justičnej spolupráce, bezpečnosti hraníc, boja proti závažnej a organizovanej trestnej činnosti, boja proti terorizmu a násilnému extrémizmu a ochrany fyzickej a digitálnej kritickej infraštruktúry EÚ. Zásadný význam má aj naďalej riadne vykonávanie už prijatých právnych predpisov a vypracovaných politík.

Povaha súčasných hrozieb a vnútorné prepojenie medzi vnútornou a vonkajšou bezpečnosťou EÚ si vyžadujú ďalšie kroky.

Rozsah hrozieb je široký. Hranice medzi **hybridnými hrozbami** a otvorenou vojnou sa stali nejasnými. Rusko vedie online a offline hybridnú kampaň proti EÚ a jej partnerom s cieľom narušiť a oslabiť spoločenskú súdržnosť a demokratické procesy a otestovať solidaritu EÚ s Ukrajinou. Nepriateľské zahraničné štáty a nimi podporované subjekty sa snažia infiltrovať do našej kritickej infraštruktúry a dodávateľských reťazcov a narušiť ich, hľadajú spôsoby, ako ukradnúť citlivé údaje a zaistiť si pozíciu, ktorá im umožní výrazne narušiť naše fungovanie v budúcnosti. Trestnú činnosť využívajú ako službu a páchateľov trestnej činnosti ako prostredníkov. Našu zraniteľnosť voči hybridným kampaniam nepriateľských štátov navyše zvyšuje naša závislosť od dodávok z tretích krajín.

Ako sa zdôrazňuje v Hodnotení hrozieb závažnej a organizovanej trestnej činnosti v EÚ (SOCTA), ktoré nedávno predložil Europol, v Európe sa rozrastajú silné **siete organizovanej trestnej činnosti**, ktoré sa šíria online, prenikajú do nášho hospodárstva a ovplyvňujú našu spoločnosť[1]. Keď sa v spoločenstve alebo v hospodárskom sektore uchytí organizovaná trestná činnosť, jej odstránenie sa stáva namáhavým bojom: tretina najnebezpečnejších zločineckých sietí pôsobí už viac ako desať rokov. Kryptomeny a paralelné finančné systémy im pomáhajú prať a skrývať príjmy z trestnej činnosti.

Hrozba teroristických útokov v Európe naďalej pretrváva. Regionálne krízy mimo EÚ vytvárajú reťazovú reakciu a podnecujú teroristov s rôznym ideologickým presvedčením, aby rozširovali, mobilizovali či budovali svoje kapacity. Svoje snahy o radikalizáciu a nábor zameriavajú najmä na najzraniteľnejšie skupiny našich spoločností, a to predovšetkým na určitých mladých ľudí. Podnecujú útoky osamelých aktérov a sú dôvodom prudkého nárastu protisystémového extrémizmu, ktorého cieľom je narušiť demokratický právny poriadok.

Rýchlo sa vyvíjajúci **technologický pokrok** zabezpečuje základné nástroje na posilnenie nášho bezpečnostného aparátu. Čoraz častejšie však dochádza ku kybernetickým útokom a zahraničnej manipulácii s informáciami, pri ktorých sa využívajú nové technológie, ako je umelá inteligencia. Online priestor nesie v sebe riziká najmä pre deti, mladých a starších ľudí. Šírenie nenávisti na internete zároveň ohrozuje slobodu prejavu a sociálnu súdržnosť.

Náš život sa stal menej bezpečným a Európania pociťujú túto skutočnosť čoraz silnejšie. Ich **vnímanie bezpečnosti a ochrany v EÚ** je narušené do takej miery, že 64 % z nich sa obáva o bezpečnosť EÚ

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

v budúcnosti[2]. Ani podniky nie sú v tomto smere výnimkou: misinformácie a dezinformácie, trestná činnosť a nezákonná činnosť či kybernetická špionáž patria medzi desať hlavných rizík identifikovaných v správe Svetového ekonomického fóra o globálnych rizikách z roku 2025[3].

Európania by mali **mať možnosť žiť svoj život bez strachu**, či už na uliciach, doma, na verejných miestach, v metre alebo na internete. Jadrom činnosti EÚ v oblasti bezpečnosti je ochrana ľudí, najmä tých, ktorí sú najzraniteľnejší voči útokom, ktorých terčom sú najmä deti, ženy a menšiny vrátane židovských a moslimských komunít. Ochrana ľudí má zásadný význam pre budovanie odolných a súdržných spoločností.

Komisia v záujme zlepšenia boja proti hrozbám v nadchádzajúcich rokoch zavádza **európsku stratégiu vnútornej bezpečnosti**. Vďaka prísnejšiemu právnemu súboru nástrojov, užšej spolupráci a intenzívnejšej výmene informácií posilníme našu odolnosť a kolektívnu schopnosť predvídať bezpečnostné hrozby, predchádzať im, odhaľovať ich a účinne na ne reagovať. Spoločný prístup k otázke vnútornej bezpečnosti podporí členské štáty pri využívaní sily technológií na posilnenie, a nie na oslabenie bezpečnosti a zároveň prispeje k zaisteniu bezpečného digitálneho priestoru pre všetkých. Bude prínosom aj pokiaľ ide o spoločnú reakciu členských štátov na globálne politické a hospodárske zmeny, ktoré majú vplyv na vnútornú bezpečnosť Únie.

Táto stratégia spočíva na **troch zásadách** a v jej centre stojí dodržiavanie zásad právneho štátu a základných práv.

Po prvé, stanovuje ambíciu zmeny kultúry v oblasti bezpečnosti. Potrebujeme zaujať **celospoločenský prístup**, ktorého súčasťou budú všetci občania a zainteresované strany vrátane občianskej spoločnosti, výskumných pracovníkov, akademickej obce a súkromných subjektov. Opatrenia v rámci stratégie musia byť preto vždy, keď je to možné, výsledkom uplatnenia integrovaného prístupu založeného na zapojení viacerých zainteresovaných strán.

Po druhé, **aspekty bezpečnosti sa musia začleniť do všetkých právnych predpisov, politík a programov EÚ** vrátane jej vonkajšej činnosti. Pri príprave, preskúmaní a vykonávaní právnych predpisov, politík a programov bude potrebné vždy zohľadniť otázku bezpečnosti a uistiť sa, že sa riešia jej jednotlivé aspekty, aby sa podporil súdržný a komplexný prístup k bezpečnosti.

Nakoniec, bezpečná, chránená a odolná Európa si vyžaduje **značné investície zo strany EÚ, jej členských štátov aj súkromného sektora**. Na zabezpečenie vykonávania priorít a opatrení stanovených v tejto stratégii sú potrebné dostatočné ľudské a finančné zdroje. Ako sa uvádza v oznámení pod názvom: Na ceste k budúcemu viacročnému finančnému rámcu[4], Európa bude musieť zvýšiť verejné výdavky na bezpečnosť a podporovať výskum a investície v tejto oblasti, čím sa posilní jej strategická autonómia.

Táto stratégia dopĺňa **Stratégiu únie pripravenosti**[5], v ktorej sa stanovuje integrovaný prístup zohľadňujúci všetky riziká, pokiaľ ide o pripravenosť na konflikty, katastrofy spôsobené ľudskou činnosťou a prírodné katastrofy a krízy, a **Bielu knihu o európskej obrannej pripravenosti 2030**[6], ktorá podporuje rozvoj a nadobúdanie obranných spôsobilostí v celej EÚ s cieľom odradiť zahraničných protivníkov. Komisia takisto navrhne **európsky štít na obranu demokracie** s cieľom posilniť demokratickú odolnosť v EÚ. Všetky tieto iniciatívy stanovujú víziu bezpečnej, chránenej a odolnej EÚ.

[2] Rýchly prieskum Eurobarometra FL550: Výzvy a priority EÚ.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, s. 17.
[4] COM(2025) 46 final.
[5] JOIN(2025) 130 final.
[6] JOIN(2025) 120 final.

Nové riadenie európskej vnútornej bezpečnosti

Komisia bude úzko spolupracovať s členskými štátmi a agentúrami EÚ na zlepšení prístupu EÚ k vnútornej bezpečnosti, a to na strategickej aj operačnej úrovni.

Dosiahne sa to prostredníctvom:

- **dôslednej identifikácie potenciálnych dôsledkov nových a revidovaných iniciatív Komisie na bezpečnosť a pripravenosť od začiatku a počas celého procesu rokovaní,**
- **pravidelných zasadnutí projektovej skupiny Komisie pre európsku vnútornú bezpečnosť, ktorú podporí strategická medziodvetvová spolupráca v rámci Komisie,**
- **prezentácií analýz hrozieb týkajúcich sa vnútornej bezpečnosti, ktoré podporia činnosť akadémie bezpečnosti,**
- **rokovaní s členskými štátmi v Rade o vyvíjajúcich sa výzvach v oblasti vnútornej bezpečnosti na základe analýzy hrozieb a výmeny informácií o kľúčových politických prioritách,**
- **pravidelného podávania správ Európskemu parlamentu a Rade s cieľom sledovať a podporovať systematické vykonávanie kľúčových bezpečnostných iniciatív.**

2. Integrovaná situačná informovanosť a analýza

Vytvoríme nové spôsoby výmeny a prepájania informácií v rámci EÚ a budeme poskytovať pravidelnú analýzu hrozieb v oblasti vnútornej bezpečnosti EÚ, čo prispeje ku komplexnému posúdeniu rizík a hrozieb.

Riešenie bezpečnostných otázok začína **účinným predvídaním** hrozieb. EÚ musí mať k dispozícii komplexnú, dostatočne nezávislú a aktuálnu situačnú informovanosť a analýzu hrozieb. Základom pre posudzovanie hrozieb a boj proti nim a v konečnom dôsledku aj podkladom pre politické a legislatívne opatrenia sú využiteľné spravodajské informácie, pričom členské štáty sa vyzývajú, aby ich ďalej rozširovali prostredníctvom jednotnej kapacity na analýzu spravodajských informácií (SIAC), ako jednotného kontaktného miesta pre spravodajské informácie členských štátov[7]. Na úrovni EÚ musíme účinnejšie využívať **analýzy založené na spravodajských informáciách** a **hodnotenia hrozieb** a lepšie v tejto oblasti spolupracovať.

Komisia bude na základe rôznych posúdení rizík a hrozieb vypracovaných na úrovni EÚ, ako aj pre konkrétne odvetvia[8] pripravovať **pravidelné analýzy hrozieb v oblasti vnútornej bezpečnosti EÚ**, v ktorých identifikuje hlavné bezpečnostné výzvy a poskytne tak podklady pre politické priority. To prispeje k vytvoreniu pružnej a reakcieschopnej politiky v oblasti vnútornej bezpečnosti, ktorá bude účinne riešiť vyvíjajúce sa hrozby, lepšie chrániť ľudí a podniky pred útokmi a umožní prijímať včasné a cielené politické opatrenia. Tieto analýzy hrozieb v oblasti vnútornej bezpečnosti EÚ prispejú aj ku **komplexnému posúdeniu (medziodvetvových, prierezových) rizík a hrozieb na úrovni EÚ**, ktoré vypracovala Komisia a vysoká predstaviteľka, ako sa uvádza v Stratégii únie pripravenosti.

Základom výmeny informácií je dôvera a bezpečné zaobchádzanie, čo si vyžaduje spoľahlivú a bezpečnú infraštruktúru. Inštitúcie, orgány a agentúry EÚ musia byť schopné používať na

[7] Správa s názvom Spoločne bezpečnejší: posilnenie európskej civilnej a vojenskej pripravenosti a pohotovosti, s. 23.

[8] Sektorové posúdenia hrozieb, ktoré prispejú k tejto analýze hrozieb, zahŕňajú Hodnotenie hrozieb závažnej a organizovanej trestnej činnosti v EÚ (SOCTA), správu EÚ o situácii a trendoch v oblasti terorizmu (TE-SAT), Spoločnú správu o posúdení kybernetickej bezpečnosti (JCAR) a budúce posúdenia hrozieb, rizík a metód prania špinavých peňazí a financovania terorizmu, ktoré má pripraviť Komisia a Úrad pre boj proti praniu špinavých peňazí.

výmenu citlivých a utajovaných skutočností medzi sebou a s členskými štátmi **bezpečné komunikačné kanály**. Investície do **interoperabilných bezpečných systémov** a spoľahlivých technológií posilnia autonómiu EÚ a zlepšia aj jej schopnosť zvládať krízy a zabezpečovať prevádzkovú odolnosť. Komisia v tejto súvislosti naliehavo vyzýva spoluzákonodarcov, aby dokončili rokovania o **navrhovanom nariadení o bezpečnosti informácií v inštitúciách, orgánoch, úradoch a agentúrach Únie**, najmä s cieľom zabezpečiť spoločný rámec pre zaobchádzanie s citlivými neutajovanými a utajovanými skutočnosťami[9].

Komisia v záujme zabezpečenia vlastnej prevádzkovej bezpečnosti a situačnej informovanosti a s cieľom chrániť ľudí, fyzický majetok a operácie na všetkých jej pracoviskách zreviduje svoj rámec riadenia bezpečnosti a zriadi **Integrované centrum bezpečnostných operácií (ISOC)**. Posilní tiež svoje operačné a analytické kapacity na identifikáciu a zmierňovanie hybridných hrozieb.

Aspekty pripravenosti a bezpečnosti sa budú v súlade so Stratégiou únie pripravenosti začleňovať do všetkých právnych predpisov, politík a programov EÚ. Komisia bude pri príprave alebo preskúmaní právnych predpisov, politík alebo programov dôsledne posudzovať potenciálne vplyvy uprednostňovanej možnosti politiky na pripravenosť a bezpečnosť. Tvorcovia politík v Komisii sa budú v tejto súvislosti zúčastňovať na pravidelnej odbornej príprave.

S cieľom podporiť členské štáty bude Komisia rokovať s Radou o vyvíjajúcich sa výzvach v oblasti vnútornej bezpečnosti a kľúčových politických prioritách a bude ju pravidelne informovať o vykonávaní stratégie. Zároveň bude informovať Európsky parlament a príslušné zainteresované strany a zapájať sa do všetkých príslušných opatrení.

Kľúčové opatrenia

Komisia:

- **bude vypracovávať a predkladať pravidelné analýzy hrozieb, ktoré predstavujú výzvy v oblasti vnútornej bezpečnosti EÚ.**

Členské štáty sa vyzývajú, aby:

- **zintenzívnili výmenu spravodajských informácií so SIAC a zabezpečili lepšiu výmenu informácií s agentúrami a orgánmi EÚ.**

Európsky parlament a Rada sa vyzývajú, aby:

- **dokončili rokovania o navrhovanom nariadení o bezpečnosti informácií v inštitúciách, orgánoch, úradoch a agentúrach Únie.**

3. Posilnené bezpečnostné spôsobilosti EÚ

Vytvoríme nové nástroje na presadzovanie práva, ako je napr. prepracovaný mandát Europolu, a lepšie prostriedky na koordináciu a zaistenie bezpečnej výmeny údajov a zákonného prístupu k údajom.

EÚ musí v záujme účinného boja proti vyvíjajúcim sa hrozbám posilniť svoje bezpečnostné spôsobilosti a podporovať inovácie. Orgány presadzovania práva a justičné orgány, ako hlavní aktéri bojujúci proti hrozbám pre vnútornú bezpečnosť, potrebujú správne operačné nástroje a spôsobilosti, aby mohli rýchlo a účinne konať. Ak chcú tieto orgány účinne predchádzať

[9] COM(2022) 119 final.

trestným činom, odhaľovať ich, vyšetrovať a stíhať, musia byť schopné komunikovať a koordinovať svoju činnosť cezhranične aj medzi jednotlivými útvarmi.

Agentúry a orgány EÚ v oblasti vnútornej bezpečnosti

Zásadný význam pre bezpečnostnú architektúru EÚ majú agentúry a orgány EÚ v oblasti spravodlivosti, vnútorných záležitostí a kybernetickej bezpečnosti a rozširovaním ich povinností rastie aj ich opodstatnenie.

Europol má dnes, 25 rokov po svojom zriadení, dôležitejšie postavenie v bezpečnostnom rámci EÚ ako kedykoľvek predtým. Podporuje komplexné cezhraničné vyšetrovania, uľahčuje výmenu informácií, vyvíja inovatívne nástroje pre policajné činnosti a poskytuje pokročilé odborné znalosti v oblasti presadzovania práva. Avšak tomu, aby naplno využíval svoj operačný potenciál pri podpore vyšetrovacích a operačných činností zameraných na boj proti cezhraničnej trestnej činnosti, bráni niekoľko faktorov: od nedostatočnej úrovne zdrojov až po skutočnosť, že jeho súčasný mandát nezahŕňa nové bezpečnostné hrozby, ako sú sabotáž, hybridné hrozby alebo manipulácia s informáciami. Komisia preto navrhne **ambiciózne prepracovanie mandátu Europolu** s cieľom premeniť ho na skutočne operačnú policajnú agentúru, ktorá bude lepšie podporovať členské štáty. Cieľom je posilniť technologické odborné znalosti a kapacitu Europolu a podporiť tak vnútroštátne orgány presadzovania práva, zlepšiť koordináciu s inými agentúrami a orgánmi a s členskými štátmi, posilniť strategické partnerstvá s partnerskými krajinami a súkromným sektorom a zabezpečiť posilnený dohľad nad Europolom.

Komisia bude okrem toho pracovať na ďalšom **zlepšovaní efektívnosti a komplementárnosti agentúr a orgánov EÚ v oblasti vnútornej bezpečnosti a na posilnení ich plynulej vzájomnej spolupráce**.

Mandát **Eurojustu** sa v záujme účinnejšej justičnej spolupráce posúdi a rozšíri, čím sa posilní komplementárnosť a spolupráca s Europolom. To povedie k zvýšeniu efektívnosti Eurojustu, ako aj jeho schopnosti poskytovať proaktívnu podporu a analýzu justičným orgánom členských štátov. V prípade **Európskej prokuratúry** Komisia vzhľadom na jej jedinečnú právomoc vyšetrovať a stíhať trestné činy poškodzujúce finančné záujmy zváži, ako najlepšie zlepšiť jej schopnosť chrániť finančné prostriedky Únie. Zároveň sa posilní spolupráca medzi Európskou prokuratúrou a Europolom.

Zásadný význam pre spoluprácu má **účinná a bezpečná výmena informácií medzi agentúrami**. Zo spoločného vyhlásenia z januára 2024[10] vyplynulo, že je potrebné zaistiť rýchlu vzájomnú výmenu informácií medzi Europolom a agentúrou Frontex, a to aj na operačné účely. Ústrednú úlohu pri zabezpečovaní bezpečného uchovávania a dostupnosti údajov v záujme lepšej koordinácie a efektívnejšej výmeny informácií medzi agentúrami zohráva **agentúra eu-LISA**. Odborné znalosti o ochrane základných práv pri vypracúvaní a vykonávaní bezpečnostných politík poskytuje **Agentúra EÚ pre základné práva**.

Úrad EÚ pre boj proti praniu špinavých peňazí (AMLA) bol oprávnený porovnávať informácie na základe pozitívnej/negatívnej lustrácie s informáciami sprístupnenými Europolom, Európskou prokuratúrou, Eurojustom a Úradom EÚ pre boj proti podvodom s cieľom vykonávať spoločné analýzy cezhraničných prípadov.

Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) zohráva ústrednú úlohu pri vykonávaní európskych právnych predpisov v oblasti kybernetickej bezpečnosti. Pri

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

nadchádzajúcej revízii **aktu o kybernetickej bezpečnosti** Komisia posúdi jej mandát a navrhne modernizáciu s cieľom posilniť jej pridanú hodnotu EÚ.

Spolupráca medzi colnými orgánmi a inými orgánmi presadzovania práva sa zintenzívni navrhovaným vytvorením **Colného orgánu EÚ** a **Colného dátového centra EÚ** v rámci balíka colných reforiem EÚ. Informácie z budúceho centra a súvisiace údaje od Europolu, Eurojustu, Európskej prokuratúry, úradu OLAF, úradu AMLA a agentúry Frontex v rámci ich príslušných právomocí posilnia spoločnú analýzu a prispejú k súdržnejším operačným činnostiam, najmä na vonkajších hraniciach. Komisia nabáda spoluzákonodarcov, aby urýchlene dokončili rokovania o colnej reforme EÚ, a bude im na tento účel naďalej pomáhať.

Posilnenie komplementárnosti medzi Európskou prokuratúrou, úradom OLAF, Europolom, Eurojustom, úradom AMLA a navrhovaným Colným orgánom EÚ bude vychádzať aj z výsledkov prebiehajúceho preskúmania **štruktúry EÚ pre boj proti podvodom**. Tento holistický prístup zameraný na lepšie využívanie trestnoprávnych aj administratívnych prostriedkov, interoperabilitu informačných systémov a lepšiu spoluprácu bude prínosom pre vnútornú bezpečnosť.

Kritická komunikácia

Kritické komunikačné systémy[11] sú dnes vo väčšine prípadov prevádzkované izolovane na vnútroštátnej úrovni. To znamená, že špecialisti prvého zásahu v mnohých prípadoch nemôžu komunikovať so svojimi partnermi, ak prekračujú hranice a vstupujú na územie iných členských štátov. V niektorých členských štátoch existujú tiež obmedzenia, ktoré neumožňujú komunikáciu medzi rôznymi typmi špecialistov prvého zásahu (napr. políciou a záchranármi). Normy väčšiny systémov nespĺňajú súčasné požiadavky z hľadiska funkčnosti a odolnosti, čo výrazne obmedzuje reakčnú kapacitu špecialistov prvého zásahu, najmä pri cezhraničných zásahoch.

V záujme zlepšenia schopnosti EÚ reagovať na krízy Komisia navrhne právne predpisy na vytvorenie **európskeho kritického komunikačného systému (EUCCS)**, ktorým sa v rámci EÚ prepoja kritické komunikačné systémy ďalšej generácie jednotlivých členských štátov. Cieľom je, aby bol EUCCS založený na troch strategických pilieroch: operačná mobilita, silná odolnosť a strategická autonómia. Iniciatívou EUCCS sa stanovia harmonizované požiadavky a prispeje sa k modernizácii kritických komunikačných systémov členských štátov, čo im umožní bezproblémové fungovanie. Takisto sa rozšíri systémové pokrytie, a to prostredníctvom budúceho multiorbitálneho systému IRIS[212]. V rámci projektov financovaných EÚ sa vybudujú technické spôsobilosti EUCCS, ktoré budú založené predovšetkým na technológiách európskych poskytovateľov, čím sa podporí strategická autonómia EÚ v tomto citlivom odvetví.

Zákonný prístup k údajom

Orgány presadzovania práva a justičné orgány musia byť schopné vyšetrovať trestnú činnosť a prijímať príslušné opatrenia. Takmer všetky formy závažnej a organizovanej trestnej činnosti obsahujú v súčasnosti digitálnu stopu[13]. Približne 85 % vyšetrovaní trestných činov v súčasnosti závisí od schopnosti orgánov presadzovania práva získať digitálne informácie[14].

Skupina na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva vo svojej záverečnej správe[15] zdôraznila, že páchatelia trestnej činnosti majú za posledné desaťročie

[11] Ide o siete využívané orgánmi presadzovania práva, pohraničnou strážou, colnými orgánmi, civilnou ochranou, hasičmi, záchranármi a inými kľúčovými aktérmi v oblasti verejnej bezpečnosti a ochrany.
[12] Satelitná infraštruktúra pre odolnosť, prepojenosť a bezpečnosť.
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:52019PC0070.
[15] Záverečná správa skupiny na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva – 15. 11. 2024, 4802e306-c364-4154-835b-e986a9a49281_en.

náskok pred orgánmi presadzovania práva a justíciou, a to z dôvodu, že využívajú nástroje a produkty platiace v iných jurisdikciách, kde poskytovatelia služieb zaviedli opatrenia, ktoré bránia príslušným orgánom riadne spolupracovať pri zákonných žiadostiach v jednotlivých trestných veciach. Systematická spolupráca medzi orgánmi presadzovania práva a súkromnými subjektmi vrátane poskytovateľov služieb je preto základom pre podporu budúceho úsilia o narušenie najnebezpečnejších zločineckých sietí a boj proti zločincom v Únii aj mimo nej.

Keďže digitalizácia čoraz viac vstupuje do nášho každodenného života a poskytuje čoraz významnejší zdroj nových nástrojov na páchanie trestnej činnosti, je nevyhnutné vytvoriť rámec pre prístup k údajom, ktorý by reagoval na potreby presadzovania našich právnych predpisov a ochrany našich hodnôt. Pre zaistenie kybernetickej bezpečnosti a ochrany pred vznikajúcimi bezpečnostnými hrozbami je zároveň rovnako dôležité zabezpečiť ochranu digitálnych systémov pred neoprávneným prístupom. Takéto rámce v oblasti prístupu musia tiež rešpektovať základné práva a zabezpečiť okrem iného primeranú ochranu súkromia a osobných údajov.

EÚ prijala v posledných rokoch opatrenia na boj proti **internetovej trestnej činnosti, ako aj na uľahčenie prístupu k digitálnym dôkazom týkajúcim sa všetkých trestných činov**, a to prijatím pravidiel týkajúcich sa elektronických dôkazov, ktoré sa budú v plnej miere uplatňovať od augusta 2026[16]. Doplnia ich medzinárodné nástroje na výmenu informácií a dôkazov. Komisia zároveň čoskoro navrhne podpísanie a uzavretie nového **Dohovoru OSN o boji proti počítačovej kriminalite**.

V nadväznosti na odporúčania skupiny na vysokej úrovni[17] Komisia predloží v prvom polroku 2025 **plán, v ktorom stanoví právne a praktické opatrenia**, ktoré navrhuje prijať na **zabezpečenie zákonného a účinného prístupu k údajom**. Ako ďalší krok uskutoční posúdenie vplyvu **pravidiel uchovávania údajov** na úrovni EÚ a pripraví **technologický plán pre šifrovanie**, ktorého cieľom bude identifikovať a posúdiť technologické riešenia, ktoré by orgánom presadzovania práva umožnili zákonný prístup k šifrovaným údajom spôsobom, ktorým sa zabezpečí kybernetická bezpečnosť a základné práva.

Operačná spolupráca

Komisia bude spolupracovať s členskými štátmi, agentúrami a orgánmi EÚ a partnerskými krajinami na posilnení operačnej spolupráce, ktorá je základom pre účinnejší prístup k boju proti nadnárodnej organizovanej trestnej činnosti a terorizmu.

Európska multidisciplinárna platforma proti hrozbám trestnej činnosti (EMPACT), ako hlavný rámec EÚ pre spoločné opatrenia proti závažnej a organizovanej trestnej činnosti, dosiahla významné operačné výsledky. Ďalší cyklus platformy EMPACT 2026 – 2029 predstavuje príležitosť ešte viac posilniť tento rámec. Aby mohla Únia narušiť najnebezpečnejšie zločinecké siete a postaviť sa proti zločincom, musí zefektívniť svoje úsilie a zamerať ho na najnaliehavejšie priority, posilniť záväzky členských štátov a zabezpečiť účinné využívanie zdrojov.

Komisia bude v tejto súvislosti spolupracovať s predsedníctvami Rady a členskými štátmi na **maximalizácii potenciálu platformy EMPACT a riešiť kľúčové priority ďalšieho cyklu EMPACT 2026 – 2029**. Riešenie týchto prioritných otázok si vyžaduje mať k dispozícii spravodajské informácie o najnebezpečnejších zločineckých sieťach, vykonávať spoločné vyšetrovania a zriaďovať operačné pracovné skupiny, ako aj zaistiť dôraznú reakciu zo strany justičných orgánov a zaujať prístup spočívajúci v „sledovaní peňazí“. Únia musí navyše riešiť

[16] Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie (Ú. v. EÚ L 191, 28.7.2023).

[17] Závery Rady o prístupe k údajom na účely účinného presadzovania práva (12. decembra 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/sk/pdf.

problém náboru páchateľov trestnej činnosti a infiltráciu trestnej činnosti, ako aj posilniť spoluprácu medzi orgánmi presadzovania práva a agentúrami na medzinárodnej úrovni a súvisiacu odbornú prípravu.

Komisia bude podporovať aj iné formy **cezhraničnej operačnej spolupráce v oblasti presadzovania práva medzi členskými štátmi a krajinami pridruženými k schengenskému priestoru**. Schengenský priestor bez kontrol na vnútorných hraniciach si na zaistenie vysokej úrovne vnútornej bezpečnosti vyžaduje úzku spoluprácu a výmenu informácií medzi orgánmi presadzovania práva členských štátov. Príslušníci orgánov presadzovania práva ešte stále čelia výzvam pri sledovaní alebo vykonávaní naliehavých cezhraničných zásahov[18] a boj proti hybridným hrozbám si tiež vyžaduje intenzívnejšiu cezhraničnú spoluprácu. V záujme vypracovania spoločnej strategickej vízie by sa mala vytvoriť **skupina na vysokej úrovni pre budúcnosť operačnej spolupráce v oblasti presadzovania práva**.

Efektívna výmena údajov medzi orgánmi presadzovania práva je nevyhnutná aj pre účinnú cezhraničnú spoluprácu. **Architektúra interoperability** poskytne orgánom presadzovania práva a Europolu po jej zavedení účinný prístup ku kľúčovým informáciám. EÚ a jej členské štáty by zároveň mali uprednostniť dvojstrannú a mnohostrannú výmenu informácií prostredníctvom právneho a technického vykonávania **prümského nariadenia II**[19] v spolupráci s agentúrou eu-LISA a Europolom. To umožní bezpečnú automatizovanú výmenu odtlačkov prstov, profilov DNA, údajov o evidencii vozidiel, podôb tváre a policajných záznamov prostredníctvom smerovačov EÚ. Na vnútroštátnej úrovni musia členské štáty vykonávať **smernicu o výmene informácií**[20], čím sa posilnia kanály výmeny informácií, a tak sa zaistí plynulý cezhraničný tok informácií, a zároveň sa zabezpečí ich integrácia so systémami na úrovni Únie, ako je SIENA[21].

Účinná cezhraničná spolupráca závisí aj od podpory **spoločnej kultúry EÚ v oblasti presadzovania práva**. Na dosiahnutie tohto cieľa sú nevyhnutné spoločné školenia, centrá excelentnosti a programy mobility. Komisia preskúma, ako môže EÚ čo najlepšie podporiť odbornú prípravu orgánov členských štátov, pričom sa bude opierať o Agentúru EÚ pre odbornú prípravu v oblasti presadzovania práva (**CEPOL**).

Posilnenie bezpečnosti hraníc

Posilnenie odolnosti a bezpečnosti vonkajších hraníc má zásadný význam pre boj proti hybridným hrozbám, napr. zneužívaniu migrácie ako zbrane, ako aj pre zabránenie vstupu aktérov a tovaru, ktoré predstavujú hrozbu, do EÚ a pre účinný boj proti cezhraničnej trestnej činnosti a terorizmu. **Plánuje sa, že sa** v roku 2026 **posilní Schengenský informačný systém (SIS)**, čo umožní členským štátom vkladať zápisy o štátnych príslušníkoch tretích krajín zapojených do terorizmu a do iných závažných trestných činov, ako aj o zahraničných teroristických bojovníkoch na základe údajov, ktoré si tretie krajiny vymieňajú s Europolom.

Vďaka zlepšenej **interoperabilite** rozsiahlych informačných systémov EÚ budú mať členské štáty prístup k základným informáciám o osobách z tretích krajín, ktoré prekračujú alebo majú v úmysle prekročiť vonkajšie hranice, čo pomôže zodpovedným orgánom posúdiť podmienky

[18] Ako sa uvádza v posúdení Komisie týkajúcom sa vykonávania odporúčania Rady (EÚ) 2022/915 z 9. júna 2022 o operačnej spolupráci v oblasti presadzovania práva členskými štátmi (5909/25).
[19] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/982 z 13. marca 2024 o automatizovanom vyhľadávaní a výmene údajov na účely policajnej spolupráce a o zmene rozhodnutí Rady 2008/615/SVV a 2008/616/SVV a nariadení Európskeho parlamentu a Rady (EÚ) 2018/1726, (EÚ) 2019/817 a (EÚ) 2019/818 (prümské nariadenie II) (Ú. v. EÚ L, 2024/982, 5.4.2024).
[20] Smernica Európskeho parlamentu a Rady (EÚ) 2023/977 z 10. mája 2023 o výmene informácií medzi orgánmi presadzovania práva členských štátov a zrušení rámcového rozhodnutia Rady 2006/960/SVV (Ú. v. EÚ L 134, 22.5.2023, s. 1 – 24).
[21] Sieťová aplikácia na zabezpečenú výmenu informácií.

na povolenie vstupu na územie členských štátov[22]. Komisia bude naďalej úzko spolupracovať s členskými štátmi a agentúrou eu-LISA na urýchlenom zavedení týchto systémov, najmä **systému vstup/výstup (EES), Európskeho systému pre cestovné povolenia (ETIAS) a revidovaného vízového informačného systému (VIS)** s cieľom zabezpečiť ich bezproblémové fungovanie a prínos v oblasti bezpečnosti.

V záujme ďalšieho posilnenia bezpečnosti hraníc a posilnenia spolupráce EÚ v súvislosti s vyvíjajúcimi sa hrozbami **Komisia navrhne posilnenie agentúry Frontex**. Počet príslušníkov európskej pohraničnej a pobrežnej stráže by sa mal časom strojnásobiť na 30 000. Agentúra by mala byť vybavená pokročilými technológiami v oblasti sledovania a situačnej informovanosti vrátane spravodajských informácií, ktoré sú relevantné z hľadiska európskeho integrovaného riadenia hraníc, a mala by mať prístup k spoľahlivým vládnym službám EÚ zameraným na pozorovanie Zeme na účely kontroly hraníc, ktoré sa majú zriadiť do roku 2027. Tým by sa mala zlepšiť schopnosť odhaľovať cezhraničnú trestnú činnosť na vonkajších hraniciach, predchádzať jej a bojovať proti nej, ako aj posilniť podpora agentúry, ktorú poskytuje členským štátom pri vykonávaní návratov, najmä v súvislosti so štátnymi príslušníkmi tretích krajín, ktorí predstavujú bezpečnostné riziko.

Podvody v oblasti dokladov a podvody s osobnými údajmi uľahčujú prevádzačstvo, obchodovanie s ľuďmi, utajované pohyby páchateľov trestnej činnosti a obchodovanie s nezákonným tovarom. Schopnosť vnútroštátnych orgánov identifikovať jednotlivcov používajúcich viacnásobné totožnosti a bojovať proti podvodom s osobnými údajmi zlepší po zavedení do prevádzky **detektor viacnásobných totožností (MID)**[23]. Komisia preskúma spôsoby, ktorými by sa zvýšila bezpečnosť cestovných dokladov a dokladov o pobyte vydávaných občanom EÚ a štátnym príslušníkom tretích krajín. Posúdi tiež, ako môžu európske peňaženky digitálnej identity, ktoré sa majú zaviesť v rámci európskeho rámca digitálnej identity do konca roka 2026, prispieť k zvýšeniu bezpečnosti cestovných dokladov a zlepšeniu overovania totožnosti. Tým sa doplnia návrhy týkajúce sa digitálnych cestovných identifikátorov a digitálnej cestovnej aplikácie EÚ[24].

Zásadný význam pri identifikácii a vyšetrovaní pohybov páchateľov trestnej činnosti, teroristov a iných osôb, ktoré predstavujú bezpečnostné hrozby, majú pre príslušné orgány **cestovné informácie**. Hoci existuje rámec EÚ pre informácie o obchodnej leteckej doprave[25], spracúvanie údajov z iných druhov dopravy na účely presadzovania práva je roztrieštené. Zločinci a teroristi tak môžu využívať rôzne spôsoby dopravy na nezákonnú činnosť bez toho, aby došlo k ich odhaleniu. Komisia bude spolupracovať s členskými štátmi a odvetvím dopravy na **posilnení rámca pre cestovné informácie** a preskúma zavedenie systému Únie, v rámci ktorého by sa od prevádzkovateľov súkromných letov vyžadoval zber a prenos údajov o cestujúcich, prehodnotí pravidlá spracúvania osobných záznamov o cestujúcich a posúdi spôsoby zefektívnenia spracúvania informácií o námornej doprave. Pokiaľ ide o cestnú

[22] Systém vstup/výstup (EES) konkrétne umožní členským štátom identifikovať štátnych príslušníkov tretích krajín na vonkajších hraniciach schengenského priestoru a zaznamenávať ich vstupy a výstupy, čo povedie k systematickej identifikácii osôb, ktoré prekročili dĺžku oprávneného pobytu. Európsky systém pre cestovné informácie a povolenia (ETIAS) a vízový informačný systém (VIS) umožnia členským štátom pred príchodom štátneho príslušníka tretej krajiny na vonkajšie hranice predbežne posúdiť, či by jeho prítomnosť na území EÚ mohla predstavovať bezpečnostné riziko.

[23] MID je jedným z komponentov interoperability zavedených nariadením (EÚ) 2019/818 a nariadením (EÚ) 2019/817.

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

[25] Rámec pre záznamy o cestujúcich (PNR) a vopred poskytované informácie o cestujúcich (API) stanovený smernicou (EÚ) 2016/681 („smernica o PNR“) a nariadeniami (EÚ) 2025/12 a (EÚ) 2025/13 („nariadenia API“).

dopravu, Komisia posúdi rozšírené využívanie systémov **automatického rozpoznávania evidenčných čísel vozidiel (ANPR)** a zvýši možnosti synergií so SIS.

Výhľad, inovácia a prístup založený na spôsobilostiach

Komisia vypracuje **komplexný výhľadový prístup k vnútornej bezpečnosti na úrovni EÚ**, pričom bude vychádzať z najlepších postupov identifikovaných na úrovni jednotlivých členských štátov. Tento prístup podporí tvorbu politík a usmerní investície do príslušného výskumu a inovácií v oblasti bezpečnosti financovaných EÚ.

Výskum a inovácie zohrávajú kľúčovú úlohu pre vnútornú bezpečnosť, pretože vytvárajú riešenia na boj proti vznikajúcim hrozbám, a to aj hrozbám vyplývajúcim zo zneužívania technológií[26]. EÚ musí pokračovať v investíciách do výskumu a inovácií v oblasti bezpečnosti[27], ktoré sa zameriavajú na vývoj inovačných nástrojov a riešení potrebných na boj proti bezpečnostným hrozbám, a pri tom dbať na to, aby sa dodržiavali jej pravidlá a základné práva. Komisia by mala podporovať prechod od výskumu k zavádzaniu a tým zabezpečiť účinné využívanie týchto moderných spôsobilostí, pričom prioritou by mali byť **moderné technológie**, ako je umelá inteligencia. Tento prístup by mal zahŕňať odbornú prípravu, vďaka ktorej by sa zlepšilo používanie systémov umelej inteligencie a iných technických spôsobilostí orgánmi presadzovania práva a justičnými orgánmi. V prípade potreby by sa mal tiež využiť potenciál technológií dvojakého použitia, a to v oboch smeroch (z civilného do obranného sektora a naopak)[28].

Európske inovačné centrum pre vnútornú bezpečnosť[29], sieť inovačných laboratórií, ktoré poskytujú najnovšie inovácie a účinné riešenia na podporu práce aktérov v oblasti vnútornej bezpečnosti v EÚ a členských štátoch, pomôže začleniť výskum do praxe a politiky. Zvýšenie efektívnosti Europolu si vyžaduje posilnenie registra nástrojov Europolu (ETR), čo mu umožní operatívne identifikovať, vyvíjať, spoločne obstarávať a používať pokročilé technológie. Komisia okrem toho zriadi vo svojom Spoločnom výskumnom centre **Výskumné a inovačné centrum v oblasti bezpečnosti**, ktoré bude spájať výskumných pracovníkov s cieľom skrátiť cyklus od výsledkov výskumu až po inovácie, vývoj a úspešnú realizáciu a zároveň znížiť náklady na vývoj, testovanie a validáciu.

Náš **európsky výskumný priestor** je vo svojej podstate založený na spolupráci, a preto doň môžu prenikať zahraničné vplyvy a dezinformácie. Komisia a členské štáty prijímajú po prijatí odporúčania Rady o bezpečnosti výskumu[30] opatrenia na posilnenie postavenia príslušných aktérov, okrem iného zriadením Odborného centra pre bezpečnosť výskumu.

Kľúčové opatrenia

Komisia prijme:

- **v roku 2026 legislatívny návrh na premenu Europolu na skutočne fungujúcu agentúru presadzovania práva,**
- **v roku 2026 legislatívny návrh na posilnenie Eurojustu,**

[26] Pozri správu Spoločného výskumného centra Komisie s názvom „*Emerging risks and opportunities for EU internal security from new technologies*“ (Vznikajúce riziká a príležitosti pre vnútornú bezpečnosť EÚ vyplývajúce z nových technológií), https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.

[27] *Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025* (Štúdia o posilnení výskumu a inovácií v oblasti bezpečnosti financovaných EÚ – 20 rokov výskumu a inovácií v oblasti civilnej bezpečnosti financovaných EÚ – 2025), https://data.europa.eu/doi/10.2837/0004501.

[28] Ako sa uvádza v Niinistöovej správe.

[29] Európske inovačné centrum pre vnútornú bezpečnosť | Europol.

[30] Ú. v. EÚ C/2024/3510, 30.5.2024.

- **v roku 2026 legislatívny návrh na posilnenie postavenia a úloh agentúry Frontex,**
- **v roku 2026 legislatívny návrh na zriadenie európskeho kritického komunikačného systému.**

Komisia:

- **v roku 2025 predloží plán, v ktorom sa stanoví ďalší postup, pokiaľ ide o zákonný a účinný prístup k údajom na účely presadzovania práva,**
- **v roku 2025 pripraví posúdenie vplyvu s cieľom podľa potreby aktualizovať pravidlá uchovávania údajov na úrovni EÚ,**
- **v roku 2026 predloží technologický plán pre šifrovanie s cieľom identifikovať a posúdiť technologické riešenia, ktoré umožnia zákonný prístup orgánov presadzovania práva k údajom,**
- **bude pracovať na vytvorení skupiny na vysokej úrovni na posilnenie operačnej spolupráce v oblasti presadzovania práva,**
- **v roku 2026 vytvorí vo svojom Spoločnom výskumnom centre Výskumné a inovačné centrum v oblasti bezpečnosti.**

Komisia v spolupráci s členskými štátmi a príslušnými agentúrami EÚ:

- **posilní architektúru platformy EMPACT,**
- **bude pracovať na rýchlom zavedení architektúry interoperability a vykonávaní prümského nariadenia II,**
- **posilní rámec pre cestovné informácie.**

Členské štáty sa vyzývajú, aby:

- **transponovali a plne vykonávali smernicu o výmene informácií.**

4. Odolnosť proti hybridným hrozbám a iným nepriateľským aktom

Budeme budovať odolnosť voči hybridným hrozbám, a to zvýšením ochrany kritickej infraštruktúry, posilnením kybernetickej bezpečnosti, zabezpečením dopravných uzlov a prístavov a bojom proti online hrozbám.

Frekvencia a sofistikovanosť nepriateľských aktov, ktoré oslabujú bezpečnosť EÚ, sa zvýšila a ich aktéri výrazne rozšírili svoj arzenál. Zintenzívnili sa hybridné kampane, ktorých cieľom je EÚ, jej členské štáty a partneri a ktoré zahŕňajú akty sabotáže zamerané na kritickú infraštruktúru, podpaľačstvo, kybernetické útoky, zasahovanie do volieb, zahraničné zasahovanie a manipuláciu s informáciami (FIMI) vrátane dezinformácií a zneužívanie migrácie ako zbrane. Výnimkou nie sú ani inštitúcie, orgány, úrady a agentúry Únie (ďalej len „subjekty Únie“), čo súvisí s ich politickou a operačnou úlohou a povahou informácií, s ktorými pracujú.

EÚ musí **zvýšiť svoju odolnosť**, účinne využívať súčasné nástroje a vyvinúť nové spôsoby, ako čeliť týmto vyvíjajúcim sa hrozbám zo strany štátnych a neštátnych subjektov, a to v súčasnosti aj v budúcnosti.

Kritická infraštruktúra

Hrozby pre **kritickú infraštruktúru** vrátane hybridných hrozieb, ako je sabotáž a škodlivá kybernetická činnosť, sú hlavným problémom, a to najmä pokiaľ ide o infraštruktúru, ktorá spája členské štáty – či už ide o spojovacie vedenie alebo cezhraničné komunikačné káble a dopravu. Od začiatku útočnej vojny Ruska proti Ukrajine sú akty sabotáže zamerané na

kritickú infraštruktúru častejšie (najčastejšie k nim dochádzalo v roku 2024), čo má vplyv na mnohé členské štáty. Aby sme mohli takéto činy účinne predvídať, odhaľovať ich, predchádzať im a reagovať na ne, je potrebné rozvinúť spoluprácu medzi orgánmi presadzovania práva, bezpečnostnými službami a službami kybernetickej bezpečnosti, vojenskou a civilnou ochranou a súkromnými prevádzkovateľmi.

Nevyhnutnou podmienkou pre zabezpečenie nepretržitého poskytovania základných služieb dôležitých pre hospodárstvo a spoločnosť je zníženie zraniteľnosti a posilnenie odolnosti kritických subjektov. V tejto súvislosti je preto dôležité, aby všetky členské štáty včas transponovali a správne vykonávali **smernicu o odolnosti kritických subjektov (CER)**[31] a **smernicu o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2)**[32].

V záujme zabezpečenia rýchleho pokroku bude Komisia v spolupráci so **skupinou pre odolnosť kritických subjektov a skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti** podporovať členské štáty pri identifikácii kritických subjektov[33] a výmene osvedčených postupov týkajúcich sa vnútroštátnych stratégií a posúdení rizík, pokiaľ ide o základné služby. Ak by došlo k narušeniam kritickej infraštruktúry so značným cezhraničným vplyvom, reakcie na úrovni EÚ sa budú koordinovať v súlade s **koncepciou kritickej infraštruktúry EÚ**. Komisia nabáda Radu, aby urýchlene prijala **kybernetickú koncepciu EÚ**, ktorá ďalej posilní koordináciu v oblasti krízového riadenia a prispeje k užšej spolupráci medzi orgánmi v oblasti fyzickej a digitálnej odolnosti. Po úspešných záťažových testoch v odvetví energetiky v roku 2023 bude Komisia podporovať **dobrovoľné záťažové testy** v iných odvetviach, ktoré sú kľúčové pre vnútornú bezpečnosť. Komisia okrem toho poskytne **prehľad na úrovni Únie o cezhraničných a medziodvetvových rizikách** pre základné služby, aby podporila prípravu posúdení rizík členskými štátmi a poskytla podklady pre komplexné posúdenie rizík na úrovni EÚ. V súlade so Stratégiou únie pripravenosti bude Komisia spolupracovať s členskými štátmi s cieľom identifikovať ďalšie odvetvia a služby, na ktoré sa nevzťahujú súčasné právne predpisy a v prípade ktorých môže byť potrebné konať.

Osobitná skupina EÚ – NATO pre odolnosť kritickej infraštruktúry podporila vynikajúcu spoluprácu pri výmene najlepších postupov a zvyšovaní odolnosti v odvetviach energetiky, dopravy, digitálnej infraštruktúry a vesmíru. Táto práca bude pokračovať v rámci **štruktúrovaného dialógu medzi EÚ a NATO o odolnosti**. **Súbor nástrojov EÚ na boj proti hybridným hrozbám** ponúka členským štátom a partnerom silnú podporu pri príprave na hybridné hrozby a boji proti nim. **Tímy rýchlej reakcie na hybridné hrozby**[34] poskytujú na požiadanie prispôsobenú krátkodobú pomoc členským štátom, rôznym misiám a partnerom EÚ. Pokiaľ ide o boj proti sabotáži, Komisia zintenzívni spoluprácu v rámci EÚ prostredníctvom odbornej činnosti[35], a to aj prostredníctvom **osobitného spoločného pracovného programu** pre expertov, ktorého cieľom je zefektívniť výmenu informácií a zmapovať protiopatrenia.

[31] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES.

[32] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

[33] Medzi odvetvia, na ktoré sa vzťahuje smernica, patria energetika, doprava, bankovníctvo, infraštruktúra finančného trhu, zdravotníctvo, pitná voda, odpadová voda, digitálna infraštruktúra, verejná správa, vesmír, výroba, spracovanie a distribúcia potravín.

[34] Strategický kompas pre bezpečnosť a obranu EÚ 2022, s. 22.

[35] Poradcovia EÚ pre ochrannú bezpečnosť, Európska sieť pre zneškodňovanie výbušných prostriedkov (EEODN), sieť ATLAS, bezpečnostná sieť EÚ pre vysokorizikové verejné priestory (EU HRSN), poradná skupina pre chemickú, biologickú, rádiologickú a jadrovú bezpečnosť, skupina pre odolnosť kritických subjektov (CERG).

Incidenty týkajúce sa **podmorských káblov** v Európe poukazujú na potrebu prísnejších opatrení a dôraznejších reakcií. Ako sa uvádza v **Akčnom pláne EÚ na zaistenie bezpečnosti káblov**[36], Komisia bude spolu s vysokým predstaviteľom spolupracovať s členskými štátmi, agentúrami EÚ a partnermi, ako je NATO, aby bola schopná predchádzať hrozbám súvisiacim s podmorskými káblami, odhaľovať ich, reagovať na ne a odrádzať od nich. Komisia bude s cieľom vypracovať integrovaný situačný prehľad hrozieb spolupracovať s členskými štátmi na vytvorení a zavedení integrovaného mechanizmu dohľadu nad podmorskými káblami, ktorý bude fungovať na dobrovoľnom základe, a to pre každú morskú oblasť, počnúc regionálnym uzlom severskej/baltskej oblasti.

Kybernetická bezpečnosť

Pretrvávajúca povaha **škodlivej kybernetickej činnosti**, ktorá je často súčasťou širšej škály viacrozmerných a hybridných hrozieb, si vyžaduje neustálu pozornosť a prijímanie opatrení na európskej úrovni. Únia prijala v posledných rokoch celý rad právnych predpisov v oblasti kybernetickej bezpečnosti, ktorými sa posilňuje kybernetická odolnosť subjektov NIS2 pôsobiacich v kritických odvetviach EÚ, ako aj subjektov Únie[37], zlepšuje bezpečnosť digitálnych produktov (akt o kybernetickej odolnosti) a stanovuje rámec pre podporu pripravenosti a reakcie na incidenty (akt o kybernetickej solidarite). V januári 2025 prijala Komisia v záujme zlepšenia odhaľovania hrozieb, pripravenosti a reakcie na krízu **európsky akčný plán pre kybernetickú bezpečnosť nemocníc a poskytovateľov zdravotnej starostlivosti**[38]. Kľúčovým prvkom je jeho úplné vykonávanie. Aby sme sa mohli postaviť novým hrozbám a reagovať na nový vývoj, musíme zároveň zintenzívniť našu činnosť, a to najmä v oblasti výmeny informácií, bezpečnosti dodávateľského reťazca, ransomvéru a kybernetických útokov, ako aj technologickej suverenity.

Jeho vykonávanie si okrem toho vyžaduje odstránenie súčasného nedostatku zručností v oblasti kybernetickej bezpečnosti, ktorý sa týka 299 000 ľudí. Komisia bude spolupracovať s členskými štátmi v rámci únie zručností[39] na rozšírení pracovnej sily v oblasti kybernetickej bezpečnosti, a to najmä využitím novej Akadémie kybernetických zručností. K zlepšeniu fondu talentov a reakcie Európy na potreby trhu práce v oblasti kybernetickej bezpečnosti prispieva Strategický plán vzdelávania v oblasti STEM[40].

Súbežne so zvyšovaním svojej odolnosti bude EÚ naďalej v plnej miere využívať na predchádzanie kybernetickým hrozbám pochádzajúcim od štátnych a neštátnych subjektov, odrádzanie od týchto hrozieb a reakciu na ne rámec pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti (**súbor nástrojov kybernetickej diplomacie**).

Bezpečnosť dodávateľských reťazcov IKT

Súbor nástrojov pre kybernetickú bezpečnosť 5G poskytuje príslušný rámec na ochranu sietí 5G, ale členské štáty ho v súčasnosti nevykonávajú dostatočne. Stále pretrvávajú neprijateľné bezpečnostné riziká, ktoré súvisia najmä s potrebou nahradiť vysokorizikových poskytovateľov. Súčasná fragmentácia vnútorného trhu vyplývajúca z rôznych prístupov k bezpečnosti dodávateľského reťazca IKT na vnútroštátnej úrovni by sa mohla riešiť prostredníctvom harmonizovaného prístupu, vďaka ktorému by sa predišlo kritickým

[36] JOIN(2025) 9 final.
[37] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2023/2841 z 13. decembra 2023, ktorým sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie (Ú. v. EÚ L, 2023/2841, 18.12.2023).
[38] https://digital-strategy.ec.europa.eu/sk/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM(2025) 90 final.
[40] COM(2025) 89 final.

závislostiam a znížilo by sa riziko, ktoré pre naše dodávateľské reťazce IKT predstavujú vysokorizikoví dodávatelia, a tak sa zabezpečila naša kritická infraštruktúra.

V súlade s týmto prístupom sa Komisia v nadchádzajúcej **revízii aktu o kybernetickej bezpečnosti** bude všeobecnejšie zaoberať bezpečnosťou a odolnosťou dodávateľských reťazcov a infraštruktúry IKT. Navrhne tiež zlepšenie **európskeho rámca certifikácie kybernetickej bezpečnosti**, čím sa zabezpečí včasné prijímanie budúcich systémov certifikácie a reakcia na politické potreby.

Komisia vypracuje spolu s členskými štátmi na základe existujúcich alebo prebiehajúcich odvetvových posúdení[41] **strategické plánovanie koordinovaných posúdení kybernetickobezpečnostných rizík**.

Cloudové a telekomunikačné služby sa stali základom dodávateľských reťazcov kritických infraštruktúr, podnikov a verejných orgánov. Komisia prijme opatrenia, ktoré podnietia kritické subjekty k tomu, aby si zvolili **cloudové a telekomunikačné služby, ktoré ponúkajú primeranú úroveň kybernetickej bezpečnosti**, pričom sa zohľadnia nielen technické riziká, ale aj strategické riziká a závislosti.

Ransomvér a kybernetické útoky

Pretrvávajúcou veľkou výzvou v EÚ a na celom svete je **ransomvér**, pričom podľa správy o ransomvéri sa celkové ročné náklady odhadujú na viac ako 250 miliárd EUR do roku 2031[42]. Postavenie subjektov v oblasti bezpečnosti výrazne zlepší **smernica NIS 2**, ako aj **akt o kybernetickej odolnosti**, v dôsledku čoho bude pre ransomvérové siete nákladnejšie vykonávať ich útoky. Komisia bude okrem toho úzko spolupracovať s členskými štátmi na zabezpečení toho, aby sa orgánom presadzovania práva nahlasovalo viac útokov ransomvéru, najmä pokročilých pretrvávajúcich hrozieb, a platby výkupného, čím sa uľahčí vyšetrovanie.

Aby EÚ predišla kybernetickým útokom a zastavila ich, musí posilniť výmenu informácií medzi orgánmi presadzovania práva, orgánmi a subjektmi v oblasti kybernetickej bezpečnosti, ako aj súkromnými subjektmi, a to pod záštitou Europolu a agentúry ENISA.

Europol a Eurojust by mali naďalej stavať na úspechoch, ktoré dosiahli pri narúšaní ransomvérových operácií a podporovať spoluprácu v oblasti presadzovania práva. Na tento účel by mali orgány presadzovania práva čo najviac využívať mechanizmy spolupráce vrátane **medzinárodného modelu reakcie na ransomvér vypracovaného Europolom** a **Medzinárodnej iniciatívy v oblasti boja proti ransomvéru (CRI)**[43]. Agentúra ENISA a Europol by mali spolupracovať na rozšírení registra dešifrovacích nástrojov pre ransomvérové kmene[44].

Technologická suverenita

Kybernetická bezpečnosť a technologická suverenita sú úzko prepojené a technologické závislosti sú oblasťou, ktorú je potrebné riešiť medzi prvými. Únia musí **riadiť vývoj a zavádzanie nových technológií** a Komisia pracovať na **posilnení spôsobilostí v oblasti strategických technológií**, ako sú umelá inteligencia, kvantové technológie, pokročilá konektivita, cloud, edge technológie a internet vecí[45], a to prostredníctvom nadchádzajúcich iniciatív, ako je akčný plán pre kontinent umelej inteligencie, kvantová stratégia a ďalšie

[41] Napríklad v oblastiach, akými sú siete 5G, telekomunikácie, elektrina, energia z obnoviteľných zdrojov a prepojené vozidlá.
[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] K dispozícii prostredníctvom projektu *No More Ransom*, https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.

iniciatívy[46]. Komisia bude naďalej podporovať včasné zavedenie najnovších dostupných medzinárodne dohodnutých **internetových protokolov**, ktoré sú nevyhnutné na zachovanie škálovateľného a efektívneho internetu so zvýšenou úrovňou kybernetickej bezpečnosti. Ďalšie opatrenia sú potrebné aj na riešenie **výziev súvisiacich s rádiovým spektrom**, napríklad v súvislosti so spoofingom GNSS, s rušením, rizikami dodávateľského reťazca a so závislosťami, ako je využívanie technológií kvantového snímania a skúmanie rozvoja kapacity na monitorovanie rádiových frekvencií.

Zásadný význam pre ochranu citlivej komunikácie, údajov v pokoji a digitálnych identít v novej kvantovej ére bude mať zavádzanie riešení **postkvantovej kryptografie (PQC)**. Komisia spolupracuje s členskými štátmi na podpore tohto prechodu vychádzajúc z odporúčania z roku 2024 o Pláne koordinovaného vykonávania prechodu na postkvantovú kryptografiu[47]. Členské štáty by mali v tejto súvislosti identifikovať vysokorizikové prípady v kritických subjektoch a čo najskôr, najneskôr však do konca roku 2030, zabezpečiť pre tieto vysokorizikové prípady kvantovo bezpečné šifrovanie. Komisia takisto spolupracuje s členskými štátmi a Európskou vesmírnou agentúrou (ESA) na vývoji a zavádzaní **európskej kvantovej komunikačnej infraštruktúry (EuroQCI)**[48] založenej na kvantovej distribúcii kľúčov (QKD) ako súčasti programu EÚ pre bezpečnú konektivitu **IRIS²**. Obe iniciatívy v konečnom dôsledku umožnia subjektom bezpečne prenášať údaje a uchovávať informácie.

Kvantové technológie budú zohrávať hlavnú úlohu aj pokiaľ ide o bezpečnostné aplikácie: v rámci **kvantovej stratégie** sa vypracuje **plán pre kvantové snímanie v bezpečnostných aplikáciách**. V rovnakom duchu Komisia pracuje na kvantovej odolnosti svojich kritických bezpečnostných systémov vrátane svojich utajovaných informačných systémov.

Rámec kybernetickej bezpečnosti priaznivý pre podnikanie

Nadchádzajúca revízia aktu o kybernetickej bezpečnosti je príležitosťou na **zjednodušenie právnych predpisov EÚ v oblasti kybernetickej bezpečnosti** v súlade s Kompasom konkurencieschopnosti. Komisia bude úzko spolupracovať s členskými štátmi na zabezpečení rýchleho, súdržného a podnikovo ústretového vykonávania horizontálneho rámca kybernetickej bezpečnosti stanoveného v smernici NIS 2, akte o kybernetickej odolnosti a akte o kybernetickej solidarite, pričom podporí jednoduchosť a súdržnosť a zabráni fragmentácii alebo duplicite pravidiel kybernetickej bezpečnosti v právnych predpisoch EÚ a vnútroštátnych právnych predpisoch.

S cieľom umožniť bezpečný prístup k online službám a posilniť digitálnu bezpečnosť v celej EÚ bude **európsky rámec digitálnej identity** do konca roka 2026 ponúkať všetkým občanom a obyvateľom EÚ dôveryhodné peňaženky digitálnej identity. Nadchádzajúca **európska podniková peňaženka** uľahčí bezpečné cezhraničné interakcie medzi podnikmi a orgánmi verejnej správy. Obidva prvky sú predpokladom bezpečného a efektívnejšieho fungovania jednotného trhu založeného na údajoch, na ktorom sa využívajú nástroje ako jednotná digitálna brána, elektronická fakturácia, elektronické obstarávanie a digitálny pas výrobku.

Online bezpečnosť

Niektoré z najzávažnejších hybridných hrozieb, ktoré ohrozujú bezpečnosť a ochranu ľudí v Európe a zameriavajú sa na demokratickú sféru EÚ, sa odohrávajú online. Medzi tieto hrozby patria nezákonné činnosti a nezákonný obsah na internete, manipulácia s informáciami

[46] Napr. spoločný podnik pre európsku vysokovýkonnú výpočtovú techniku – https://eurohpc-ju.europa.eu/index_en, hlavná kvantová iniciatíva – domovská stránka hlavnej kvantovej iniciatívy | hlavná kvantová iniciatíva, siete 3C [COM(2024) 81 final] a Akčný plán EÚ na zaistenie bezpečnosti káblov [JOIN(2025) 9 final].

[47] Odporúčanie o Pláne koordinovaného vykonávania prechodu na postkvantovú kryptografiu | formovanie digitálnej budúcnosti Európy.

[48] https://digital-strategy.ec.europa.eu/sk/policies/european-quantum-communication-infrastructure-euroqci.

zahŕňajúca ich umelé šírenie, zavádzajúce informácie a zahraničná manipulácia s informáciami a zahraničné zasahovanie.

Na zaistenie bezpečného a prístupného online prostredia, v ktorom sú aktéri zodpovední za svoje činy a ktoré je odolné aj voči hybridným hrozbám, je mimoriadne dôležité dôsledné presadzovanie **aktu o digitálnych službách**. V akte o digitálnych službách sa poskytovateľom veľmi veľkých online platforiem a veľmi veľkých internetových vyhľadávačov ukladá povinnosť vykonávať posúdenia rizík a zaviesť zmierňujúce opatrenia pre systémové riziká vyplývajúce z koncepcie, fungovania alebo využívania ich služieb. Takéto riziká môžu zahŕňať negatívne účinky na občiansku diskusiu a volebné procesy, ako aj na verejnú bezpečnosť, ako je rozsiahle zasahovanie zahraničných štátnych aktérov so zlými úmyslami, napríklad do volebných procesov. Dôležitá je odborná príprava príslušných orgánov členských štátov v oblasti používania právnych nástrojov na rýchle odstránenie nezákonného obsahu na internete, najmä pokiaľ ide o rodovo motivované kybernetické násilie. V akte o digitálnych službách sa stanovuje mechanizmus reakcie na krízu, ktorý možno aktivovať, ak mimoriadne okolnosti vedú k vážnemu ohrozeniu verejnej bezpečnosti alebo verejného zdravia v Únii alebo v jej podstatných častiach. Na doplnenie tohto mechanizmu Komisia a príslušné vnútroštátne orgány určené za koordinátorov digitálnych služieb vypracovali aj dobrovoľný **rámec pre reakciu na incidenty na základe aktu o digitálnych službách**. Koordinátori digitálnych služieb takisto prijali opatrenia na ochranu integrity volieb, napríklad organizovaním volebných okrúhlych stolov a záťažových testov[49]. Akt o digitálnych službách spolu s nariadením o politickej reklame[50] predstavuje jeden z mnohých prvkov na ochranu demokracie a integrity demokratických procesov, na ktoré by sa mohli zamerať nepriateľské subjekty, a to aj prostredníctvom digitálnych nástrojov a na sociálnych médiách.

Ďalším dôležitým prvkom, ktorý ponúka kľúčovú podporu na úrovni EÚ, je vykonávanie súboru nástrojov proti **zahraničnej manipulácii s informáciami a zahraničnému zasahovaniu**. Ústredným prvkom tohto úsilia je aj podpora digitálnej a mediálnej gramotnosti a kritického myslenia[51].

Boj proti zneužívaniu migrácie ako zbrane

Rusko s pomocou a rozhodnou podporou Bieloruska zámerne využívalo migráciu ako zbraň a nezákonne uľahčovalo migračné toky smerom k vonkajším hraniciam EÚ s cieľom destabilizovať naše spoločnosti a oslabiť jednotu Európskej únie. Takéto konanie ohrozuje nielen národnú bezpečnosť a zvrchovanosť členských štátov, ale aj bezpečnosť a integritu schengenského priestoru a bezpečnosť Únie ako celku. Európska rada vo svojich záveroch z októbra 2024 zdôraznila, že Rusko a Bielorusko, ani žiadna iná krajina nemôžu zneužívať naše hodnoty, vrátane práva na azyl, a oslabovať našu demokraciu.

Ako sa uvádza v oznámení Komisie z roku 2024 o využívaní migrácie ako zbrane, Únia okrem silnej politickej podpory vynaložila aj finančné, operatívne a diplomatické prostriedky, a to aj vo vzťahu ku krajinám pôvodu a tranzitu s cieľom účinne riešiť tieto hrozby[52]. Táto reakcia zahŕňa využívanie nového rámca zriadeného Radou na sankcionovanie jednotlivcov a organizácií zapojených do činností a politík, ako je využívanie migrácie ako zbrane Ruskom,

[49] Súbor volebných nástrojov aktu o digitálnych službách pre koordinátorov digitálnych služieb 2025 https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/900 z 13. marca 2024 o transparentnosti a cielení politickej reklamy (Ú. v. EÚ L, 2024/900, 20.3.2024).
[51] Akčný plán digitálneho vzdelávania (2021 – 2027) – európsky vzdelávací priestor.
[52] COM(2024) 570 final.

a to prostredníctvom zmrazenia aktív a zákazu cestovania[53]. EÚ bude v prípade potreby naďalej využívať tento rámec a podporovať členské štáty v boji proti tejto hrozbe.

Bezpečnosť dopravy

Námorné prístavy, letiská a pozemná infraštruktúra sú kľúčovými vstupnými a výstupnými bodmi. Zohrávajú dôležitú úlohu v hospodárstve a spoločnosti EÚ a sú nevyhnutné pre vojenskú mobilitu. Tieto dopravné uzly a prostriedky sú však aj hlavnými cieľmi vonkajších hrozieb a trestnej činnosti. Nedávne incidenty vrátane narušenia bezpečnostnej ochrany leteckého nákladu a útokov na železničnú infraštruktúru poukazujú na vážne riziká. **Prevádzkovatelia dopravy** môžu byť cieľmi aj nástrojmi pre aktérov s nekalými úmyslami. Existujúce právne nástroje EÚ zlepšili bezpečnostnú ochranu letectva[54], ale vysoká úroveň ohrozenia civilného letectva si vyžaduje prostriedky na predvídanie incidentov a rýchle konzultácie s príslušnými členskými štátmi. Komisia bude spolupracovať s členskými štátmi na zmene existujúcich vykonávacích právnych predpisov v oblasti bezpečnostnej ochrany letectva na účely výmeny utajovaných skutočností o **udalostiach v oblasti bezpečnostnej ochrany letectva**. Komisia okrem toho zváži **regulačné opatrenia** na riešenie nových hrozieb, ako sú **incidenty s leteckým nákladom**, a na posilnenie noriem bezpečnostnej ochrany letectva. To bude zahŕňať aj posilnenie **právnych predpisov v oblasti bezpečnostnej ochrany letectva (AVSEC)** s cieľom umožniť opatrenia okamžitej reakcie a zároveň zachovať bezpečnostný priestor s jednorazovou bezpečnostnou kontrolou na letiskách EÚ.

Komisia bude pri vypracúvaní nadchádzajúcej **stratégie EÚ v oblasti prístavov** vychádzať z **Aliancie prístavov EÚ** a preskúma spôsoby ďalšieho posilnenia právnych predpisov v oblasti námornej bezpečnosti s cieľom účinne riešiť vznikajúce hrozby, zabezpečiť prístavy a zvýšiť bezpečnosť dodávateľského reťazca EÚ. Na tento účel Komisia zabezpečí jej dôsledné vykonávanie a bude pracovať na harmonizácii vnútroštátnych postupov a posilnení kontrol v prístavoch. V nadväznosti na protokoly bezpečnostnej ochrany zavedené pre leteckú nákladnú dopravu bude Komisia spolupracovať s členskými štátmi a súkromným sektorom na rozšírení týchto protokolov s cieľom zabezpečiť námorné dopravné reťazce.

Navrhovaný Colný orgán EÚ bude analyzovať a posudzovať riziká na základe **colných informácií** týkajúcich sa tovaru, ktorý vstupuje do EÚ, vystupuje z nej a prechádza cez ňu, s cieľom podporiť členské štáty pri predchádzaní zneužívaniu medzinárodných dodávateľských reťazcov aktérmi s nekalými úmyslami. V súlade so stratégiou námornej bezpečnosti Európskej únie[55] bude nadchádzajúci **európsky pakt o oceánoch** zohrávať kľúčovú úlohu pri posilňovaní námornej bezpečnosti v morských oblastiach v okolí EÚ aj mimo nej, a to aj prostredníctvom podpory rozširovania viacúčelových námorných operácií a cvičení.

Odolnosť dodávateľských reťazcov

Európa musí znížiť svoju závislosť od technológií tretích krajín, čo môže viesť k závislosti a bezpečnostným rizikám. Komisia má v úmysle zmierniť závislosti od výhradných zahraničných dodávateľov, obmedziť vystavenosť našich dodávateľských reťazcov voči vysokorizikovým dodávateľom a zabezpečiť kritickú infraštruktúru a priemyselnú kapacitu na pôde EÚ, ako sa uvádza v **Kompase konkurencieschopnosti[56]** a **v Dohode o čistom**

[53] Nariadenie Rady (EÚ) 2024/2642 z 8. októbra 2024 o reštriktívnych opatreniach vzhľadom na destabilizačné činnosti Ruska, ST/8744/2024/INIT (Ú. v. EÚ L, 2024/2642, 9.10.2024).
[54] Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva (Ú. v. EÚ L 97, 9.4.2008, s. 72 – 84).
[55] JOIN(2023) 8 final.
[56] COM(2025) 30 final.

priemysle[57]. Komisia bude podporovať **priemyselnú politiku zameranú na vnútornú bezpečnosť** prostredníctvom spolupráce s priemyselnými odvetviami EÚ v kľúčových odvetviach (napr. dopravné uzly, kritické infraštruktúry) s cieľom vytvoriť bezpečnostné riešenia, ako sú detekčné zariadenia, biometrické technológie a drony, ktoré budú zahŕňať bezpečnostné prvky už v štádiu návrhu. Pri **prehodnotení pravidiel EÚ v oblasti verejného obstarávania** Komisia posúdi, či sú bezpečnostné aspekty v smernici o verejnom obstarávaní v oblasti obrany a bezpečnosti z roku 2009[58] dostatočné na riešenie potrieb orgánov presadzovania práva a odolnosti kritických subjektov.

Komisia bude podporovať členské štáty pri **preverovaní priamych zahraničných investícií (PZI)** a obstarávaní vybavenia pre logistické centrá, čím sa zaistí bezpečnosť kritickej infraštruktúry a technológií.

Po tom, ako sa začne uplatňovať **akt o núdzovej situácii na vnútornom trhu a jeho odolnosti (IMERA)**, pomôže EÚ zvládať krízy, ktoré narúšajú kritické dodávateľské reťazce a voľný pohyb tovaru, služieb a osôb. Umožní rýchlu krízovú koordináciu, identifikáciu tovaru a služieb dôležitých v krízovej situácii a poskytne súbor nástrojov na zabezpečenie ich dostupnosti. Okrem toho Komisia v úzkej spolupráci s členskými štátmi navrhne zriadenie **multiagentúrneho mechanizmu varovania v oblasti bezpečnosti dopravy a dodávateľského reťazca** s cieľom zaručiť bezpečnú a včasnú výmenu relevantných informácií potrebných na predvídanie hrozieb a boj proti nim.

Vďaka vykonávaniu aktu o kritických surovinách a aktu o emisne neutrálnom priemysle sa zvýši využívanie kritérií udržateľnosti, odolnosti a európskej preferencie vo verejnom obstarávaní EÚ, čím sa podporí rozvoj vedúcich trhov. Posilnené obchodné väzby, napríklad prostredníctvom partnerstiev v oblasti surovín a partnerstiev pre čistý obchod a investície, pomôžu diverzifikovať dodávateľské reťazce.

Odolnosť a pripravenosť na chemické, biologické, rádiologické a jadrové hrozby

Ruská útočná vojna proti Ukrajine zvýšila riziko **chemických, biologických, rádiologických a jadrových (CBRN) hrozieb**. Komisia bude s cieľom riešiť potenciálne nadobúdanie a zneužívanie CBRN materiálov ako zbraní podporovať členské štáty a partnerské krajiny prostredníctvom špecializovaného výcviku a cvičení. Komisia takisto posilní spôsobilosti v rámci pripravenosti a reakcie v oblasti CBRN prostredníctvom stanovenia prioritných hrozieb, inovačného financovania protiopatrení, kapacít rescEU a vytvárania zásob zdravotníckych protiopatrení v rámci nového **akčného plánu pripravenosti a reakcie na CBRN hrozby**. **Stratégia EÚ pre prostriedky zdravotníckych protiopatrení** bude okrem toho podporovať vývoj zdravotníckych protiopatrení od výskumu po výrobu a distribúciu s cieľom chrániť EÚ pred pandémiami a CBRN hrozbami.

Na základe skúseností s pandémiou COVID-19 EÚ posilnila rámec zdravotnej bezpečnosti[59]. Komisia určuje referenčné laboratóriá EÚ v oblasti verejného zdravia s cieľom posilniť kapacity dohľadu a rýchleho odhaľovania na úrovni EÚ a na vnútroštátnej úrovni. Plán Únie týkajúci sa pripravenosti, prevencie a reakcie v oblasti zdravotnej bezpečnosti bude uverejnený v roku 2025.

Kľúčové opatrenia

Komisia:

[57] COM(2025) 85 final.

[58] Smernica 2009/81/ES o koordinácii postupov pre zadávanie určitých zákaziek na práce, zákaziek na dodávku tovaru a zákaziek na služby verejnými obstarávateľmi alebo obstarávateľmi v oblastiach obrany a bezpečnosti (Ú. v. EÚ L 216, 20.8.2009).

[59] Najmä prostredníctvom nariadenia (EÚ) 2022/2371 o závažných cezhraničných ohrozeniach zdravia.

- **v roku 2025 preskúma a zreviduje akt o kybernetickej bezpečnosti,**
- **vypracuje opatrenia na zaistenie kyberneticky bezpečného využívania cloudových služieb,**
- **v roku 2025 navrhne stratégiu EÚ v oblasti prístavov,**
- **v roku 2026 zreviduje pravidlá verejného obstarávania EÚ v oblasti obrany a bezpečnosti,**
- **v roku 2026 predloží nový akčný plán pripravenosti a reakcie na CBRN hrozby.**

Komisia v spolupráci s členskými štátmi:

- **vyvinie a zavedie európsku kvantovú komunikačnú infraštruktúru (EuroQCI),**
- **zabezpečí účinné presadzovanie aktu o digitálnych službách,**
- **bude bojovať proti využívaniu migrácie ako zbrane,**
- **zriadi systém bezpečnostnej ochrany letectva,**
- **bude pracovať na vytvorení multiagentúrneho mechanizmu varovania v oblasti bezpečnosti dopravy a dodávateľského reťazca.**

Rada sa naliehavo vyzýva, aby:

- **prijala odporúčanie Rady týkajúce sa kybernetickej koncepcie EÚ.**

Členské štáty sa vyzývajú, aby:

- **transponovali a v plnej miere vykonávali smernicu o odolnosti kritických subjektov a smernicu NIS 2.**

5. Zintenzívnenie boja proti závažnej a organizovanej trestnej činnosti

Pomôžeme vykoreniť organizovanú trestnú činnosť navrhnutím prísnejších pravidiel na boj proti organizovaným zločineckým skupinám, a to aj pokiaľ ide o vyšetrovanie, znižovanie zraniteľnosti mladých ľudí v EÚ voči náboru na trestnú činnosť a zintenzívnenie opatrení na obmedzenie prístupu k nástrojom a aktívam trestnej činnosti.

Organizovaná trestná činnosť zneužíva vyvíjajúce sa prostredie a exponenciálne sa šíri. Využíva pokročilé technológie, pôsobí vo viacerých jurisdikciách a má silné prepojenia za hranicami EÚ. Vzhľadom na tieto zložité nadnárodné hrozby je nevyhnutná koordinácia a podpora na úrovni EÚ.

Prevencia trestnej činnosti

Nábor mladých ľudí na organizovanú trestnú činnosť vyvoláva v EÚ čoraz väčšie obavy. Boj proti organizovanej trestnej činnosti si vyžaduje riešenie jej **základných príčin** tým, že sa ponúkne vzdelávanie a alternatívy k páchaniu trestnej činnosti prostredníctvom celospoločenského prístupu. Komisia bude podporovať začlenenie bezpečnostných aspektov do politík EÚ v oblasti vzdelávania, sociálnych vecí, zamestnanosti a regiónov. EÚ bude podporovať **politiky predchádzania trestnej činnosti založené na dôkazoch**[60], ktoré sú prispôsobené miestnym podmienkam.

S cieľom chrániť používateľov online služieb, najmä maloletých, okrem iného pred osobami sexuálne zneužívajúcimi deti, obchodníkmi s ľuďmi a online náborom na trestnú činnosť alebo násilným extrémizmom, sa v opatreniach podľa **aktu o digitálnych službách** vyžaduje, aby poskytovatelia online platforiem prístupných maloletým riadili riziká súvisiace s nezákonným

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

obsahom, vrátane nenávistných prejavov, a konali proti nemu. Komisia plánuje vydať **usmernenia o ochrane maloletých** s cieľom pomôcť poskytovateľom online platforiem pri zabezpečovaní vysokej úrovne súkromia, bezpečnosti a ochrany maloletých online. Usmernenia budú obsahovať súbor odporúčaní pre všetky digitálne služby pôsobiace v Únii s cieľom posilniť ochranu maloletých online. Komisia okrem toho v roku 2025 plánuje podporiť zavedenie **riešenia EÚ na overovanie veku, ktoré bude chrániť súkromie** a ktoré vyplní legislatívnu medzeru, kým nebude koncom roka 2026 k dispozícii peňaženka EUDI. Komisia predloží aj akčný plán proti kybernetickému šikanovaniu.

Komisia bude okrem toho naďalej podporovať dobrovoľnú spoluprácu viacerých zainteresovaných strán s online platformami a inými príslušnými aktérmi, a to aj prostredníctvom internetového fóra EÚ a cielených kódexov správania podľa aktu o digitálnych službách, ako je kódex správania pre boj proti nezákonným nenávistným prejavom online z roku 2025. Cieľom je zvýšiť informovanosť, spoločne reagovať na súčasné a vznikajúce hrozby a vypracovať a vymieňať si osvedčené postupy v oblasti zmierňujúcich opatrení.

Na miestnej úrovni vplyv organizovanej trestnej činnosti zdôrazňuje potrebu regionálnych riešení, aby sa znížila zraniteľnosť jednotlivých regiónov a atraktívnosť nezákonných činností. Program EÚ pre mestá bude riešiť bezpečnostné výzvy v mestách, pričom bude vychádzať z iniciatívy EÚ Mestá proti radikalizácii. Komisia bude podporovať členské štáty pri zvyšovaní bezpečnosti miest a regiónov prostredníctvom Európskeho fondu regionálneho rozvoja.

Základom odolných a súdržných spoločností je intenzívne vzdelávanie a pevné zručnosti. Únia bude prostredníctvom **únie zručností** a **akčného plánu pre integráciu a začlenenie** pracovať na pomoci ľuďom, aby sa stali odolnejšími voči mylným informáciám a dezinformáciám, radikalizácii a náboru na trestnú činnosť.

Kľúčovým cieľom EÚ je ochrana detí pred všetkými formami násilia vrátane trestnej činnosti, fyzického alebo duševného násilia online, ako aj offline. S cieľom riešiť osobitné potreby obzvlášť zraniteľných skupín, ako sú deti, ktoré sú čoraz viac vystavené náboru a radikalizácii, zvádzaniu maloletých a sexuálnemu zneužívaniu detí, kybernetickému šikanovaniu, dezinformáciám a iným hrozbám, EÚ vypracuje **akčný plán na ochranu detí pred trestnou činnosťou**, ktorý bude zahŕňať online aj offline rozmer. Stanoví sa v ňom súdržný a koordinovaný prístup založený na dostupných rámcoch a nástrojoch vrátane budúceho centra EÚ na predchádzanie sexuálnemu zneužívaniu detí a boj proti nemu a ďalších orgánov a agentúr EÚ a navrhnú sa spôsoby, ako napredovať v oblastiach, kde pretrvávajú nedostatky.

Rozloženie zločineckých sietí a ich podporovateľov

Musí sa zintenzívniť boj proti vysokorizikovým zločineckým sieťam, ich vodcom a podporovateľom. Hoci nedávne úspechy sú pozoruhodné[61], zastarané pravidlá a nejednotné vymedzenia zločineckých sietí bránia účinnej reakcii trestného súdnictva a cezhraničnej spolupráci. Komisia preskúma zastarané právne predpisy v tejto oblasti a navrhne obnovený **právny rámec pre organizovanú trestnú činnosť** s cieľom posilniť túto reakciu.

Ako ukazujú Európska prokuratúra a Európsky úrad pre boj proti podvodom (OLAF), k rýchlejšiemu riešeniu **cezhraničných podvodov a trestných činov poškodzujúcich finančné záujmy EÚ** prispieva, ak presadzovanie práva dopĺňajú správne predpisy. Podvodníci v oblasti dotácií sa zameriavajú na odvetvia, ako je energia z obnoviteľných zdrojov, výskumné programy a odvetvie poľnohospodárstva[62]. Komisia preskúma spôsoby koordinácie využívania

[61] Vrátane nedávnych prípadov platformy EMPACT.
[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

trestnoprávnych a administratívnych nástrojov, čím sa posilní spolupráca s Europolom, Eurojustom a Európskou prokuratúrou. Komisia bude takisto naďalej podporovať širšie uplatňovanie **administratívneho prístupu** s cieľom umožniť miestnym a iným správnym orgánom narušiť infiltráciu trestnej činnosti[63].

EÚ pracuje na posilnení svojho právneho rámca pre boj proti **korupcii**[64]. Európsky parlament a Rada by mali urýchlene uzavrieť rokovania o aktualizovanom protikorupčnom rámci, ktorý navrhla Komisia. Komisia predloží protikorupčnú stratégiu EÚ na podporu integrity a posilnenie koordinácie medzi všetkými príslušnými orgánmi a zainteresovanými stranami v tejto oblasti.

Strelné zbrane sú kľúčovým faktorom, ktorý umožňuje rastúce násilie páchané organizovanými zločineckými skupinami. Komisia navrhne spoločné trestnoprávne normy týkajúce sa nedovoleného obchodovania so strelnými zbraňami. Nový **akčný plán EÚ na boj proti nedovolenému obchodovaniu so strelnými zbraňami** sa zameria na ochranu legálneho trhu, obmedzenie trestnej činnosti na základe lepších spravodajských informácií a posilnenie medzinárodnej spolupráce s osobitným zameraním na Ukrajinu a západný Balkán.

Pokiaľ ide o pyrotechnické výrobky, s ktorými sa nezákonne obchoduje a ktoré sa používajú na trestnú činnosť, je nutné zaviesť opatrenia na zlepšenie prevencie a vysledovateľnosti. Komisia v súčasnosti hodnotí smernicu o pyrotechnických výrobkoch a zváži aj **trestné sankcie za nedovolené obchodovanie s pyrotechnickými výrobkami**.

Sledovanie finančných prostriedkov

Sledovanie finančných prostriedkov má zásadný význam v boji proti organizovanej trestnej činnosti a terorizmu, stále je však veľmi náročné. Prepojenie medzi organizovanou trestnou činnosťou a peňažnými tokmi si vyžaduje intenzívne a spoločné úsilie o zastavenie prístupu zločineckých sietí k zdrojom financovania a lepšiu ochranu ľudí, podnikov a verejných rozpočtov.

EÚ posilnila svoje úsilie novými pravidlami boja proti praniu špinavých peňazí vrátane zriadenia **Úradu EÚ pre boj proti praniu špinavých peňazí (AMLA)**[65]. Spolupráca medzi úradom AMLA, úradom OLAF, Európskou prokuratúrou, Eurojustom a Europolom je nevyhnutná na vykonávanie účinných finančných vyšetrovaní. Komisia bude podporovať vytváranie **partnerstiev**, a to tak tých, ktoré uľahčujú spoluprácu medzi agentúrami, ako aj partnerstiev zahŕňajúcich súkromný sektor.

Na odstránenie finančných motívov organizovanej trestnej činnosti je nevyhnutné zabavenie majetku a konfiškácia ziskov z trestnej činnosti. Členské štáty by mali bezodkladne transponovať a v plnej miere využívať nedávno prijaté prísnejšie pravidlá **vymáhania a konfiškácie majetku**[66]. Boj proti paralelným finančným systémom obchádzajúcim rámec EÚ pre boj proti praniu špinavých peňazí vrátane systémov založených na kryptoaktívach si takisto vyžaduje inovatívne opatrenia, výmenu najlepších postupov medzi členskými štátmi a zvýšenú podporu zo strany Europolu a Eurojustu. Komisia preskúma uskutočniteľnosť nového

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Návrh smernice Európskeho parlamentu a Rady o boji proti korupcii, ktorou sa nahrádza rámcové rozhodnutie Rady 2003/568/SVV a Dohovor o boji proti korupcii úradníkov Európskych spoločenstiev alebo úradníkov členských štátov Európskej únie a ktorou sa mení smernica Európskeho parlamentu a Rady (EÚ) 2017/1371, COM(2023) 234 final z 3. mája 2023.

[65] https://www.amla.europa.eu/index_en.

[66] Smernica Európskeho parlamentu a Rady (EÚ) 2024/1260 z 24. apríla 2024 o vymáhaní majetku a konfiškácii (Ú. v. EÚ L, 2024/1260, 2.5.2024).

celoeurópskeho systému na sledovanie ziskov z organizovanej trestnej činnosti a financovania terorizmu a podporí aj včasné a rozšírené informačné toky od **finančných spravodajských jednotiek** k orgánom presadzovania práva. Komisia preskúma spôsoby odstránenia nedostatkov, podporí členské štáty pri budovaní kapacít a bude ďalej pracovať na posilnení spolupráce s tretími krajinami, ktoré páchatelia trestnej činnosti zneužívajú na ilegálne bankové operácie.

Boj proti závažným trestným činom

Boj proti závažným trestným činom si okrem rozkladania zločineckých sietí vyžaduje cielené úsilie. S cieľom posilniť našu schopnosť bojovať proti **online podvodom**, ktoré spôsobujú veľmi významnú finančnú ujmu[67], bude Komisia podporovať preventívne opatrenia a účinnejšie opatrenia na presadzovanie práva a bude spolupracovať s členskými štátmi a zainteresovanými stranami na podpore a ochrane obetí, a to aj prostredníctvom pomoci pri vymáhaní ich finančných prostriedkov. Toto úsilie sa formalizuje v **akčnom pláne boja proti online podvodom**.

Komisia na základe stratégie EÚ pre boj proti **sexuálnemu zneužívaniu detí**[68] na roky 2020 – 2025 podporí spoluzákonodarcov pri finalizácii dvoch legislatívnych návrhov[69] na predchádzanie sexuálnemu zneužívaniu detí online a boj proti nemu a na zabezpečenie väčšej účinnosti opatrení v oblasti presadzovania práva proti sexuálnemu zneužívaniu a vykorisťovaniu detí. Keďže dočasné pravidlá platia do apríla 2026, je nevyhnutné vytvoriť trvalý právny rámec a Komisia nabáda spoluzákonodarcov, aby začali rokovania o návrhu nariadenia, ktorým sa stanovia pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu. Spoluzákonodarcovia sa takisto vyzývajú, aby pokročili v rokovaniach o smernici o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti materiálu obsahujúcemu sexuálne zneužívanie detí, ktorou sa stanovia minimálne pravidlá týkajúce sa vymedzenia trestných činov a sankcií v oblasti sexuálneho vykorisťovania detí.

Polovica najnebezpečnejších zločineckých sietí EÚ je zapojená do násilného **obchodovania s drogami**. Hoci EÚ nedávno posilnila svoj boj proti tejto trestnej činnosti[70], najmä rozšírením mandátu **Agentúry EÚ pre drogy**, sú potrebné ďalšie opatrenia. Komisia bude úzko spolupracovať s členskými štátmi na návrhu novej **protidrogovej stratégie EÚ**. Zreviduje aj **právny rámec týkajúci sa drogových prekurzorov** a navrhne **akčný plán EÚ na boj proti obchodovaniu s drogami** s cieľom narušiť trasy a obchodné modely. **Verejno-súkromné partnerstvo Aliancia prístavov EÚ** zamerané na posilnenie ochrany prístavov sa rozšíri o menšie a vnútrozemské prístavy a zabezpečí presadzovanie pravidiel námornej bezpečnosti. Vzhľadom na závažné miestne vplyvy obchodovania s drogami bude Komisia naďalej podporovať vyváženú, na dôkazoch založenú a multidisciplinárnu protidrogovú politiku, ktorá umožní vyrovnať sa s náhlym prílevom drog, najmä syntetických opioidov.

S cieľom bojovať proti vykorisťovaniu ľudí prijala EÚ nové pravidlá[71] a zavedie **obnovenú stratégiu EÚ v oblasti boja proti obchodovaniu s ľuďmi** na roky 2026 – 2030, ktorá sa bude vzťahovať na všetky fázy od prevencie až po trestné stíhanie so zameraním na podporu obetí na úrovni EÚ aj na medzinárodnej úrovni.

[67] Global Anti-Scam Report 2024.
[68] COM(2020) 607 final.
[69] COM(2022) 209 final a COM(2024) 60 final.
[70] COM(2023) 641 final.
[71] Smernica (EÚ) 2024/1712 z 13. júna 2024, ktorou sa mení smernica 2011/36/EÚ o prevencii obchodovania s ľuďmi a boji proti nemu a o ochrane obetí obchodovania (Ú. v. EÚ L, 2024/1712, 24.6.2024).

V boji proti **prevádzačstvu** bude Komisia viesť úsilie s kľúčovými partnermi prostredníctvom novej globálnej aliancie na boj proti prevádzačstvu v spolupráci s Europolom, Eurojustom a agentúrou Frontex, a to aj v online rozmere. Návrhy Komisie týkajúce sa boja proti prevádzačstvu[72] by sa mali bezodkladne prijať a vykonať. Komisia okrem toho po prijatí **súboru nástrojov pre prevádzkovateľov dopravy**[73] zvýšila dosah na zahraničné orgány a prevádzkovateľov a bude naďalej spolupracovať s leteckým priemyslom a organizáciami civilného letectva[74] s cieľom zvýšiť informovanosť o prevádzačstve migrantov leteckou dopravou[75].

Trestné činy proti životnému prostrediu ohrozujú životné prostredie, verejné zdravie a hospodárstva z dlhodobého hľadiska. Komisia bude podporovať členské štáty pri vykonávaní smernice o trestných činoch proti životnému prostrediu[76] a posilní operačné siete a opatrenia v tejto oblasti[77]. Zásadné je dôsledné presadzovanie. Okrem toho nedávno prijatý Dohovor Rady Európy o ochrane životného prostredia prostredníctvom trestného práva[78] pomôže zabezpečiť silné a porovnateľné úsilie v boji proti trestným činom proti životnému prostrediu v Európe aj mimo nej.

Reakcia trestného súdnictva

Trestná činnosť a terorizmus môžu zasiahnuť všetkých, a preto je nevyhnutné podporovať a chrániť práva **obetí** s cieľom znížiť škody a zvýšiť celkovú bezpečnosť a dôveru v orgány. Na základe smernice o právach obetí Komisia zavedie novú **stratégiu EÚ v oblasti práv obetí**.

Trestnoprávne systémy EÚ potrebujú účinné nástroje na riešenie vznikajúcich hrozieb. Na dosiahnutie tohto cieľa Komisia spustila **fórum na vysokej úrovni o budúcnosti trestnoprávnych systémov EÚ**. Na tomto fóre sa stretávajú členské štáty, Európsky parlament, agentúry a orgány EÚ a ďalšie príslušné zainteresované strany. Jeho cieľom je diskutovať o spôsoboch, ako zabezpečiť, aby naše trestnoprávne systémy zostali účinné, spravodlivé a odolné v kontexte vyvíjajúcich sa výziev, a zároveň posilniť justičnú spoluprácu a vzájomnú dôveru, a to aj prostredníctvom digitalizácie[79].

Kľúčové opatrenia

Komisia:

- **v roku 2026 predloží legislatívny návrh modernizovaných pravidiel o organizovanej trestnej činnosti,**
- **v roku 2025 predloží legislatívny návrh na revíziu právneho rámca pre drogové prekurzory,**
- **v roku 2025 predloží návrh spoločných trestnoprávnych noriem týkajúcich sa nedovoleného obchodovania so strelnými zbraňami,**
- **posúdi potrebu revízie smerníc o pyrotechnických výrobkoch a výbušninách na civilné použitie,**

[72] COM(2023) 755 final a COM(2023) 754 final.
[73] Súbor nástrojov na riešenie využívania komerčných dopravných prostriedkov na uľahčenie nelegálnej migrácie do EÚ.
[74] Vrátane Medzinárodnej organizácie civilného letectva (ICAO).
[75] Komisia bude podporovať aj finalizáciu nariadenia o opatreniach proti prevádzkovateľom dopravy, ktorí uľahčujú alebo vykonávajú obchodovanie s ľuďmi alebo prevádzačstvo migrantov, COM(2021) 753 final.
[76] Smernica Európskeho parlamentu a Rady (EÚ) 2024/1203 z 11. apríla 2024 o ochrane životného prostredia prostredníctvom trestného práva (Ú. v. EÚ L, 2024/1203, 30.4.2024).
[77] Európska sieť pre implementáciu a vymáhanie environmentálneho práva (IMPEL), Európska sieť prokurátorov pre životné prostredie (ENPE), neformálna sieť na boj proti trestným činom proti životnému prostrediu (EnviCrimeNet) a Fórum sudcov Európskej únie pre životné prostredie (EUFJE).
[78] Výbor expertov na ochranu životného prostredia prostredníctvom trestného práva (PC-ENV) – Európsky výbor pre problémy trestnej činnosti.
[79] Najmä prostredníctvom zriadenia systému komunikácie v oblasti elektronickej justície prostredníctvom výmeny údajov online (eCODEX) a európskeho informačného systému registrov trestov pre štátnych príslušníkov tretích krajín (ECRIS-TCN).

- **posúdi potrebu ďalšieho posilnenia európskeho vyšetrovacieho príkazu a európskeho zatykača,**
- **v roku 2026 predloží novú stratégiu EÚ v oblasti boja proti obchodovaniu s ľuďmi,**
- **v roku 2026 predloží novú stratégiu EÚ v oblasti práv obetí,**
- **do roku 2027 predloží akčný plán EÚ na ochranu detí pred trestnou činnosťou,**
- **v roku 2025 predloží akčný plán EÚ na boj proti obchodovaniu s drogami,**
- **v roku 2026 predloží akčný plán EÚ na boj proti nedovolenému obchodovaniu so strelnými zbraňami,**
- **od roku 2025 bude postupne rozširovať Alianciu prístavov EÚ,**
- **v roku 2026 prijme usmernenia na základe aktu o digitálnych službách o ochrane maloletých,**
- **v roku 2026 predloží akčný plán EÚ proti kybernetickému šikanovaniu.**

Členské štáty sa vyzývajú, aby:

- **do konca roka 2026 plne transponovali nové pravidlá vymáhania a konfiškácie majetku a využívali ich plný potenciál,**
- **uplatňovali administratívny prístup v boji proti infiltrácii trestnej činnosti,**
- **vytvárali verejno-súkromné partnerstvá v boji proti praniu špinavých peňazí,**
- **transponovali a plne vykonávali smernicu o predchádzaní násiliu na ženách a domácemu násiliu a boji proti nemu.**

Európsky parlament a Rada sa vyzývajú, aby:

- **pokročili v rokovaniach o nariadení, ktorým sa stanovujú pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu, a o smernici o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti materiálu obsahujúcemu sexuálne zneužívanie detí,**
- **ukončili rokovania o smernici o boji proti korupcii.**

6. Boj proti terorizmu a násilnému extrémizmu

Zavedieme komplexný program boja proti terorizmu s cieľom predchádzať radikalizácii, zabezpečiť online a verejné priestory, obmedziť možnosti financovania a reagovať na útoky, keď k nim dôjde.

Riziko teroristickej hrozby v EÚ je naďalej vysoké. Úzko súvisí s účinkami presahovania geopolitických udalostí, nových technológií a nových prostriedkov financovania terorizmu. Musíme zabezpečiť, aby bola EÚ dobre vybavená na predvídanie hrozieb, predchádzanie radikalizácii (offline aj online), ochranu občanov a verejných priestorov pred útokmi a účinnú reakciu na útoky, keď k nim dôjde. V roku 2025 sa predloží **nový program EÚ na predchádzanie terorizmu a násilnému extrémizmu a boj proti nim** s cieľom stanoviť budúce opatrenia EÚ. V súlade s novým programom EÚ a západný Balkán v roku 2025 podpíšu nový **spoločný akčný plán** na predchádzanie terorizmu a násilnému extrémizmu a boj proti nim.

Predchádzanie radikalizácii a ochrana ľudí na internete

Podobne ako v boji proti organizovanej trestnej činnosti sa boj proti terorizmu a násilnému extrémizmu začína **riešením jeho základných príčin**. **Znalostné centrum EÚ pre prevenciu radikalizácie** zintenzívni svoju podporu odborníkom z praxe a tvorcom politík prostredníctvom nového **komplexného súboru nástrojov na prevenciu**, ktorý umožní včasnú identifikáciu a zásahy

zamerané na zraniteľné osoby, najmä maloletých. Keďže k radikalizácii často dochádza vo väzniciach, Komisia vydá nové odporúčania s cieľom podporiť členské štáty pri riešení tejto otázky.

Teroristi a násilní extrémisti využívajú online platformy na šírenie teroristického a škodlivého obsahu a zhromažďovanie finančných prostriedkov a nábor. Zraniteľní používatelia, najmä maloletí, sa radikalizujú na internete alarmujúcou rýchlosťou. **Nariadenie o teroristickom obsahu online** bolo nápomocné v boji proti šíreniu teroristického obsahu online, čo umožnilo rýchle odstránenie najhoršieho a najnebezpečnejšieho materiálu[80]. Komisia v súčasnosti hodnotí jeho fungovanie a posúdi, ako čo najlepšie posilniť tento rámec.

Krízový protokol EÚ pre spoločnú a rýchlu reakciu orgánov presadzovania práva a technologického priemyslu v súvislosti s teroristickým útokom sa zmení tak, aby sa zabezpečila škálovateľnosť a flexibilita s cieľom reagovať na rastúci online rozmer teroristických útokov. Internetové fórum EÚ bude aj naďalej hlavným prostriedkom dobrovoľnej spolupráce s technologickým priemyslom v boji proti teroristickému a škodlivému obsahu na internete. Komisia sa okrem toho zapája do medzinárodných iniciatív, ako je nadácia Christchurch Call Foundation a globálne internetové fórum na boj proti terorizmu (GIFCT).

Boj proti financovaniu terorizmu

Teroristi financujú svoje činnosti kampaňami hromadného financovania, kryptoaktívami, prostredníctvom neobánk alebo online platobných platforiem. Orgány presadzovania práva musia tieto finančné toky odhaľovať a vyšetrovať. To si vyžaduje prostriedky, nástroje a odborné znalosti. Kľúčovú úlohu zohráva **sieť finančných vyšetrovateľov na boj proti terorizmu**. Komisia preskúma vytvorenie **nového celoúnijného systému na sledovanie financovania terorizmu**, ktorý by zahŕňal transakcie v rámci EÚ a SEPA, prevody kryptoaktív, online a elektronické platby, a dopĺňal tak dohodu o Programe na sledovanie financovania terorizmu (TFTP) medzi EÚ a USA.

Rozpočet EÚ musí byť **chránený pred zneužitím na podporu radikálnych/extrémistických názorov** v členských štátoch. Revidované **nariadenie o rozpočtových pravidlách** teraz zahŕňa odsúdenie za „podnecovanie k diskriminácii, nenávisti alebo násiliu“ ako dôvod na vylúčenie z financovania EÚ. Komisia bude naďalej skúmať najlepší spôsob plného využitia súboru nástrojov, a to aj pri výbere potenciálnych prijímateľov. Ochrana rozpočtu EÚ závisí aj od úzkej spolupráce a výmeny informácií s vnútroštátnymi orgánmi, agentúrami a orgánmi EÚ.

Ochrana pred útokmi

Okrem investícií do predchádzania radikalizácii je dôležitou zložkou ochrany občanov obmedzenie prostriedkov teroristov a zločincov na páchanie útokov. Je potrebné prijať opatrenia týkajúce sa nástrojov, ktoré používajú teroristi, ako aj ochrany cieľov, ktorým hrozí útok.

Komisia okrem opatrení týkajúcich sa strelných zbraní **preskúma aj pravidlá** týkajúce sa **prekurzorov výbušnín** s cieľom zahrnúť vysokorizikové chemické látky. **Verejné priestory** sú aj naďalej najbežnejšími cieľmi teroristických útokov, najmä pre osamelých aktérov. V záujme ochrany občanov sa posilní **poradný program EÚ v oblasti ochrany bezpečnosti**, v rámci ktorého sa budú posúdenia zraniteľnosti verejných priestorov, kritickej infraštruktúry a vysokorizikových udalostí vykonávať na žiadosť členských štátov a ktorý bude financovaný z rozpočtu EÚ v rámci Fondu pre vnútornú bezpečnosť. EÚ sa bude snažiť rozšíriť dostupné

[80] Do 31. decembra 2024 bolo vydaných 1 426 príkazov na odstránenie s cieľom odstrániť teroristický obsah alebo zablokovať prístup k nemu, z ktorých veľká väčšina sa zameriava na džihádistický teroristický obsah, ale aj pravicový teroristický obsah.

finančné prostriedky na ochranu verejného priestoru. Komisia ponúka podporu orgánom členských štátov a súkromným prevádzkovateľom prostredníctvom špecializovaných usmernení a nástrojov, ako je vedomostné centrum pre ochranu verejných priestorov[81], a od roku 2020 už bolo na podporu ochrany verejného priestoru sprístupnených 70 miliónov EUR.

Komisia takisto preskúma zavedenie požiadaviek na organizácie, aby zvážili alebo uplatňovali bezpečnostné opatrenia na verejne prístupných miestach prostredníctvom spolupráce s miestnymi orgánmi a súkromnými partnermi.

Vzhľadom na zjavné zraniteľné miesta bude **stratégia EÚ pre boj proti antisemitizmu a podporu židovského života na roky 2021 – 2030** naďalej usmerňovať opatrenia Komisie na ochranu židovskej komunity. Komisia rovnako zabezpečí zavedenie vhodných nástrojov na podporu členských štátov v boji proti **nenávisti voči moslimom**.

Čoraz väčšiu bezpečnostnú výzvu predstavuje používanie **dronov** na špionáž a útoky. Komisia vypracuje **harmonizovanú metodiku testovania protidronových systémov**, zriadi **centrum excelentnosti na obranu proti dronom** a posúdi potrebu harmonizácie právnych predpisov a postupov členských štátov[82].

Zahraniční teroristickí bojovníci

V záujme identifikácie zahraničných teroristických bojovníkov na vonkajších hraniciach EÚ, ktorí sa vracajú alebo vstupujú na územie EÚ, sú potrebné údaje o osobách, ktoré predstavujú teroristickú hrozbu. Na tento účel Komisia spolu s Europolom posilní svoju **spoluprácu s kľúčovými tretími krajinami s cieľom získať biografické a biometrické údaje o osobách, ktoré by mohli predstavovať teroristickú hrozbu**, vrátane zahraničných teroristických bojovníkov, ktoré sa potom môžu vložiť do Schengenského informačného systému v plnom súlade s platnými právnymi rámcami EÚ a vnútroštátnymi právnymi rámcami. Je preto veľmi dôležité, aby členské štáty využívali všetky existujúce nástroje. To zahŕňa vloženie všetkých relevantných informácií do **SIS**, zlepšenie biometrických kontrol a vykonávanie povinných systematických kontrol všetkých osôb na vonkajších hraniciach EÚ[83]. Orgány hraničnej kontroly členských štátov budú pri identifikácii a posudzovaní rizika podozrivých pohybov potenciálnych zahraničných teroristických bojovníkov naďalej môcť využívať **spoločné ukazovatele rizika** vypracované agentúrou Frontex.

Okrem toho s cieľom zabezpečiť, aby si členské štáty zachovali prístup k **dôkazom z bojiska** zhromaždeným vyšetrovacím tímom OSN na podporu vyvodenia zodpovednosti za zločiny spáchané Dá'išom/ISIL-om (UNITAD) na účely stíhania zahraničných teroristických bojovníkov, Komisia spolu s Eurojustom posúdi možnosť uchovávať tieto dôkazy v databáze dôkazov najzávažnejších medzinárodných trestných činov Eurojustu. Nový Európsky **justičný register na boj proti terorizmu** bude navyše naďalej podporovať justičné orgány členských štátov pri rýchlom zisťovaní cezhraničných prepojení v prípadoch terorizmu.

Kľúčové opatrenia

Komisia:

- **v roku 2025 prijme nový program EÚ na predchádzanie terorizmu a násilnému extrémizmu a boj proti nim,**

[81] Vedomostné centrum pre ochranu verejných priestorov.

[82] V nadväznosti na súbor kľúčových opatrení uvedených v oznámení o boji proti dronom z roku 2023, COM(2023) 659 final.

[83] V plnom súlade s Kódexom schengenských hraníc a nariadením o preverovaní.

- **v roku 2025 s partnermi zo západného Balkánu podpíše nový spoločný akčný plán na predchádzanie terorizmu a násilnému extrémizmu a boj proti nim,**
- **so znalostným centrom EÚ vypracuje nový komplexný súbor nástrojov v oblasti prevencie,**
- **v roku 2026 vyhodnotí uplatňovanie nariadenia o teroristickom obsahu online,**
- **v roku 2025 zmení krízový protokol EÚ,**
- **v roku 2026 predloží legislatívny návrh na revíziu nariadenia o uvádzaní prekurzorov výbušnín na trh a ich používaní,**
- **preskúma uskutočniteľnosť nového celoúnijného systému na sledovanie financovania terorizmu.**

Členské štáty sa vyzývajú, aby:

- **zlepšili biometrické kontroly a vykonávali povinné systematické kontroly na vonkajších hraniciach EÚ,**
- **v plnom rozsahu využívali Európsky justičný register na boj proti terorizmu.**

7. EÚ ako silný globálny aktér v oblasti bezpečnosti

V záujme posilnenia bezpečnosti EÚ zintenzívnime operačnú spoluprácu prostredníctvom partnerstiev s kľúčovými regiónmi, ako sú partneri zapojení do procesu rozširovania a susedskí partneri, Latinská Amerika a stredozemský región. Bezpečnostné záujmy EÚ sa zohľadnia v medzinárodnej spolupráci, a to aj s využitím nástrojov EÚ.

V posledných rokoch sa ukázalo pevné prepojenie medzi vonkajšou a vnútornou bezpečnosťou EÚ. Ruská útočná vojna proti Ukrajine, konflikt v Gaze, situácia v Sýrii a vznikajúce konflikty na celom svete mali závažný dosah na vnútornú bezpečnosť EÚ. S cieľom bojovať proti vplyvu globálnej nestability na svoju vnútornú bezpečnosť musí **EÚ aktívne brániť svoje bezpečnostné záujmy** riešením vonkajších hrozieb, narúšaním trás nezákonného obchodovania a ochranou koridorov strategického záujmu, ako sú obchodné trasy. EÚ bude zároveň aj naďalej silným spojencom partnerských krajín, pričom bude spolupracovať na posilnení globálnej bezpečnosti a budovaní vzájomnej odolnosti voči hrozbám.

EÚ podnikla v posledných rokoch významné kroky na posilnenie svojej bezpečnostnej spolupráce. Uzavrela operačné dohody o presadzovaní práva a justičnej spolupráci, ako aj iné typy dohôd s partnerskými krajinami. Aktívne sa usiluje o uzavretie dodatočných medzinárodných dohôd v súlade so smernicami Rady na rokovania a o uskutočňovanie iniciatív zameraných na budovanie kapacít, ktoré podporujú agentúry a orgány EÚ. Zásadný význam pri posilňovaní bezpečnosti s partnerskými krajinami má aj Nástroj susedstva a rozvojovej a medzinárodnej spolupráce – Globálna Európa (NDICI – Globálna Európa).

Základným kameňom posilnenia globálnej bezpečnosti je **medzinárodný poriadok založený na pravidlách**. Na posilnenie tohto úsilia sú nevyhnutné bezpečnostné dialógy vrátane tematických dialógov. Vykonávanie **Strategického kompasu pre bezpečnosť a obranu** spolu s rámcami dvojstrannej a mnohostrannej spolupráce, ako sú dohody o stabilizácii a pridružení a dohody o pridružení, a spolupráca s organizáciami, ako sú OSN a NATO, majú zásadný význam pre rozvoj účinných bezpečnostných riešení. EÚ bude naďalej zohrávať svoju úlohu na multilaterálnych fórach[84] a posilní spoluprácu s príslušnými medzinárodnými

[84] Globálne fórum pre boj proti terorizmu, globálna koalícia na boj proti Dá'iš, globálne internetové fórum na boj proti terorizmu (GIFCT), nadácia Christchurch Call Foundation, Globálna koalícia na riešenie hrozieb syntetických drog.

a regionálnymi organizáciami a rámcami vrátane NATO, Organizácie Spojených národov, Rady Európy, Interpolu, G7, OBSE a občianskej spoločnosti.

Regionálna spolupráca

Prioritou je, aby EÚ naďalej neochvejne podporovala **Ukrajinu** a posilňovala bezpečnosť a odolnosť **krajín zapojených do procesu rozširovania EÚ**, čo je politickou a geostrategickou nevyhnutnosťou. Podpora bezpečnosti EÚ by mala ísť ruka v ruke s **urýchlenou integráciou kandidátskych krajín** do **bezpečnostnej architektúry EÚ** súbežne s konsolidáciou ich regionálnej spolupráce. Komisia využije politiku rozširovania EÚ na podporu kapacít kandidátskych krajín a potenciálnych kandidátov na členstvo v EÚ reagovať na hrozby, na zintenzívnenie operačnej spolupráce a výmenu informácií, ako aj zabezpečenie súladu so zásadami, právnymi predpismi a nástrojmi EÚ. Zásadný význam pre posilnenie bezpečnosti v kandidátskych krajinách aj na území potenciálnych kandidátov má nástroj predvstupovej pomoci (IPA III), ako aj nástroje pre Ukrajinu, Moldavsko a západný Balkán.

EÚ bude takisto ďalej integrovať do bezpečnostnej architektúry EÚ **partnerov zo susedstva**. Prostredníctvom **nového paktu pre Stredozemie** a nadchádzajúceho **strategického prístupu k Čiernemu moru** sa Únia bude usilovať pokračovať v budovaní regionálnej spolupráce a dvojstranných strategických komplexných partnerstiev s bezpečnostným rozmerom a v prípade potreby uskutoční pravidelné dialógy na vysokej úrovni o bezpečnosti. Posilní sa operačná spolupráca s krajinami severnej Afriky, **Blízkeho východu a Perzského zálivu**, a to najmä v súvislosti s bojom proti terorizmu, bojom proti praniu špinavých peňazí, bojom proti nedovolenému obchodovaniu so strelnými zbraňami a bojom proti výrobe a pašovaniu drog, predovšetkým captagonu.

S cieľom riešiť nárast teroristickej a trestnej činnosti a jej potenciálne účinky presahovania v **subsaharskej Afrike**, **najmä v regióne Sahel, Africkom rohu** a **západnej Afrike**, EÚ posilní podporu Africkej únii, regionálnym hospodárskym spoločenstvám a krajinám v regióne. V súlade so stratégiou námornej bezpečnosti EÚ[85] posilní EÚ spoluprácu v **Guinejskom zálive, Červenom mori a Indickom oceáne** s cieľom bojovať proti nezákonnému obchodovaniu a pirátstvu, a to podporou spolupráce v rámci Afriky a regiónu a za pomoci koordinovanej námornej prítomnosti EÚ a Námorného centra analýz a operácií (narkotiká) (MAOC-N).

Pokiaľ ide o **Latinskú Ameriku a Karibik**, EÚ posilní operačnú spoluprácu s cieľom rozložiť a stíhať vysokorizikové zločinecké siete a narušať nezákonné činnosti a trasy, pričom posilní rámce spolupráce, ako je Výbor Latinskej Ameriky pre vnútornú bezpečnosť (EU-CLASI) a mechanizmus koordinácie a spolupráce v oblasti drog EÚ – CELAC. Medzi priority budú patriť odolnosť a partnerstvá logistických centier a prístup založený na sledovaní peňazí. EÚ bude ďalej podporovať rozvoj Policajného spoločenstva amerického kontinentu (AMERIPOL), aby sa stal regionálnym ekvivalentom Europolu, a posilní justičnú spoluprácu medzi členskými štátmi a týmto regiónom. EÚ bude spolupracovať aj s **Južnou a Strednou Áziou** na spoločných bezpečnostných výzvach týkajúcich sa terorizmu, nedovoleného obchodovania s tovarom vrátane drog, obchodovania s ľuďmi a prevádzačstva migrantov.

EÚ bude okrem toho podporovať rámce regionálnej spolupráce v tretích krajinách s cieľom ďalej im pomáhať pri zastavení nedovoleného obchodovania pri zdroji v súlade so zásadou spoločnej zodpovednosti za celý dodávateľský reťazec trestnej činnosti. Okrem toho EÚ prispeje k posilneniu bezpečnosti logistických centier v zahraničí koordináciou **spoločných inšpekcií v prístavoch tretích krajín**.

[85] JOIN(2023) 8 final.

Operatívna spolupráca

Stratégia **Global Gateway** bude podporovať projekty udržateľnej a kvalitnej infraštruktúry v digitálnom, klimatickom a energetickom, dopravnom, zdravotníckom, vzdelávacom a výskumnom sektore. Komisia teraz v prípade potreby zahrnie bezpečnostné aspekty do budúcich investícií stratégie Global Gateway. Bude sa to týkať iniciatív, ktoré majú zásadný význam pre strategickú autonómiu EÚ a jej partnerských krajín, ako sú projekty v oblasti infraštruktúry zahŕňajúce posúdenia bezpečnosti a opatrenia na zmiernenie rizika.

Komisia bude pokračovať v uzatváraní ďalších **dohôd medzi EÚ a tretími krajinami o spolupráci s Europolom a Eurojustom**, najmä s krajinami Latinskej Ameriky.

Jedným z najúčinnejších prostriedkov na posilnenie operačnej spolupráce je okrem toho aktívna účasť krajín mimo EÚ na platforme **EMPACT**. EÚ bude naďalej podporovať zapojenie tretích krajín, najmä západného Balkánu, východného susedstva, subsaharskej Afriky, severnej Afriky, Blízkeho východu, Latinskej Ameriky a Karibiku, do tohto rámca. Ďalším nástrojom na zintenzívnenie spolupráce s tretími krajinami v oblasti boja proti trestnej činnosti sú operačné pracovné skupiny medzi členskými štátmi koordinované Europolom, na ktorých sa môžu zúčastniť tretie krajiny. Cieľom Komisie je tiež ukončiť rokovania o medzinárodnej dohode[86] medzi **EÚ a Interpolom**, zabezpečiť jednotnejší prístup k globálnym bezpečnostným hrozbám a bojovať proti nadnárodnej trestnej činnosti.

Únia **musí byť prítomná v teréne v rámci prístupu Tímu Európa**. Špecializovaní zamestnanci Únie a členských štátov zohrávajú kľúčovú úlohu pri zabezpečovaní dobrej informovanosti, koordinácie a reakcie na vonkajšiu činnosť Únie. Komisia s cieľom posunúť tento prístup na vyššiu úroveň s podporou vysokého predstaviteľa pre zahraničné veci a bezpečnostnú politiku posilní **styčné siete** a uľahčí nasadenie regionálnych **styčných dôstojníkov Europolu a Eurojustu** v súlade s operačnými potrebami členských štátov.

EÚ sa bude usilovať o užšiu operačnú spoluprácu v oblasti presadzovania práva a justičnú spoluprácu, podporovať výmenu informácií v reálnom čase a spoločné operácie prostredníctvom **spoločných vyšetrovacích tímov** v tretích krajinách s podporou Europolu a Eurojustu. Komisia bude podporovať aj členské štáty pri zriaďovaní **spoločných centier pre syntézu informácií**, ktoré budú združovať odborníkov a miestne orgány presadzovania práva v strategických tretích krajinách.

Nástroje spoločnej zahraničnej a bezpečnostnej politiky (SZBP)

Naplno sa využije aj potenciál **misií spoločnej bezpečnostnej a obrannej politiky** (SBOP) na lepšiu identifikáciu a riešenie vonkajších hrozieb pre vnútornú bezpečnosť EÚ v súlade s mandátmi týchto misií stanovenými Radou. V záujme budovania kapacít tretích krajín budú vysoký predstaviteľ pre zahraničné veci a bezpečnostnú politiku a Komisia podporovať akcie SBOP špecializovanými nástrojmi financovania a preskúmajú všetky vhodné spôsoby financovania.

Reštriktívne opatrenia EÚ sú dobre zavedeným nástrojom SZBP, ktorý sa používa aj na boj proti terorizmu. Na základe návrhov vysokého predstaviteľa pre zahraničné veci a bezpečnostnú politiku, členských štátov alebo Komisie by Rada mohla posúdiť, ako by sa existujúce autonómne reštriktívne opatrenia EÚ (zoznam teroristov, ktorý zostavila EÚ) mohli stať účinnejšími, operatívnejšími a pružnejšími. Okrem toho by mohli zvážiť preskúmanie ďalších reštriktívnych opatrení zameraných na zločinecké siete v súlade s cieľmi SZBP.

Vízová politika a výmena informácií

Vízová politika EÚ je kľúčovým nástrojom spolupráce s tretími krajinami a zabezpečenia našich hraníc prostredníctvom kontroly vstupu do EÚ a stanovenia príslušných podmienok. Komisia

[86] Rozhodnutie Rady (EÚ) 2021/1312 z 19. júla 2021 a rozhodnutie Rady (EÚ) 2021/1313 z 19. júla 2021.

plne začlení **bezpečnostné aspekty do vízovej politiky EÚ** prostredníctvom nadchádzajúcej stratégie EÚ v oblasti vízovej politiky. Komisia bude spolupracovať so spoluzákonodarcami na prijatí návrhu na revíziu a zefektívnenie mechanizmu pozastavenia oslobodenia od vízovej povinnosti, najmä v konkrétnych prípadoch zneužitia bezvízového režimu[87]. Tretie krajiny sa budú nabádať, aby si vymieňali informácie o osobách, ktoré môžu predstavovať bezpečnostné hrozby, ktoré budú vložené do informačných systémov a databáz EÚ.

S cieľom dosiahnuť koordináciu politík, zvýšiť úsilie a dosiahnuť účinnejšiu, rýchlejšiu a plynulejšiu spoluprácu bude Komisia pracovať na vytvorení **mechanizmov toku údajov** a preskúma spôsoby, ako **zlepšiť výmenu informácií** na účely presadzovania práva a riadenia hraníc s dôveryhodnými tretími krajinami v súlade so základnými právami a pravidlami ochrany údajov.

Kľúčové opatrenia

Komisia:

- **uzavrie medzinárodné dohody medzi EÚ a prioritnými tretími krajinami o spolupráci s Europolom a Eurojustom,**
- **bude podporovať účasť partnerských krajín na platforme EMPACT s cieľom bojovať proti organizovanej trestnej činnosti a terorizmu,**
- **bude podporovať agentúry a orgány EÚ pri vytváraní a posilňovaní pracovných dohôd s partnerskými krajinami,**
- **bude ďalej zohľadňovať bezpečnostné aspekty vo vízovej politike EÚ prostredníctvom nadchádzajúcej vízovej stratégie,**
- **posilní výmenu informácií s dôveryhodnými tretími krajinami na účely presadzovania práva a riadenia hraníc.**

Komisia v spolupráci s vysokým predstaviteľom pre zahraničné veci:

- **bude v plnej miere využívať civilné misie spoločnej bezpečnostnej a obrannej politiky (SBOP),**
- **do roku 2027 bude koordinovať spoločné inšpekcie v prístavoch tretích krajín.**

Komisia v spolupráci s vysokým predstaviteľom pre zahraničné veci a členskými štátmi:

- **posilní styčné siete a spoluprácu v rámci prístupu Tímu Európa,**
- **od roku 2025 zriadi spoločné operačné tímy a centrá pre syntézu informácií v tretích krajinách.**

Európsky parlament a Rada sa vyzývajú, aby:

- **dokončili rokovania o revízii mechanizmu pozastavenia oslobodenia od vízovej povinnosti.**

8. Záver

Vo svete plnom neistoty je potrebné zlepšiť schopnosť Únie predvídať bezpečnostné hrozby, predchádzať im a reagovať na ne.

Nestačí len reagovať na krízy, keď k nim dôjde. Musíme zvýšiť naše povedomie, mať úplný obraz o hrozbách, ktoré sa vyvíjajú, a zabezpečiť, aby naše nástroje a spôsobilosti boli na túto úlohu dostatočne pripravené.

Komplexný súbor opatrení, ktoré sú podrobne opísané v tejto stratégii, pomôže vytvoriť silnejšiu Úniu vo svete: Úniu, ktorá je schopná predvídať vlastné bezpečnostné potreby,

[87] COM(2023) 642.

plánovať ich a starať sa o ne, ktorá dokáže účinne reagovať na hrozby pre svoju vnútornú bezpečnosť a vyvodiť zodpovednosť voči páchateľom a ktorá chráni svoje otvorené, slobodné a prosperujúce spoločnosti a demokracie.

To si vyžaduje zásadnú zmenu nášho zmýšľania o vnútornej bezpečnosti. Budeme pracovať na podpore novej bezpečnostnej kultúry EÚ, v ktorej sa bezpečnostné aspekty zohľadňujú vo všetkých našich právnych predpisoch, politikách a programoch – od ich návrhu až po ich vykonávanie – a kde nám spolupráca medzi jednotlivými oblasťami politiky umožňuje uskutočňovať prelomové kroky.

Nie je to úloha len jednej inštitúcie, vlády alebo aktéra. Je to spoločné úsilie celej Európy.