Rada
Evropské unie

Brusel 3. dubna 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	

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	2. dubna 2025
Příjemce:	Thérèse BLANCHETOVÁ, generální tajemnice Rady Evropské unie
Č. dok. Komise:	COM(2025) 148 final
Předmět:	SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ ProtectEU: Evropská strategie vnitřní bezpečnosti

Delegace naleznou v příloze dokument COM(2025) 148 final.

Příloha: COM(2025) 148 final

EVROPSKÁ
KOMISE

Ve Štrasburku dne 1.4.2025
COM(2025) 148 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ

ProtectEU: Evropská strategie vnitřní bezpečnosti

1. ProtectEU: Evropská strategie vnitřní bezpečnosti

Bezpečnost je základním kamenem, na němž stojí všechny naše svobody. Demokracie, právní stát, základní práva, dobré životní podmínky Evropanů, konkurenceschopnost a prosperita – to vše závisí na naší schopnosti zajistit základní bezpečnostní záruky. V nové éře bezpečnostních hrozeb, v níž dnes žijeme, závisí schopnost členských států EU zajistit bezpečnost svých občanů více než kdy dříve na **jednotném evropském přístupu k ochraně naší vnitřní bezpečnosti**. V měnící se geopolitické situaci musí Evropa i nadále naplňovat svůj neochvějný závazek zachování míru.

První kroky k vybudování evropského bezpečnostního aparátu byly již učiněny. V posledním desetiletí jsme Unii vybavili lepšími kolektivními mechanismy pro přijímání opatření v oblasti prosazování práva a justiční spolupráce, ochrany hranic, boje proti závažné a organizované trestné činnosti, boje proti terorismu a násilnému extremismu a ochrany fyzické i digitální kritické infrastruktury EU. Klíčové zůstává řádné provádění dříve přijatých právních předpisů a vypracovaných politik.

Povaha současných hrozeb a neoddělitelná vazba mezi vnitřní a vnější bezpečností EU však vyžadují, abychom své úsilí posunuli na vyšší úroveň.

Obraz hrozeb je neúprosný. Stírají se hranice mezi **hybridními hrozbami** a otevřenou válkou. Rusko vede proti EU a jejím partnerům online i offline hybridní kampaň s cílem narušit a oslabit společenskou soudržnost a demokratické procesy a otestovat solidaritu EU s Ukrajinou. Nepřátelské cizí státy a státem sponzorované subjekty se snaží proniknout do naší kritické infrastruktury a dodavatelských řetězců a narušit je, ukrást citlivé údaje a nabýt schopnosti způsobovat v budoucnu narušení co největšího rozsahu. Využívají trestnou činnost jako službu a zločince jako prostředníky. Vůči hybridním kampaním nepřátelských států jsme navíc zranitelnější kvůli naší závislosti na třetích zemích v oblasti dodavatelských řetězců.

V Evropě se rozmáhají mocné **organizované zločinecké skupiny**, které jsou posilovány online, pronikají do naší ekonomiky a ovlivňují naši společnost, jak je zdůrazněno v posouzení hrozeb závažné a organizované trestné činnosti v EU (SOCTA), které nedávno představil Europol[1]. Jakmile se v určité komunitě nebo hospodářském odvětví zapustí kořeny organizovaná trestná činnost, je velmi obtížné ji vymýtit: třetina nejnebezpečnějších zločineckých sítí je aktivní déle než deset let. Prát a skrývat výnosy z trestné činnosti jim pomáhají kryptoměny a paralelní finanční systémy.

Evropa stále čelí teroristickým hrozbám. Regionální krize za hranicemi EU vytvářejí dominový efekt a poskytují teroristickým aktérům napříč celým ideologickým spektrem novou motivaci k náboru, mobilizaci nebo budování kapacit. Své úsilí o radikalizaci a nábor zaměřují zejména na nejzranitelnější skupiny naší společnosti, především pak na určité mladé lidi. Podněcují útoky osamělých aktérů a nárůst antisystémového extremismu, jehož cílem je narušit demokratický právní řád.

Zdrojem základních nástrojů pro posílení našeho bezpečnostního aparátu je rychlý **technologický pokrok**. Stále častěji však dochází ke kybernetickým útokům a zahraničním manipulacím s informacemi, při nichž jsou využívány nové technologie, jako je umělá inteligence. Nejohroženější skupiny na internetu tvoří děti, mladiství a starší lidé, přičemž šíření nenávisti online ohrožuje svobodu projevu a sociální soudržnost.

Naše životy jsou dnes méně bezpečné, což čím dál intenzivněji pociťují i Evropané, jejichž **vnímání bezpečnosti v EU** se zhoršilo natolik, že v odpovědi na otázku ohledně budoucnosti

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

vyjádřilo obavy ohledně bezpečnost v EU celých 64 % dotázaných[2]. Stále větší obavy mají také podniky; misinformace a dezinformace, kriminalita a nezákonná činnost a kybernetická špionáž – to vše patří mezi deset největších rizik identifikovaných ve zprávě Světového ekonomického fóra o globálních rizicích z roku 2025[3].

Evropané by měli být **schopni žít beze strachu**, ať už v ulicích, doma, na veřejných místech, v metru, nebo na internetu. Jádrem práce EU v oblasti bezpečnosti je ochrana lidí, zejména těch nejzranitelnějších vůči útokům, které obvykle neúměrně postihují dětí, ženy a menšiny, včetně židovských a muslimských komunit. Je to nezbytné pro budování odolné a soudržné společnosti.

Aby EU dokázala v nadcházejících letech čelit hrozbám lépe, vypracovala Komise **Evropskou strategii vnitřní bezpečnosti**. Pomocí silnějšího souboru právních nástrojů, prohloubené spolupráce a širšího sdílení informací dokážeme zvýšit svou odolnost a kolektivní schopnost předvídat bezpečnostní hrozby, předcházet jim, odhalovat je a účinně na ně reagovat. Jednotný přístup k vnitřní bezpečnosti může podpořit členské státy při využívání možností technologií k posílení, nikoli oslabení bezpečnosti a zároveň podpořit bezpečný digitální prostor pro všechny. Tento přístup nadto podporuje společnou reakci členských států na globální politické a ekonomické změny, které ovlivňují vnitřní bezpečnost Unie.

Tato strategie se řídí **třemi zásadami** a její základ tvoří dodržování zásad právního státu a základních práv.

Za prvé, stanoví ambici změnit kulturu v oblasti bezpečnosti. Potřebujeme **celospolečenský přístup** zahrnující všechny občany a zainteresované strany, včetně občanské společnosti, výzkumné sféry, akademické obce a soukromých subjektů. Opatření v rámci této strategie proto využívají pokud možno integrovaný přístup zapojující různé zainteresované strany.

Za druhé, **do všech právních předpisů, politik a programů EU**, včetně vnější činnosti EU, **je nutné začlenit bezpečnostní aspekty**. Při přípravě, přezkumu a provádění právních předpisů, politik a programů bude třeba brát v úvahu bezpečnostní hledisko, aby byly vzaty v potaz nezbytné bezpečnostní aspekty, a tím pádem byl podpořen konzistentní a ucelený přístup k bezpečnosti.

A konečně, k zajištění bezpečné a odolné Evropy je zapotřebí **značných investic ze strany EU, jejích členských států i soukromého sektoru**. Priority a opatření stanovené v této strategii vyžadují dostatečné lidské a finanční zdroje k zajištění jejich realizace. Jak je uvedeno ve sdělení o cestě k příštímu víceletému finančnímu rámci[4], Evropa bude muset navýšit veřejné výdaje na bezpečnost a podpořit bezpečnostní výzkum a investice v oblasti bezpečnosti, a posílit tak svou strategickou autonomii.

Tato strategie doplňuje **Strategii unie připravenosti**[5], která stanoví integrovaný přístup ke všem rizikům v oblasti připravenosti na konflikty, katastrofy způsobené člověkem a přírodní katastrofy a krize, a **Bílou knihu o evropské obraně – připravenost 2030**[6], která podporuje rozvoj a získávání obranných kapacit v celé EU s cílem odradit zahraniční agresory. S cílem posílit demokratickou odolnost EU Komise rovněž navrhne vytvoření **Evropského štítu pro demokracii**. Tyto iniciativy společně vytvářejí vizi bezpečné a odolné EU.

[2] Bleskový průzkum Eurobarometr FL550: Výzvy a priority EU.
[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 řízení evropské vnitřní bezpečnosti

Komise bude úzce spolupracovat s členskými státy a agenturami EU na zlepšení přístupu EU k vnitřní bezpečnosti na strategické i operativní úrovni.

Toho dosáhneme prostřednictvím:

- **důsledné identifikace možných dopadů nových i revidovaných iniciativ Komise na bezpečnost a připravenost od samého počátku i v průběhu celého procesu vyjednávání,**
- **pravidelných schůzek Projektové skupiny Komise pro evropskou vnitřní bezpečnost, podporovaných strategickou meziodvětvovou spoluprací napříč Komisí,**
- **prezentací analýz hrozeb souvisejících s vnitřní bezpečností s cílem podpořit práci bezpečnostního kolegia,**
- **diskuzí s členskými státy na půdě Rady o vyvíjejících se výzvách v oblasti vnitřní bezpečnosti na základě analýzy hrozeb a výměny informací o klíčových politických prioritách,**
- **pravidelného podávání zpráv Evropskému parlamentu a Radě s cílem sledovat a podporovat systematické provádění klíčových iniciativ v oblasti bezpečnosti.**

2. Integrovaná situační orientace a analýza rizik

Poskytneme EU nové způsoby sdílení a kombinování informací a pravidelnou analýzu hrozeb pro vnitřní bezpečnost EU, což přispěje ke komplexnímu posouzení rizik a hrozeb.

Bezpečnost začíná **účinným předvídáním**. EU musí vycházet z ucelené, dostatečně autonomní a aktuální situační orientace a analýzy hrozeb. Pro posouzení hrozeb a boj proti nim, což v konečném důsledku představuje východisko pro politická a legislativní opatření, mají zásadní význam bezprostředně využitelné zpravodajské informace, přičemž členské státy jsou vybízeny k tomu, aby dále posilovaly jejich shromažďování prostřednictvím společné zpravodajsko-analytické složky (SIAC) jako jednotného vstupního místa pro zpravodajské informace členských států[7]. Musíme účinněji spolupracovat a využívat **analýzy založené na zpravodajských informacích** a **posouzení hrozeb** na úrovni EU.

Na základě různých posouzení rizik a hrozeb vypracovaných na úrovni EU i pro konkrétní odvětví[8] bude Komise vypracovávat **pravidelné analýzy hrozeb pro vnitřní bezpečnost EU** s cílem identifikovat hlavní bezpečnostní výzvy a následně stanovit příslušné politické priority. Ty pomohou vytvořit pružnou a pohotovou vnitřní bezpečnostní politiku, která bude účinně reagovat na vyvíjející se hrozby, lépe chránit lidi a podniky před útoky a umožní včas realizovat cílené politické zásahy. Tyto analýzy hrozeb pro vnitřní bezpečnost EU rovněž přispějí ke **komplexnímu posouzení rizik a hrozeb v EU (meziodvětvově, všechna rizika)**, vypracovanému Komisí a vysokou představitelkou, jak je stanoveno ve Strategii unie připravenosti.

Pro sdílení informací je zásadní důvěra a bezpečné nakládání s nimi, což vyžaduje spolehlivou a bezpečnou infrastrukturu. Orgány, instituce a jiné subjekty EU musí zajistit svou schopnost

[7] Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness (Společně bezpečněji – posílení civilní a vojenské připravenosti a pohotovosti Evropy), s. 23.

[8] K odvětvovým posouzením hrozeb, která k této analýze hrozeb přispějí, patří posouzení hrozeb závažné a organizované trestné činnosti v EU (SOCTA), zpráva o situaci a vývoji terorismu v EU (TE-SAT), společná zpráva o posouzení kybernetické bezpečnosti (JCAR) a budoucí posouzení hrozeb, rizik a metod praní peněz a financování terorismu, jež provedou Komise a Orgán pro boj proti praní peněz.

používat **bezpečné komunikační kanály** pro výměnu citlivých a utajovaných informací mezi sebou navzájem i s členskými státy. Investice do **interoperabilních bezpečných systémů** a spolehlivých technologií posílí autonomii EU a její schopnost zvládat krize a zajistit provozní odolnost. V této souvislosti Komise naléhavě vyzývá spolunormotvůrce, aby dokončili jednání o **návrhu nařízení o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie**, jehož cílem je zejména zajistit společný rámec pro nakládání s citlivými neutajovanými a utajovanými informacemi[9].

V zájmu zajištění vlastní provozní bezpečnosti a situační orientace Komise zreviduje svůj rámec pro řízení organizační bezpečnosti a zřídí **integrované bezpečnostní operační středisko (ISOC)**, které bude chránit osoby, fyzický majetek a operace na všech pracovištích Komise. Komise rovněž posílí své operační a analytické kapacity pro identifikaci a zmírňování hybridních hrozeb.

V souladu se Strategií unie připravenosti budou do všech právních předpisů, politik a programů EU začleněny aspekty připravenosti a bezpečnosti. Při přípravě nebo přezkumu právních předpisů, politik nebo programů bude Komise s ohledem na hledisko připravenosti a bezpečnosti důsledně identifikovat potenciální dopady upřednostňované politické varianty na připravenost a bezpečnost. Za tímto účelem budou tvůrci politik v Komisi pravidelně školeni.

S cílem podpořit členské státy bude Komise projednávat vyvíjející se výzvy v oblasti vnitřní bezpečnosti a klíčové politické priority s Radou a bude ji o provádění této strategie pravidelně informovat. Komise bude průběžně informovat i Evropský parlament a relevantní zainteresované strany a bude je zapojovat do všech příslušných opatření.

Klíčová opatření

Komise:

- **bude vypracovávat a předkládat pravidelné analýzy hrozeb týkající se výzev v oblasti vnitřní bezpečnosti EU**

Členské státy se vyzývají, aby:

- **posílily sdílení zpravodajských informací se společnou zpravodajsko-analytickou složkou (SIAC) a zajistily lepší sdílení informací s institucemi a jinými subjekty EU**

Komise vyzývá Evropský parlament a Radu, aby:

- **dokončily jednání o návrhu nařízení o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie**

3. Posílení bezpečnostních kapacit EU

Vyvineme nové nástroje pro prosazování práva, jako je renovovaný Europol, a lepší prostředky pro koordinaci a zajištění bezpečné výměny údajů a zákonného přístupu k nim.

Aby EU mohla účinně čelit vyvíjejícím se hrozbám, musí posílit své bezpečnostní kapacity a podporovat inovace. Donucovací a justiční orgány jako hlavní aktéři v boji proti hrozbám pro vnitřní bezpečnost potřebují správné operační nástroje a kapacity, aby mohly jednat rychle a účinně. Je důležité, aby tyto orgány byly schopny komunikovat a koordinovat svou činnost přes hranice a napříč útvary, a zajistit tak účinnou prevenci, odhalování, vyšetřování a stíhání.

[9] COM(2022) 119 final.

Instituce a jiné subjekty EU pro vnitřní bezpečnost

Instituce a jiné subjekty EU v oblasti spravedlnosti, vnitřních věcí a kybernetické bezpečnosti hrají klíčovou roli v bezpečnostní architektuře EU – roli, která se s rozšiřováním jejich pravomocí neustále zvyšuje.

Dnes, 25 let po svém zřízení, je **Europol** pro bezpečnostní rámec EU důležitější než kdykoli dříve. Podporuje složitá přeshraniční vyšetřování, usnadňuje výměnu informací, vyvíjí inovativní nástroje pro policejní práci a poskytuje pokročilé odborné znalosti pro prosazování práva. Europolu však v plném využití jeho operačního potenciálu při podpoře vyšetřovacích a operativních činností v boji proti přeshraniční trestné činnosti brání několik faktorů: od nedostatečných zdrojů až po skutečnost, že jeho současný mandát nepokrývá nové bezpečnostní hrozby, jako jsou sabotáže, hybridní hrozby nebo manipulace s informacemi. Proto Komise navrhne **ambiciózní revizi mandátu Europolu**, aby se z něj stala skutečně operativní policejní agentura, která bude lépe podporovat členské státy. Cílem je posílit technologické odborné znalosti a kapacitu Europolu na podporu vnitrostátních donucovacích orgánů, zlepšit koordinaci s ostatními institucemi a jinými subjekty a s členskými státy, posílit strategická partnerství s partnerskými zeměmi a soukromým sektorem a zajistit posílený dohled nad Europolem.

Komise bude pracovat na dalším **zlepšení efektivity a komplementarity institucí a jiných subjektů EU pro vnitřní bezpečnost a na posílení hladké spolupráce** mezi nimi.

Bude posouzen a posílen mandát **Eurojustu** v zájmu účinnější justiční spolupráce, posílení komplementarity a spolupráce s Europolem. To zahrnuje zvýšení efektivity Eurojustu i jeho schopnosti poskytovat proaktivní podporu a analýzy justičním orgánům členských států. Dále, vzhledem k jedinečné pravomoci **Úřadu evropského veřejného žalobce (EPPO)** vyšetřovat a stíhat trestné činy poškozující finanční zájmy Unie, Komise zváží, jak nejlépe zlepšit jeho schopnost chránit finanční prostředky Unie. To bude zahrnovat posílení spolupráce mezi úřadem EPPO a Europolem.

Pro spolupráci je zásadní **efektivní a bezpečná výměna informací mezi agenturami**. Europol a Frontex potřebují rychlou vzájemnou výměnu informací, včetně výměny informací pro operativní účely, v návaznosti na společné prohlášení z ledna 2024[10]. **Agentura eu-LISA** má ústřední úlohu při zajišťování bezpečného ukládání a dostupnosti údajů pro lepší koordinaci a efektivnější výměnu informací mezi agenturami. **Agentura EU pro základní práva** poskytuje odborné znalosti v oblasti ochrany základních práv při vytváření a provádění bezpečnostních politik.

Orgán EU pro boj proti praní peněz (AMLA) dostal pravomoc porovnávat informace podle existence či neexistence záznamu s informacemi poskytnutými Europolem, úřadem EPPO, Eurojustem a Evropským úřadem pro boj proti podvodům (OLAF) za účelem provádění společných analýz přeshraničních případů.

Agentura EU pro kybernetickou bezpečnost (ENISA) hraje ústřední roli při provádění evropských právních předpisů v oblasti kybernetické bezpečnosti. Při nadcházející **revizi aktu o kybernetické bezpečnosti** Komise posoudí jeho působnost a navrhne modernizaci, aby se posílila jeho přidaná hodnota EU.

Spolupráce mezi celními orgány a dalšími donucovacími orgány se zvýší díky navrhovanému zřízení **Celního úřadu EU** a **celního datového centra EU** v rámci balíčku celní reformy EU. Informace z budoucího centra a související údaje z Europolu, Eurojustu, úřadu EPPO, úřadu OLAF, orgánu AMLA a Frontexu v rámci jejich příslušných pravomocí posílí společnou

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

analýzu a přispějí ke konzistentnějším operativním činnostem, zejména na vnějších hranicích. Komise vybízí spolunormotvůrce k rychlému dokončení jednání o celní reformě EU a bude jim v tomto směru i nadále nápomocna.

Z výsledků probíhajícího přezkumu **architektury EU pro boj proti podvodům** bude rovněž vycházet posílení komplementarity mezi úřadem EPPO, úřadem OLAF, Europolem, Eurojustem, orgánem AMLA a navrhovaným Celním úřadem EU. Z tohoto holistického přístupu, který se zaměřuje na lepší využívání trestních i správních prostředků, interoperabilitu IT systémů a zdokonalenou spolupráci, může těžit vnitřní bezpečnost.

Kritická komunikace

Kritické komunikační systémy[11] jsou v současnosti ve většině případů provozovány izolovaně na vnitrostátní úrovni. To znamená, že když zásahové složky v první linii překročí hranice do jiných členských států, často nemohou komunikovat se svými kolegy. V některých členských státech je také omezena komunikace mezi různými typy zásahových složek v první linii (např. policie a sanitky). Standardy většiny systémů neodpovídají stávajícím požadavkům na funkčnost a odolnost, což výrazně omezuje schopnost reakce zásahových složek v první linii, zejména přes hranice.

Aby se zlepšila schopnost EU reagovat na krize, navrhne Komise legislativu, která vytvoří **evropský kritický komunikační systém (EUCCS)**, jenž propojí kritické komunikační systémy nové generace v členských státech EU. Cílem je, aby byl systém EUCCS založen na třech strategických pilířích: operační mobilitě, silné odolnosti a strategické autonomii. Iniciativa EUCCS stanoví harmonizované požadavky a pomůže modernizovat kritické komunikační systémy členských států, což umožní jejich hladké fungování. Rozšíří také systémové pokrytí pomocí budoucího multiorbitálního systému IRIS[212]. Technické možnosti pro systém EUCCS budou vyvíjeny v rámci projektů financovaných EU, přičemž budou využíváni především evropští dodavatelé technologií, aby se podpořila strategická autonomie EU v tomto citlivém odvětví.

Zákonný přístup k údajům

Donucovací a justiční orgány musí být schopny vyšetřovat trestné činy a zasahovat proti nim. Téměř všechny formy závažné a organizované trestné činnosti mají dnes digitální stopu[13]. Přibližně 85 % vyšetřování trestných činů se nyní opírá o schopnost donucovacích orgánů získat přístup k digitálním informacím.[14]

Skupina na vysoké úrovni pro přístup k údajům pro účely účinného prosazování práva ve své závěrečné zprávě[15] zdůraznila, že donucovací a justiční orgány v posledním desetiletí za zločinci zaostávají, protože ti využívají nástroje a produkty poskytované z jiných jurisdikcí poskytovateli, kteří zavedli opatření, jež je zbavují prostředků pro spolupráci při zákonných žádostech v jednotlivých trestních věcech. Pro budoucí úsilí o narušení nejnebezpečnějších zločineckých sítí a zločinců v Unii i mimo ni je proto nezbytná systematická spolupráce mezi donucovacími orgány a soukromými subjekty, včetně poskytovatelů služeb.

Vzhledem k tomu, že digitalizace je stále rozšířenější a poskytuje zločincům stále více nových nástrojů, je nezbytné vytvořit rámec pro přístup k údajům, který bude odpovídat potřebám

[11] Tj. sítě, které používají donucovací orgány, pohraniční stráž, celní úřady, civilní ochrana, hasiči, zdravotnické záchranné služby a další klíčové subjekty pro veřejnou bezpečnost a ochranu.
[12] Družicová infrastruktura EU pro odolnost, propojení a bezpečnost.
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52019PC0070.
[15] Závěrečná zpráva Skupiny na vysoké úrovni pro přístup k údajům pro účely účinného prosazování práva – 15. 11. 2024, 4802e306-c364-4154-835b-e986a9a49281_en.

prosazování našich právních předpisů a ochrany našich hodnot. Zároveň je pro zachování kybernetické bezpečnosti a ochranu před novými bezpečnostními hrozbami stejně tak důležité zajistit, aby digitální systémy zůstaly zabezpečené proti neoprávněnému přístupu. Tyto přístupové rámce musí rovněž respektovat základní práva a zajistit mimo jiné odpovídající ochranu soukromí a osobních údajů.

V posledních letech přijala EU opatření jak k boji proti **trestné činnosti páchané online**, tak k **usnadnění přístupu k digitálním důkazům u všech trestných činů**, a to přijetím pravidel pro elektronické důkazy, která se budou v plném rozsahu uplatňovat od srpna 2026[16]. Tato pravidla budou doplněna mezinárodními nástroji pro výměnu informací a důkazů. Komise brzy navrhne podepsání a uzavření nové **Úmluvy OSN o boji proti kyberkriminalitě**.

V návaznosti na doporučení skupiny na vysoké úrovni[17] Komise v první polovině roku 2025 předloží **plán, v němž stanoví právní a praktická opatření**, která navrhuje přijmout **k zajištění zákonného a účinného přístupu k údajům**. V návaznosti na tento plán provede Komise přednostně posouzení dopadu **pravidel pro uchovávání údajů** na úrovni EU a přípravu **Technologického plánu pro šifrování** s cílem identifikovat a posoudit technologická řešení, která by donucovacím orgánům umožnila zákonný přístup k zašifrovaným údajům při zachování kybernetické bezpečnosti a základních práv.

Operativní spolupráce

Komise bude spolupracovat s členskými státy, institucemi a jinými subjekty EU a partnerskými zeměmi na posílení operativní spolupráce, která je nezbytná pro účinnější přístup k boji proti nadnárodní organizované trestné činnosti a terorismu.

Významných operativních výsledků dosáhla **evropská multidisciplinární platforma pro boj proti hrozbám vyplývajícím z trestné činnosti (EMPACT)** jako hlavní rámec EU pro společný postup proti závažné a organizované trestné činnosti. Příští cyklus EMPACT 2026–2029 představuje příležitost k dalšímu posílení tohoto rámce. Aby bylo možné narušit činnost nejnebezpečnějších zločineckých sítí a zločinců, musí Unie zefektivnit své úsilí a zaměřit je na nejnaléhavější priority, posílit závazky členských států a zajistit účinné využívání zdrojů.

Za tímto účelem bude Komise spolupracovat s předsednictvími Rady a členskými státy, aby **maximalizovala potenciál EMPACT a řešila klíčové priority pro příští cyklus EMPACT 2026–2029**. Ve všech těchto prioritních oblastech jsou potřebné zpravodajské informace o nejnebezpečnějších zločineckých sítích, společné vyšetřovací a operativní pracovní skupiny a důrazná justiční reakce, včetně přístupu založeném na sledování toku peněz. Kromě toho musí Unie bojovat proti náboru pro trestnou činnost a proti infiltraci a posílit spolupráci mezi různými agenturami a donucovacími orgány o mezinárodních záležitostech a výcvik.

Komise bude rovněž podporovat další formy **přeshraniční operativní spolupráce v oblasti prosazování práva mezi členskými státy a zeměmi přidruženými k Schengenu**. Schengenský prostor, bez kontrol na vnitřních hranicích, vyžaduje úzkou spolupráci a výměnu informací mezi donucovacími orgány členských států, aby byla zajištěna vysoká úroveň vnitřní bezpečnosti. V současnosti se příslušníci donucovacích orgánů stále potýkají s problémy při sledování nebo provádění neodkladných zásahů přes hranice[18] a také boj proti hybridním

[16] Nařízení Evropského parlamentu a Rady (EU) 2023/1543 ze dne 12. července 2023 o evropském vydávacím příkazu a evropském uchovávacím příkazu pro elektronické důkazy v trestním řízení a pro výkon trestu odnětí svobody po skončení trestního řízení (Úř. věst. L 191, 28.7.2023).

[17] Závěry Rady o přístupu k údajům pro účely účinného prosazování práva (12. prosince 2024), https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/cs/pdf.

[18] Jak Komise uvedla v posouzení provádění doporučení Rady (EU) 2022/915 ze dne 9. června 2022 o operativní spolupráci v oblasti prosazování práva členskými státy (5909/25).

hrozbám vyžaduje posílení přeshraniční spolupráce. Měla by být vytvořena **skupina na vysoké úrovni pro budoucnost operativní spolupráce v oblasti prosazování práva**, která by vypracovala společnou strategickou vizi.

Pro účinnou přeshraniční spolupráci je rovněž nezbytná účinná výměna údajů mezi donucovacími orgány. Po vytvoření **architektury interoperability** budou mít donucovací orgány a Europol účinný přístup ke klíčovým informacím. EU a její členské státy by zároveň měly upřednostnit dvoustrannou a mnohostrannou výměnu informací, a to prostřednictvím právního a technického provádění **nařízení Prüm II**[19], ve spolupráci s agenturou eu-LISA a Europolem. To umožní bezpečnou automatickou výměnu otisků prstů, profilů DNA, údajů o registraci vozidel, zobrazení obličeje a policejních záznamů prostřednictvím směrovačů EU. Na vnitrostátní úrovni musí členské státy provést **směrnici o výměně informací**[20], která posiluje kanály výměny informací pro jejich hladký přeshraniční tok a zároveň zajišťuje jejich integraci s celounijními systémy, jako je SIENA[21].

Účinná přeshraniční spolupráce závisí také na podpoře **společné kultury EU v oblasti prosazování práva**. Pro dosažení tohoto cíle jsou zásadní společná školení, centra excelence a programy mobility. Komise prozkoumá, jak by EU mohla nejlépe podpořit školení orgánů členských států, přičemž bude využívat **CEPOL** jakožto agenturu EU pro vzdělávání a výcvik v oblasti prosazování práva.

Posílení ochrany hranic

Posílení odolnosti a bezpečnosti vnějších hranic má zásadní význam pro boj proti hybridním hrozbám, jako je například zneužívání migrace jako zbraně, aby se zabránilo vstupu nebezpečných subjektů a zboží do EU a aby bylo možné účinně bojovat proti přeshraniční trestné činnosti a terorismu. V roce 2026 **se plánuje rozšíření Schengenského informačního systému (SIS)**, aby členské státy mohly na základě údajů sdílených třetími zeměmi s Europolem vkládat záznamy o státních příslušnících třetích zemí zapojených do terorismu, včetně zahraničních teroristických bojovníků, a u dalších závažných trestných činů.

Lepší **interoperabilita** rozsáhlých informačních systémů EU poskytne členským státům zásadní informace o osobách ze třetích zemí, které překračují nebo mají v úmyslu překročit vnější hranice, a pomůže tak orgánům posoudit podmínky pro povolení jejich vstupu na území členských států[22]. Komise bude i nadále úzce spolupracovat s členskými státy a agenturou eu-LISA na rychlém zavedení těchto systémů, zejména **Systému vstupu/výstupu (EES), Evropského systému pro cestovní informace a povolení (ETIAS) a revidovaného Vízového informačního systému (VIS),** aby zajistila jejich hladké fungování a bezpečnostní přínosy.

[19] Nařízení Evropského parlamentu a Rady (EU) 2024/982 ze dne 13. března 2024 o automatizovaném vyhledávání a výměně údajů pro policejní spolupráci a o změně rozhodnutí Rady 2008/615/SVV a 2008/616/SVV a nařízení Evropského parlamentu a Rady (EU) 2018/1726, (EU) 2019/817 a (EU) 2019/818 (nařízení Prüm II) (Úř. věst. L, 2024/982, 5.4.2024).

[20] Směrnice Evropského parlamentu a Rady (EU) 2023/977 ze dne 10. května 2023 o výměně informací mezi donucovacími orgány členských států a o zrušení rámcového rozhodnutí Rady 2006/960/SVV (Úř. věst. L 134, 22.5.2023, s. 1).

[21] Aplikace sítě pro bezpečnou výměnu informací.

[22] Konkrétně Systém vstupu/výstupu (EES) umožní členským státům identifikovat státní příslušníky třetích zemí na vnějších hranicích schengenského prostoru a zaznamenávat jejich příjezdy a odjezdy, což umožní systematickou identifikaci osob, které překročily povolenou délku pobytu. Evropský systém pro cestovní informace a povolení (ETIAS) a Vízový informační systém (VIS) umožní členským státům ještě před příjezdem státního příslušníka třetí země na vnější hranice předběžně posoudit, zda jeho přítomnost na území EU nepředstavuje bezpečnostní riziko.

V zájmu dalšího zvýšení ochrany hranic a posílení spolupráce EU tváří v tvář vyvíjejícím se hrozbám **Komise navrhne posílení Frontexu**. Počet příslušníků Evropské pohraniční a pobřežní stráže by se měl časem ztrojnásobit na 30 000. Agentura by měla být vybavena vyspělou technologií pro dohled a situační orientaci, včetně zpravodajských informací relevantních pro evropskou integrovanou správu hranic, a přístupem k robustním vládním službám EU pro pozorování Země za účelem ochrany hranic, které mají být zavedeny do roku 2027. To by mělo dále posílit její schopnost odhalovat přeshraniční trestnou činnost na vnějších hranicích, předcházet jí a bojovat proti ní a posílit její podporu poskytovanou členským státům při provádění navracení, zejména pokud jde o státní příslušníky třetích zemí, kteří představují bezpečnostní riziko.

Podvody s doklady a totožností usnadňují převaděčství migrantů, obchodování s lidmi, utajené přemísťování zločinců a obchodování s nelegálním zbožím. Jakmile bude uveden do provozu **detektor vícenásobné totožnosti (MID)**[23], zlepší schopnost vnitrostátních orgánů identifikovat osoby používající více totožností a bojovat proti podvodům s totožností. Komise prozkoumá způsoby, jak zvýšit bezpečnost cestovních a pobytových dokladů vydávaných občanům EU a státním příslušníkům třetích zemí. Kromě toho Komise posoudí, jak mohou ke zvýšení bezpečnosti cestovních dokladů a lepšímu ověřování totožnosti přispět unijní peněženky digitální identity, které mají být podle evropského rámce pro digitální identitu zavedeny do konce roku 2026. Doplní tak legislativní návrhy týkající se digitálních cestovních oprávnění a digitální cestovní aplikace EU[24].

Cestovní informace jsou pro úřady zásadní při identifikaci a vyšetřování pohybu zločinců, teroristů a dalších osob, které představují bezpečnostní hrozbu. Zatímco pro informace o komerční letecké dopravě existuje rámec EU[25], zpracování údajů z jiných druhů dopravy pro účely prosazování práva je roztříštěné. Zločinci a teroristé tak mohou nepozorovaně využívat různé druhy dopravy k nezákonným činnostem. Komise bude spolupracovat s členskými státy a odvětvím dopravy na **posílení rámce pro cestovní informace** tím, že zváží možnost vytvořit unijní systém, který by provozovatelům soukromých letů ukládal povinnost shromažďovat a předávat údaje o cestujících, vyhodnotí pravidla pro zpracování jmenné evidence cestujících a posoudí způsoby, jak zefektivnit zpracování informací o cestování po moři. V oblasti silniční dopravy Komise posoudí širší využití systémů **automatického rozpoznávání registračních značek (ANPR)** a zvýší možnosti součinnosti se Schengenským informačním systémem.

Přístup založený na prognózách, inovacích a schopnostech

Komise vypracuje **ucelený prognostický přístup k vnitřní bezpečnosti na úrovni EU**, který bude vycházet z osvědčených postupů identifikovaných na vnitrostátní úrovni. Tento přístup podpoří tvorbu politik a bude sloužit jako vodítko pro investice do relevantního bezpečnostního výzkumu a inovací financovaných EU.

Výzkum a inovace hrají v oblasti vnitřní bezpečnosti zásadní roli, neboť vytvářejí řešení, jak čelit novým hrozbám, včetně hrozeb plynoucích ze zneužití technologií[26]. EU musí za účelem potírání bezpečnostních hrozeb nadále investovat prostřednictvím bezpečnostního výzkumu a inovací financovaných EU[27] do vývoje inovativních nástrojů a řešení a zároveň dbát

[23] MID je jedním z prvků interoperability zavedených nařízením (EU) 2019/818 a nařízením 2019/817.
[24] https://ec.europa.eu/commission/presscorner/detail/cs/ip_24_5047.
[25] Rámec jmenné evidence cestujících (PNR) a předběžných údajů o cestujících (API) stanovený směrnicí (EU) 2016/681 („směrnice o PNR“) a nařízením (EU) 2025/12 a nařízením (EU) 2025/13 („nařízení o API“).
[26] Viz zpráva Společného výzkumného střediska Komise Nová rizika a příležitosti pro vnitřní bezpečnost EU plynoucí z nových technologií, https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] Studie o posílení bezpečnostního výzkumu a inovací financovaných EU – 20 let výzkumu a inovací v oblasti civilní bezpečnosti financovaných EU – 2025, https://data.europa.eu/doi/10.2837/0004501.

na dodržování pravidel EU a základních práv. Komise by měla podpořit přechod od výzkumu k zavádění do praxe, aby zajistila účinné využívání těchto moderních kapacit, přičemž prioritou by měly být **moderní technologie**, jako je umělá inteligence. Součástí tohoto přístupu by měla být i školení s cílem zlepšit využívání systémů umělé inteligence a dalších technických možností ze strany donucovacích a justičních orgánů. Kromě toho by měl být potenciál technologií dvojího užití v případě potřeby využíván obousměrně (z civilního užití do obranného a naopak)[28].

Začlenit výzkum do praxe a tvorby politik pomůže **Inovační centrum EU pro vnitřní bezpečnost**[29], což je síť inovačních laboratoří, které poskytují nejnovější inovační aktualizace a účinná řešení na podporu práce aktérů vnitřní bezpečnosti v EU a členských státech. Zvýšení efektivity Europolu vyžaduje posílit úložiště nástrojů Europolu (ETR), což umožní identifikovat, vyvíjet, společně pořizovat a operativně používat pokročilé technologie. Kromě toho Komise ve svém Společném výzkumném středisku zřídí **Kampus pro bezpečnostní výzkum a inovace**, který bude sdružovat výzkumné pracovníky, aby se zkrátil cyklus od výsledků výzkumu k inovacím, vývoji a úspěšnému zavedení do praxe a zároveň se snížily náklady na vývoj, testování a validaci.

Náš **Evropský výzkumný prostor** je ze své podstaty založen na spolupráci, a proto je vystaven zahraničnímu vměšování a dezinformacím. V návaznosti na přijetí doporučení Rady o posílení bezpečnosti výzkumu[30] přijímají Komise a členské státy opatření, která mají posílit postavení příslušných aktérů, mimo jiné zřízením Odborného centra pro bezpečnost výzkumu.

Klíčová opatření

Komise přijme:

- **v roce 2026 legislativní návrh na přeměnu Europolu ve skutečně operativní donucovací orgán**
- **v roce 2026 legislativní návrh na posílení Eurojustu**
- **v roce 2026 legislativní návrh na posílení úlohy a úkolů Frontexu**
- **v roce 2026 legislativní návrh na zřízení evropského kritického komunikačního systému**

Komise:

- **v roce 2025 předloží plán, v němž stanoví další postup v oblasti zákonného a účinného přístupu k údajům pro účely prosazování práva**
- **v roce 2025 připraví posouzení dopadů s cílem podle potřeby aktualizovat pravidla pro uchovávání údajů na úrovni EU**
- **v roce 2026 předloží Technologický plán pro šifrování s cílem identifikovat a posoudit technologická řešení, která umožní donucovacím orgánům zákonný přístup k údajům**
- **bude pracovat na vytvoření skupiny na vysoké úrovni pro posílení operativní spolupráce v oblasti prosazování práva**
- **v roce 2026 zřídí ve svém Společném výzkumném středisku Kampus pro bezpečnostní výzkum a inovace**

Komise ve spolupráci s členskými státy a příslušnými agenturami EU:

[28] Jak je uvedeno v Niinistöově zprávě.
[29] Inovační centrum EU pro vnitřní bezpečnost | Europol.
[30] Úř. věst. C/2024/3510, 30.5.2024.

- **posílí architekturu EMPACT**
- **bude pracovat na rychlém zavedení architektury interoperability a provádění nařízení Prüm II**
- **posílí rámec pro cestovní informace**

Členské státy se vyzývají, aby:

- **transponovaly a v plném rozsahu prováděly směrnici o výměně informací**

4. Odolnost proti hybridním hrozbám a dalším nepřátelským aktům

Budeme zvyšovat odolnost vůči hybridním hrozbám tím, že zlepšíme ochranu kritické infrastruktury, posílíme kybernetickou bezpečnost, zabezpečíme dopravní uzly a přístavy a budeme bojovat proti online hrozbám.

Četnost a sofistikovanost nepřátelských aktů, které ohrožují bezpečnost EU, se zvýšila a zlovolní aktéři výrazně rozšířili svůj arzenál. Hybridní kampaně namířené proti EU, jejím členským státům a partnerům se zintenzivnily a zahrnují sabotáže zaměřené na kritickou infrastrukturu, žhářství, kybernetické útoky, vměšování do voleb, zahraniční vměšování a manipulace s informacemi, včetně dezinformací, a zneužívání migrace jako zbraně. Vzhledem ke své politické a operativní úloze a povaze informací, s nimiž nakládají, nejsou ušetřeny ani orgány, instituce a jiné subjekty Unie (dále jen „subjekty Unie“).

EU musí **zvýšit svou odolnost**, účinně využívat stávající nástroje a vyvinout nové způsoby, jak čelit těmto vyvíjejícím se hrozbám ze strany státních i nestátních aktérů, a to jak nyní, tak v budoucnu.

Kritická infrastruktura

Velkým problémem jsou hrozby pro **kritickou infrastrukturu**, včetně hybridních hrozeb, jako jsou sabotáže a nepřátelská činnost v kyberprostoru, zejména pokud jde o infrastrukturu, která propojuje členské státy – ať už jde o energetické propojení nebo přeshraniční komunikační kabely a dopravu. Od začátku útočné války Ruska proti Ukrajině se zejména v roce 2024 zvýšil počet sabotážních akcí zaměřených na kritickou infrastrukturu, které postihly řadu členských států. Pro účinné předvídání, odhalování a prevenci takových činů a reakci na ně je nezbytná spolupráce mezi donucovacími orgány, bezpečnostními útvary a útvary kybernetické bezpečnosti, vojenskou a civilní ochranou a soukromými subjekty.

Pro zajištění nepřetržitého poskytování základních služeb, které jsou pro ekonomiku a společnost životně důležité, je nezbytné snižovat zranitelnost a posilovat odolnost kritických subjektů. Proto je v tomto ohledu zásadní včasná transpozice a řádné provádění **směrnice o odolnosti kritických subjektů (CER)**[31] a **směrnice o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v celé Unii (NIS 2)**[32] ve všech členských státech.

V zájmu zajištění rychlého pokroku bude Komise ve spolupráci se **Skupinou pro odolnost kritických subjektů a Skupinou pro spolupráci v oblasti bezpečnosti sítí a informací** podporovat členské státy při identifikaci kritických subjektů[33] a při výměně osvědčených

[31] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES.

[32] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

[33] Směrnice se vztahuje na tato odvětví: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, pitná voda, odpadní vody, digitální infrastruktura, veřejná správa, vesmír a výroba, zpracování a distribuce potravin.

postupů v oblasti vnitrostátních strategií a posuzování rizik, pokud jde o základní služby. Dojde-li k narušení kritické infrastruktury se značným přeshraničním dopadem, budou reakce na úrovni EU koordinovány podle **plánu EU pro kritickou infrastrukturu**. Komise vyzývá Radu, aby urychleně přijala **kybernetický plán EU**, který dále posílí koordinaci v kontextu řešení krizí a usnadní užší spolupráci mezi orgány v oblasti fyzické a digitální odolnosti. Po úspěšných zátěžových testech v odvětví energetiky, které proběhly v roce 2023, bude Komise podporovat **dobrovolné zátěžové testy** v dalších klíčových odvětvích pro vnitřní bezpečnost. Kromě toho Komise poskytne **celounijní přehled přeshraničních a meziodvětvových rizik** pro základní služby, aby podpořila posouzení rizik členskými státy a poskytla informace pro komplexní posouzení rizik na úrovni EU. V souladu se Strategií unie připravenosti bude Komise spolupracovat s členskými státy s cílem identifikovat další odvětví a služby, na něž se nevztahují stávající právní předpisy a v nichž by bylo případně potřeba přijmout opatření.

Vynikající spolupráci při sdílení osvědčených postupů a zvyšování odolnosti v odvětvích energetiky, dopravy, digitální infrastruktury a vesmíru podpořila **Pracovní skupina EU–NATO pro odolnost kritické infrastruktury**. Tato práce bude pokračovat v rámci **strukturovaného dialogu EU–NATO o odolnosti**. Silnou podporu při přípravě na hybridní hrozby a boji proti nim nabízí členským státům a partnerům **soubor nástrojů EU proti hybridním hrozbám**. **Týmy rychlé reakce na hybridní hrozby**[34] poskytují na požádání členským státům, různým misím EU a partnerům krátkodobou pomoc přizpůsobenou konkrétním potřebám. Kromě toho bude Komise pokračovat ve spolupráci EU v oblasti boje proti sabotážím prostřednictvím činností odborníků[35], včetně **specializovaného společného pracovního programu** pro odborníky, jehož cílem je zefektivnit výměnu informací a zmapovat protiopatření.

Incidenty, při nichž byly poškozeny **podmořské kabely** v Evropě, zdůrazňují potřebu přísnějších opatření a jasnějších reakcí. Jak je uvedeno v **Akčním plánu EU o bezpečnosti kabelů**[36], bude Komise spolu s vysokou představitelkou spolupracovat s členskými státy, agenturami EU a partnery, jako je NATO, aby hrozbám pro podmořské kabely předcházeli, odhalovali je, reagovali na ně a odrazovali od nich. Za účelem vytvoření integrovaného situačního obrazu hrozeb bude Komise spolupracovat s členskými státy na vývoji a dobrovolném zavedení integrovaného mechanismu dohledu nad podmořskými kabely v jednotlivých mořských oblastech, počínaje severským/pobaltským regionálním centrem.

Kybernetická bezpečnost

Trvalou pozornost a opatření na evropské úrovni vyžaduje neutuchající **nepřátelská činnost v kyberprostoru**, která je často součástí širšího spektra vícerozměrných a hybridních hrozeb. V posledních letech Unie přijala řadu právních předpisů v oblasti kybernetické bezpečnosti, jež posilují kybernetickou odolnost subjektů, na které se vztahuje směrnice NIS 2 a které působí v kritických odvětvích EU, i subjektů Unie[37], zlepšují bezpečnost digitálních produktů (akt o kybernetické odolnosti) a vytvářejí rámec pro připravenost a podporu při reakci na incidenty (akt o kybernetické solidaritě). V lednu 2025 přijala Komise **Evropský akční plán pro**

[34] Strategický kompas pro posílení bezpečnosti a obrany EU 2022, s. 22

[35] Poradci EU pro ochranu bezpečnosti, Evropská síť pro odstraňování výbušných zařízení (EEODN), síť ATLAS, Bezpečnostní síť EU pro vysoká rizika (EU HRSN), Poradní skupina CBRN pro bezpečnost, Skupina pro odolnost kritických subjektů (CERG).

[36] JOIN(2025) 9 final.

[37] Nařízení Evropského parlamentu a Rady (EU, Euratom) 2023/2841 ze dne 13. prosince 2023, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie (Úř. věst. L, 2023/2841, 18.12.2023).

kybernetickou bezpečnost nemocnic a poskytovatelů zdravotní péče[38] s cílem zlepšit odhalování hrozeb, připravenost a reakci na krize. Klíčová je jeho realizace v plném rozsahu. Abychom mohli řešit nové hrozby a reagovat na vývoj, musíme současně zintenzivnit naše opatření zejména v oblastech výměny informací, bezpečnosti dodavatelských řetězců, ransomwaru a kybernetických útoků, jakož i technologické suverenity.

Kromě toho je pro jeho realizaci potřeba vyřešit stávající nedostatek odborníků v oblasti kybernetické bezpečnosti, který čítá 299 000 osob. Komise bude spolupracovat s členskými státy v rámci unie dovedností[39] na rozšíření počtu pracovníků v oblasti kybernetické bezpečnosti, zejména s využitím nové Akademie kybernetických dovedností. K rozšíření rezervy talentů a k tomu, aby Evropa dokázala reagovat na potřeby trhu práce v oblasti kybernetické bezpečnosti, přispívá Strategický plán vzdělávání v oborech STEM[40].

Souběžně se zvyšováním své odolnosti bude EU i nadále plně využívat rámec pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru **(soubor nástrojů pro diplomacii v oblasti kybernetiky**), aby předcházela kybernetickým hrozbám pocházejícím od státních i nestátních aktérů, odrazovala od nich a reagovala na ně.

Bezpečnost dodavatelských řetězců IKT

Příslušný rámec pro ochranu sítí 5G poskytuje **soubor nástrojů pro kybernetickou bezpečnost sítí 5G**, ale členské státy jej v současnosti uplatňují nedostatečně. Přetrvávají nepřijatelná bezpečnostní rizika, zejména pokud jde o nahrazování vysoce rizikových poskytovatelů. Harmonizovaný přístup k bezpečnosti dodavatelských řetězců IKT může vyřešit současnou roztříštěnost vnitřního trhu způsobenou rozdílnými přístupy na vnitrostátní úrovni, zamezit kritickým závislostem a snížit riziko v našich dodavatelských řetězcích IKT plynoucí z vysoce rizikových dodavatelů, a tím zabezpečit naši kritickou infrastrukturu.

V souladu s tímto přístupem se bude Komise v nadcházející **revizi aktu o kybernetické bezpečnosti** šířeji zabývat bezpečností a odolností dodavatelských řetězců a infrastruktury IKT. Kromě toho Komise navrhne zlepšení **evropského rámce pro certifikaci kybernetické bezpečnosti**, aby bylo zajištěno včasné přijetí budoucích certifikačních systémů, které budou reagovat na politické potřeby.

V návaznosti na stávající nebo probíhající odvětvová hodnocení[41] Komise společně s členskými státy vypracuje **Strategický plán koordinovaného posouzení rizik v oblasti kybernetické bezpečnosti**.

Běžnou součástí dodavatelských řetězců kritických infrastruktur, podniků a orgánů veřejné správy se staly cloudové a telekomunikační služby. Komise přijme opatření motivující kritické subjekty, aby si vybíraly **cloudové a telekomunikační služby, které nabízejí odpovídající úroveň kybernetické bezpečnosti**, a to při zohlednění nejen technických rizik, ale také strategických rizik a závislostí.

Ransomware a kybernetické útoky

Přetrvávajícím velkým problémem v EU i celosvětově je **ransomware**, přičemž jedna zpráva odhaduje, že do roku 2031 budou celosvětové roční náklady přesahovat 250 miliard EUR[42]. Bezpečnostní pozici subjektů výrazně zlepší jak **směrnice NIS 2**, tak **akt o kybernetické**

[38] https://digital-strategy.ec.europa.eu/cs/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM(2025) 90 final.
[40] COM(2025) 89 final.
[41] Například v oblasti sítí 5G, telekomunikací, elektřiny, obnovitelných zdrojů energie a propojených vozidel.
[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

odolnosti, čímž se pro ransomwarové sítě stane provádění útoků nákladnější. Kromě toho bude Komise úzce spolupracovat s členskými státy, aby se zajistilo, že donucovacím orgánům bude hlášeno více ransomwarových útoků, zejména pokročilých přetrvávajících hrozeb, a případů, kdy je požadováno zaplacení výkupného, což usnadní vyšetřování.

Aby bylo možné kybernetickým útokům předcházet a zastavit je, musí EU posílit výměnu informací mezi donucovacími orgány, orgány a subjekty v oblasti kybernetické bezpečnosti i soukromými subjekty pod záštitou Europolu a agentury ENISA.

Europol a Eurojust by měly i nadále stavět na úspěších, jichž dosáhly při likvidaci ransomwarových operací, a podporovat spolupráci při prosazování práva. Za tímto účelem by měly donucovací orgány maximálně využívat mechanismy spolupráce, včetně **mezinárodního modelu Europolu pro reakci na ransomware** a **mezinárodní iniciativy pro boj proti ransomwaru (CRI)**[43], a agentura ENISA a Europol by měly spolupracovat na rozšíření úložiště dešifrovacích nástrojů pro různé typy ransomwaru[44].

Technologická suverenita

Kybernetická bezpečnost a technologická suverenita jsou úzce propojeny a přednostně je třeba řešit technologické závislosti. Unie musí **řídit vývoj a zavádění nových technologií**, přičemž Komise pracuje na **posílení kapacit v oblasti strategických technologií**, jako je umělá inteligence, kvantová technologie, pokročilá konektivita, cloud, edge a internet věcí[45], prostřednictvím připravovaných iniciativ, jako je Akční plán pro kontinent umělé inteligence, Kvantová strategie a další[46]. Komise bude i nadále podporovat včasné zavádění nejnovějších dostupných mezinárodně dohodnutých **internetových protokolů**, které jsou nezbytné pro zachování škálovatelného a účinného internetu s vyšší úrovní kybernetické bezpečnosti. Další opatření jsou rovněž zapotřebí k řešení **problémů souvisejících s rádiovým spektrem**, například v souvislosti se spoofingem a rušením signálu GNSS a riziky a závislostmi v dodavatelských řetězcích, jako je využití technologií kvantového snímání a zkoumání vývoje kapacity pro monitorování rádiových kmitočtů.

Pro zabezpečení citlivých komunikací, uložených dat a pro ochranu digitálních identit v nové kvantové éře bude mít zásadní význam nasazení řešení **postkvantové kryptografie** (PQC). Na základě doporučení z roku 2024 o plánu pro koordinovanou implementaci přechodu na postkvantovou kryptografii[47] Komise spolupracuje s členskými státy na podpoře tohoto přechodu. V tomto ohledu by členské státy měly identifikovat vysoce rizikové případy u kritických subjektů a co nejdříve, nejpozději však do konce roku 2030, zajistit pro tyto vysoce rizikové případy kvantově bezpečné šifrování. Komise rovněž spolupracuje s členskými státy a Evropskou kosmickou agenturou (ESA) na vývoji a zavedení **evropské kvantové komunikační infrastruktury (EuroQCI)**[48] založené na kvantové distribuci klíčů (QKD) jako součásti **IRIS²**, programu EU pro bezpečnou konektivitu. Obě iniciativy nakonec umožní subjektům bezpečně přenášet data a ukládat informace.

Kvantové technologie budou hrát klíčovou roli také v bezpečnostních aplikacích: v rámci **Kvantové strategie** bude vypracován **plán pro kvantové snímání v bezpečnostních**

[43] https://counter-ransomware.org/.
[44] K dispozici prostřednictvím projektu No More Ransom, https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] Např. společný podnik EuropHPC, https://eurohpc-ju.europa.eu/index_en, Quantum Flagship, úvodní stránka Quantum Flagship | Quantum Flagship, sítě 3C (COM(2024) 81 final) a Akční plán EU o bezpečnosti kabelů (JOIN(2025) 9 final).
[47] Doporučení o plánu pro koordinovanou implementaci přechodu na postkvantovou kryptografii | Utváření digitální budoucnosti Evropy.
[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

aplikacích. Komise pracuje také na kvantovém zabezpečení svých kritických organizačních systémů, včetně IT systémů podléhajících utajení.

Rámec kybernetické bezpečnosti příznivý pro podnikání

Nadcházející revize aktu o kybernetické bezpečnosti je příležitostí ke **zjednodušení právních předpisů EU v oblasti kybernetické bezpečnosti** v souladu s Kompasem konkurenceschopnosti. Komise bude úzce spolupracovat s členskými státy, aby zajistila rychlé, konzistentní a pro podnikání příznivé provádění horizontálního rámce kybernetické bezpečnosti stanoveného ve směrnici NIS 2, aktu o kybernetické odolnosti a aktu o kybernetické solidaritě, přičemž bude podporovat jednoduchost a konzistentnost, aby nedocházelo k roztříštěnosti nebo duplicitě pravidel kybernetické bezpečnosti v právních předpisech EU a členských států.

S cílem umožnit bezpečný přístup k online službám a posílit digitální bezpečnost v celé EU nabídne **evropský rámec pro digitální identitu** do konce roku 2026 všem občanům a obyvatelům EU důvěryhodné peněženky digitální identity. Připravovaná **evropská podnikatelská peněženka** usnadní bezpečnou přeshraniční interakci mezi podniky a veřejnou správou. Obojí je předpokladem pro bezpečné a efektivnější fungování jednotného trhu založeného na datech, který obsahuje nástroje, jako je jednotná digitální brána, elektronická fakturace, elektronické zadávání zakázek a digitální pas výrobku.

Bezpečnost online

Některé z nejzávažnějších hybridních hrozeb, jež ohrožují bezpečnost lidí v Evropě a jsou namířeny proti demokratické sféře EU, se odehrávají online. Mezi tyto hrozby patří nezákonné činnosti a nezákonný obsah online, manipulace s informacemi zahrnující umělé zvyšování dosahu, zavádějící informace a zahraniční vměšování a manipulace s informacemi.

Zásadní význam pro zajištění bezpečného a přístupného online prostředí s odpovědnými subjekty, které je odolné i vůči hybridním hrozbám, má důsledné prosazování **aktu o digitálních službách**. Akt o digitálních službách ukládá poskytovatelům velmi velkých online platforem (VLOP) a velmi velkých internetových vyhledávačů (VLOSE) povinnost provést posouzení rizik a zavést opatření ke zmírnění systémových rizik plynoucích z koncepce, fungování nebo používání jejich služeb. Tato rizika mohou zahrnovat negativní dopady na občanský diskurz a volební procesy, jakož i na veřejnou bezpečnost, jako je dalekosáhlé vměšování zlovolných zahraničních státních aktérů, například do volebních procesů. Důležité je proškolení příslušných orgánů členských států v oblasti využívání právních nástrojů sloužících k rychlému odstraňování nezákonného obsahu online, zejména pokud jde o genderově podmíněné kybernetické násilí. Akt o digitálních službách stanoví mechanismus reakce na krize, který může být aktivován, když mimořádné okolnosti vedou k vážnému ohrožení veřejné bezpečnosti nebo veřejného zdraví v Unii nebo v jejích podstatných částech. Jako doplněk k tomuto mechanismu Komise a příslušné vnitrostátní orgány určené jako koordinátoři digitálních služeb rovněž vypracovaly dobrovolný **rámec pro reakci na incidenty podle aktu o digitálních službách**. Koordinátoři digitálních služeb rovněž přijali opatření, která mají pomoci chránit integritu voleb, například pořádáním volebních kulatých stolů a zátěžových testů[49]. Akt o digitálních službách spolu s nařízením o politické reklamě[50] představuje jeden z několika aspektů spojených s ochranou demokracie a integrity

[49] Soubor volebních nástrojů podle aktu o digitálních službách pro koordinátory digitálních služeb 2025, https://digital-strategy.ec.europa.eu/cs/library/dsa-elections-toolkit-digital-services-coordinators.

[50] Nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy (Úř. věst. L, 2024/900, 20.3.2024).

demokratických procesů, které jsou zranitelné vůči nepřátelským aktérům, a to i prostřednictvím digitálních nástrojů a sociálních médií.

Další důležitou složkou, která nabízí klíčovou podporu na úrovni EU, je zavedení souboru nástrojů **proti zahraničnímu vměšování a manipulaci s informacemi**. Ústředním prvkem těchto snah je také podpora digitální a mediální gramotnosti a kritického myšlení[51].

Boj proti zneužívání migrace jako zbraně

Rusko s pomocí a rozhodnou podporou Běloruska cíleně zneužívá migraci jako zbraň a nezákonně usnadňuje migrační toky směrem k vnějším hranicím EU s cílem destabilizovat naši společnost a podkopat jednotu Evropské unie. To ohrožuje nejen národní bezpečnost a svrchovanost členských států, ale také bezpečnost a integritu schengenského prostoru a bezpečnost Unie jako celku. Evropská rada ve svých závěrech z října 2024 zdůraznila, že Rusku a Bělorusku ani žádné jiné zemi nelze dovolit zneužívat naše hodnoty, včetně práva na azyl, a oslabovat naši demokracii.

Jak se uvádí ve sdělení Komise z roku 2024 o zneužívání migrace jako zbraně, Unie kromě silné politické podpory přijala finanční, operativní a diplomatická opatření, včetně spolupráce se zeměmi původu a tranzitu, aby těmto hrozbám účinně čelila[52]. Tato reakce spočívá ve využití nového rámce zavedeného Radou k sankcionování osob a organizací zapojených do činností a politik, jako je zneužívání migrace jako zbraně ze strany Ruska, prostřednictvím zmrazení majetku a zákazu cestování[53]. EU bude tento rámec v případě potřeby nadále využívat a podporovat členské státy v boji proti této hrozbě.

Bezpečnost dopravy

Námořní přístavy, letiště a pozemní infrastruktura představují klíčové vstupní a výstupní body. Hrají zásadní roli v ekonomice a společnosti EU a jsou nezbytné pro vojenskou mobilitu. Tyto dopravní uzly a prostředky jsou však také hlavním cílem vnějších hrozeb a trestné činnosti. Nedávné incidenty, včetně narušení bezpečnosti letecké nákladní dopravy a útoků na železniční infrastrukturu, poukazují na vážná rizika. **Dopravci** mohou být cílem i nástrojem zlovolných aktérů. Stávající právní nástroje EU posílily ochranu letectví před protiprávními činy[54], avšak vysoká míra ohrožení civilního letectví vyžaduje prostředky pro předvídání incidentů a rychlé konzultace s příslušnými členskými státy. Komise bude spolupracovat s členskými státy na změně stávajících prováděcích právních předpisů v oblasti ochrany letectví před protiprávními činy, aby bylo možné sdílet utajované informace o **incidentech v oblasti ochrany letectví**. Kromě toho Komise zváží **regulační opatření** k řešení nových hrozeb, jako jsou **incidenty v nákladní letecké dopravě**, a k posílení norem v oblasti ochrany letectví před protiprávními činy. To bude zahrnovat také posílení **právních předpisů v oblasti ochrany letectví před protiprávními činy (AVSEC)**, aby bylo možné okamžitě reagovat opatřeními a zároveň zachovat jednotný bezpečnostní prostor na letištích EU.

Při přípravě nadcházející **Strategie EU pro přístavy**, která vychází z **Evropské aliance přístavů**, Komise prozkoumá způsoby dalšího posílení právních předpisů v oblasti námořní bezpečnosti, aby bylo možné účinně čelit vznikajícím hrozbám, zabezpečit přístavy a zvýšit bezpečnost dodavatelských řetězců EU. Za tímto účelem Komise zajistí její důkladné provádění a bude pracovat na harmonizaci vnitrostátních postupů a posílení bezpečnostních kontrol v

[51] Akční plán digitálního vzdělávání (2021–2027) – Evropský prostor vzdělávání.
[52] COM(2024) 570 final.
[53] Nařízení Rady (EU) 2024/2642 ze dne 8. října 2024 o omezujících opatřeních vzhledem k destabilizujícím činnostem Ruska, ST/8744/2024/INIT (Úř. věst. L, 2024/2642, 9.10.2024).
[54] Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy (Úř. věst. L 97, 9.4.2008, s. 72).

přístavech. V návaznosti na bezpečnostní protokoly zavedené pro leteckou nákladní dopravu bude Komise spolupracovat s členskými státy a soukromým sektorem na rozšíření těchto protokolů i na zabezpečení řetězců námořní dopravy.

Navrhovaný Celní úřad EU bude analyzovat a posuzovat rizika na základě **celních informací** týkajících se zboží, které do EU vstupuje, opouští ji a je přes ni přepravováno, aby podpořil členské státy v jejich úsilí předcházet zneužívání mezinárodních dodavatelských řetězců zlovolnými aktéry. V souladu se Strategií EU pro námořní bezpečnost[55] bude hrát klíčovou roli při posilování námořní bezpečnosti v přímořských oblastech kolem EU i mimo ni připravovaný **Evropský pakt pro oceány**, mimo jiné prostřednictvím podpory rozšiřování víceúčelových námořních operací a cvičení.

Odolnost dodavatelských řetězců

Evropa musí zredukovat využívání technologií třetích zemí, které může vést k závislosti a bezpečnostním rizikům. Cílem Komise je zmírnit závislost na jednotlivých zahraničních dodavatelích, snížit riziko v našich dodavatelských řetězcích plynoucí z vysoce rizikových dodavatelů a zabezpečit kritickou infrastrukturu a průmyslové kapacity na území EU, jak je uvedeno v **Kompasu konkurenceschopnosti[56]** a v **Dohodě o čistém průmyslu[57]**. Komise bude podporovat **průmyslovou politiku pro vnitřní bezpečnost** prostřednictvím spolupráce s průmyslovými podniky EU v klíčových odvětvích (např. dopravní uzly, kritické infrastruktury), aby vytvářely bezpečnostní řešení, jako jsou detekční zařízení, biometrické technologie a drony, které budou zahrnovat bezpečnostní prvky již od fáze návrhu. Při **revizi pravidel EU pro zadávání veřejných zakázek** Komise posoudí, zda jsou bezpečnostní aspekty ve směrnici o zadávání veřejných zakázek v oblasti obrany a bezpečnosti z roku 2009[58] dostatečné pro řešení potřeb v oblasti prosazování práva a odolnosti kritických subjektů.

Komise podpoří členské státy při **prověřování přímých zahraničních investic** a při pořizování vybavení pro logistické uzly, čímž zajistí, aby kritická infrastruktura a technologie zůstaly bezpečné.

Jakmile vstoupí v platnost **akt pro odolnost a mimořádné situace na vnitřním trhu (IMERA)**, pomůže Evropské unii zvládat krize, které narušují kritické dodavatelské řetězce a volný pohyb zboží, služeb a osob. Umožní rychlou koordinaci v krizových situacích, identifikaci krizově relevantního zboží a služeb a poskytne soubor nástrojů k zajištění jejich dostupnosti. Kromě toho Komise v úzké spolupráci s členskými státy navrhne zřízení **mnohostranného mechanismu varování v oblasti bezpečnosti dopravy a dodavatelských řetězců**, který zaručí bezpečné a včasné sdílení relevantních informací nezbytných k předvídání hrozeb a boji proti nim.

Nadto, díky provádění nařízení o kritických surovinách a aktu o průmyslu pro nulové čisté emise, širší využívání kritérií udržitelnosti, odolnosti a evropských preferencí v oblasti zadávání veřejných zakázek v EU podpoří rozvoj rozhodujících trhů. Posílení obchodních vazeb, například prostřednictvím partnerství v oblasti surovin a partnerství v oblasti čistého obchodu a investic, pak přispěje k diverzifikaci dodavatelských řetězců.

Odolnost a připravenost na chemické, biologické, radiologické a jaderné hrozby

[55] JOIN(2023) 8 final.
[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Směrnice 2009/81/ES o koordinaci postupů při zadávání některých zakázek na stavební práce, dodávky a služby zadavateli v oblasti obrany a bezpečnosti (Úř. věst. L 216, 20.8.2009).

Ruská útočná válka proti Ukrajině zvýšila riziko **chemických, biologických, radiologických a jaderných (CBRN) hrozeb**. Komise bude podporovat členské státy a partnerské země prostřednictvím specializovaných školení a cvičení s cílem čelit potenciálnímu získávání a zneužívání CBRN materiálů jako zbraně. Komise rovněž posílí připravenost a schopnost reakce v oblasti CBRN, a to stanovením prioritních hrozeb, inovativním financováním protiopatření, kapacitami rescEU a vytvářením zásob lékařských protiopatření v rámci nového **Akčního plánu připravenosti a reakce v oblasti CBRN**. Kromě toho bude **Strategie EU v oblasti lékařských protiopatření** podporovat vývoj lékařských protiopatření od výzkumu až po výrobu a distribuci, aby se EU chránila před pandemiemi a CBRN hrozbami.

Na základě zkušeností s pandemií COVID-19 posílila EU rámec zdravotní bezpečnosti[59]. Komise určuje referenční laboratoře EU v oblasti veřejného zdraví s cílem posílit kapacity EU a členských států v oblasti dohledu a rychlého odhalování. V roce 2025 bude zveřejněn Plán Unie pro připravenost, prevenci a reakci v oblasti zdravotní bezpečnosti.

Klíčová opatření

Komise:

- **v roce 2025 přezkoumá a zrevidiuje akt o kybernetické bezpečnosti**
- **vypracuje opatření k zajištění kyberneticky bezpečného využívání cloudových služeb**
- **v roce 2025 navrhne Strategii EU pro přístavy**
- **v roce 2026 zrevidiuje pravidla EU pro zadávání veřejných zakázek v oblasti obrany a bezpečnosti**
- **v roce 2026 předloží nový Akční plán připravenosti a reakce v oblasti CBRN**

Komise ve spolupráci s členskými státy:

- **vyvine a zavede evropskou kvantovou komunikační infrastrukturu (EuroQCI)**
- **zajistí účinné prosazování aktu o digitálních službách**
- **bude bojovat proti zneužívání migrace jako zbraně**
- **zavede informační systém o incidentech v oblasti ochrany letectví**
- **bude pracovat na vytvoření mnohostranného mechanismu varování v oblasti bezpečnosti dopravy a dodavatelských řetězců**

Komise vyzývá Radu, aby:

- **přijala doporučení Rady o kybernetickém plánu EU**

Členské státy se vyzývají, aby:

- **transponovaly a v plném rozsahu prováděly směrnice CER a NIS 2**

5. Utáhnutí sítě kolem závažné a organizované trestné činnosti

Pomůžeme vymýtit organizovanou trestnou činnost tím, že navrhneme přísnější pravidla pro boj proti organizovaným zločineckým skupinám, včetně vyšetřování, snížíme náchylnost mladých lidí v EU k náboru pro trestnou činnost a zintenzivníme opatření, která omezují přístup k nástrojům a majetku používaným při páchání trestné činnosti.

Organizovaná trestná činnost těží ze stále se měnícího prostředí a exponenciálně se šíří. Využívá pokročilé technologie, je aktivní v různých jurisdikcích a má silné vazby za hranicemi

[59] Zejména prostřednictvím nařízení (EU) 2022/2371 o vážných přeshraničních zdravotních hrozbách.

EU. Vzhledem k těmto komplexním nadnárodním hrozbám je koordinace a podpora na úrovni EU zásadní.

Prevence trestné činnosti

Nábor mladých lidí pro organizovanou trestnou činnost je v EU stále větším problémem. Boj proti organizované trestné činnosti vyžaduje řešení jejích **základních příčin** nabídkou vzdělávání a alternativ k dráze zločinu, a to prostřednictvím celospolečenského přístupu. Komise bude podporovat začlenění bezpečnostních aspektů do vzdělávací, sociální, zaměstnanecké a regionální politiky EU. EU bude **podporovat politiky prevence kriminality založené na důkazech**[60] a přizpůsobené místním podmínkám.

V zájmu ochrany uživatelů online služeb, zejména nezletilých osob, mimo jiné před osobami, které se dopouštějí pohlavního zneužívání dětí, obchodníky s lidmi a online náborem pro trestnou činnost nebo násilný extremismus, vyžadují opatření podle **aktu o digitálních službách**, aby poskytovatelé online platforem přístupných nezletilým osobám řídili rizika a reagovali na nezákonný obsah, včetně nenávistných projevů. Komise plánuje vydat **pokyny k ochraně nezletilých osob**, které mají poskytovatelům online platforem pomoci zajistit vysokou úroveň ochrany soukromí a bezpečnosti nezletilých osob na internetu. Tyto pokyny budou obsahovat soubor doporučení pro všechny digitální služby provozované v Unii, aby se zvýšila ochrana nezletilých osob na internetu. V roce 2025 Komise rovněž plánuje usnadnit řešení EU pro **ověřování věku chránící soukromí**, které vyplní mezeru před unijní peněženkou digitální identity, jež bude k dispozici do konce roku 2026. Komise rovněž předloží Akční plán proti kyberšikaně.

Komise bude dále podporovat dobrovolné zapojení různých zainteresovaných stran do činnosti online platforem a dalších relevantních aktérů, mimo jiné prostřednictvím internetového fóra EU a cílených kodexů chování podle aktu o digitálních službách, jako je například Kodex chování z roku 2025 proti nezákonným nenávistným projevům online. Cílem je zvyšovat informovanost, společně reagovat na současné a nově vznikající hrozby a vytvářet a sdílet osvědčené postupy pro jejich zmírnění.

Dopad organizované trestné činnosti na místní úrovni zdůrazňuje potřebu regionálních řešení, která by snížila zranitelnost a přitažlivost nelegálních činností. Bezpečnostními problémy ve městech se bude zabývat Agenda EU pro města, jež naváže na unijní iniciativu Města proti radikalizaci. Komise bude podporovat členské státy při zvyšování bezpečnosti měst a regionů prostřednictvím Evropského fondu pro regionální rozvoj.

Předpokladem odolné a soudržné společnosti jsou silnější základy vzdělání a dovednosti. Prostřednictvím **unie dovedností** a **Akčního plánu pro integraci a začleňování** bude Unie pracovat na tom, aby pomohla lidem stát se odolnějšími vůči misinformacím a dezinformacím, radikalizaci a náboru pro trestnou činnost.

Jedním z hlavních cílů EU je ochrana dětí před všemi formami násilí, včetně trestné činnosti, fyzického nebo psychického násilí, a to jak online, tak offline. S cílem řešit specifické potřeby obzvláště zranitelných skupin, jako jsou děti, které jsou stále více vystaveny náboru a radikalizaci, groomingu a pohlavnímu zneužívání, kyberšikaně, dezinformacím a dalším hrozbám, vypracuje EU **Akční plán na ochranu dětí před trestnou činností**, který bude zahrnovat online i offline aspekty. Tento plán stanoví konzistentní a koordinovaný přístup založený na dostupných rámcích a nástrojích, včetně budoucího Střediska EU pro prevenci a potírání pohlavního zneužívání dětí a dalších institucí a subjektů EU, a navrhne další postup v případě přetrvávajících nedostatků.

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

Rozbití zločineckých sítí a jejich podporovatelů

Je třeba zintenzivnit boj proti vysoce rizikovým zločineckým sítím, jejich vůdcům a podporovatelům. Nedávné úspěchy jsou sice pozoruhodné,[61] ale zastaralá pravidla a nejednotné definice zločineckých sítí brání účinné reakci trestního soudnictví a přeshraniční spolupráci. Komise přezkoumá zastaralé právní předpisy v této oblasti a navrhne obnovený **právní rámec pro boj proti organizované trestné činnosti** s cílem tuto reakci posílit.

Prosazování práva mohou doplňovat správní opatření, která přinášejí rychlejší výsledky – jak ukázal úřad EPPO a úřad OLAF při řešení **přeshraničních podvodů a trestných činů proti finančním zájmům EU**. Podvodníci s dotacemi se zaměřují na odvětví, jako jsou obnovitelné zdroje energie, výzkumné programy a zemědělství[62]. Komise prozkoumá způsoby koordinace využívání trestněprávních a správních nástrojů a posílí spolupráci s Europolem, Eurojustem a úřadem EPPO. Komise bude širší uplatňování **správního přístupu** i nadále podporovat, aby místní a další správní orgány měly možnost narušit pronikání trestné činnosti[63].

EU pracuje na posílení svého právního rámce pro boj proti **korupci**[64]. Evropský parlament a Rada by měly urychleně dokončit jednání o aktualizovaném protikorupčním rámci navrženém Komisí. Komise předloží Protikorupční strategii EU, která podpoří integritu a posílí koordinaci mezi všemi příslušnými orgány a z zainteresovanými stranami v této oblasti.

Klíčovým faktorem umožňujícím rostoucí násilí páchané organizovanými zločineckými skupinami jsou palné zbraně. Komise navrhne společné trestněprávní normy proti nedovolenému obchodu s palnými zbraněmi. Nový **Akční plán EU proti nedovolenému obchodu s palnými zbraněmi** bude zacílen na ochranu legálního trhu a omezení trestné činnosti na základě lepších zpravodajských informací a posílení mezinárodní spolupráce se zvláštním zaměřením na Ukrajinu a západní Balkán.

Nelegálně obchodovaná pyrotechnika používaná při trestné činnosti vyžaduje opatření ke zlepšení prevence a vysledovatelnosti. Komise v současnosti vyhodnocuje směrnici o pyrotechnických výrobcích a zváží rovněž **trestní postihy za nedovolený obchod s pyrotechnikou**.

Sledování toku peněz

Sledování toku peněz je v boji proti organizované trestné činnosti a terorismu klíčové, přesto je stále velmi náročné. Spojení mezi organizovanou trestnou činností a toky peněz vyžaduje intenzivní a společné úsilí, aby se zločineckým sítím zamezil přístup k finančním zdrojům a aby se lépe chránili lidé, podniky a veřejné rozpočty.

EU posílila své úsilí novými pravidly proti praní peněz, včetně zřízení **orgánu AMLA**[65]. Pro provádění účinných finančních vyšetřování je nezbytná spolupráce mezi orgánem AMLA, úřadem OLAF, úřadem EPPO, Eurojustem a Europolem. Komise bude podporovat vytváření **partnerství**, a to jak partnerství, která usnadňují spolupráci mezi agenturami, tak partnerství, která zahrnují soukromý sektor.

[61] Včetně nedávných případů EMPACT.
[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.
[64] Návrh směrnice Evropského parlamentu a Rady o boji proti korupci, kterou se nahrazuje rámcové rozhodnutí Rady 2003/568/SVV a Úmluva o boji proti korupci úředníků Evropských společenství nebo členských států Evropské unie a kterou se mění směrnice Evropského parlamentu a Rady (EU) 2017/1371, COM(2023) 234 final, Brusel, 3.5.2023.
[65] https://www.amla.europa.eu/index_cs.

K odstranění finančních motivů stojících za organizovanou trestnou činností je nezbytné zabavovat majetek a konfiskovat zisky z trestné činnosti. Členské státy by měly neprodleně transponovat nedávno přijatá přísnější pravidla pro **vymáhání a konfiskaci majetku**[66] a plně využívat jejich potenciál. Inovativní opatření, osvědčené postupy sdílené mezi členskými státy a větší podporu ze strany Europolu a Eurojustu vyžaduje rovněž boj proti paralelním finančním systémům, které obcházejí rámec EU pro boj proti praní peněz, včetně systémů založených na kryptoměnách. Komise prozkoumá možnost vytvoření nového celounijního systému pro sledování zisků z organizované trestné činnosti a financování terorismu a rovněž podpoří včasný a rozšířený tok informací od **finančních zpravodajských jednotek** k donucovacím orgánům. Komise prozkoumá způsoby, jak odstranit mezery v právních předpisech, podpoří členské státy při budování kapacit a bude dále pracovat na posílení spolupráce se třetími zeměmi, které zločinci zneužívají pro nelegální bankovní operace.

Boj proti závažné trestné činnosti

Kromě rozbití zločineckých sítí vyžaduje boj proti závažné trestné činnosti také cílené úsilí. V zájmu posílení naší schopnosti bojovat proti **podvodům na internetu**, které způsobují velmi značné finanční škody[67], bude Komise podporovat preventivní opatření a účinnější prosazování práva a bude spolupracovat s členskými státy a zainteresovanými stranami na podpoře a ochraně obětí, včetně pomoci při vymáhání jejich finančních prostředků. Toto úsilí bude formalizováno v **Akčním plánu pro boj proti podvodům na internetu**.

V návaznosti na Strategii EU pro boj proti **pohlavnímu zneužívání dětí** na období 2020–2025[68] bude Komise podporovat spolunormotvůrce při finalizaci dvou legislativních návrhů[69], jejichž cílem je předcházet pohlavnímu zneužívání dětí na internetu a bojovat proti němu a zefektivnit činnost donucovacích orgánů v boji proti pohlavnímu zneužívání a vykořisťování dětí. Vzhledem k tomu, že prozatímní pravidla platí do dubna 2026, je nezbytné vytvořit trvalý právní rámec a Komise vyzývá spolunormotvůrce, aby zahájili jednání o návrhu nařízení, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu. Spolunormotvůrci se rovněž vyzývají, aby přikročili k jednání o směrnici o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti materiálům pohlavního zneužívání dětí, která stanoví minimální pravidla pro definici trestných činů a sankce v oblasti pohlavního vykořisťování dětí.

Polovina nejnebezpečnějších zločineckých sítí v EU je zapojena do násilného **obchodu s drogami**. Ačkoli EU v poslední době svůj boj proti této trestné činnosti posílila[70], zejména rozšířením mandátu **Agentury EU pro drogy**, jsou nutná další opatření. Komise v úzké spolupráci s členskými státy navrhne novou **Protidrogovou strategii EU**. Rovněž zreviduje **právní rámec pro prekurzory drog** a navrhne **Akční plán EU pro boj proti obchodu s drogami** s cílem narušit trasy a obchodní modely. **Partnerství veřejného a soukromého sektoru v rámci Aliance přístavů EU** pro posílenou ochranu přístavů bude rozšířeno na menší a vnitrozemské přístavy a zajistí prosazování pravidel námořní bezpečnosti. Komise si je vědoma závažných místních dopadů obchodu s drogami, a proto bude i nadále podporovat vyváženou, na důkazech založenou a multidisciplinární protidrogovou politiku, která bude připravena na náhlý příliv drog, zejména syntetických opioidů.

[66] Směrnice Evropského parlamentu a Rady (EU) 2024/1260 ze dne 24. dubna 2024 o vymáhání a konfiskaci majetku (Úř. věst. L, 2024/1260, 2.5.2024).
[67] Zpráva organizace Global Anti-Scam Alliance z roku 2024.
[68] COM(2020) 607 final.
[69] COM(2022) 209 final a COM(2024) 60 final.
[70] COM(2023) 641 final.

Za účelem boje proti vykořisťování lidí přijala EU nová pravidla[71] a zavede **obnovenou Strategii EU pro boj proti obchodování s lidmi** (2026–2030), která bude zahrnovat všechny fáze od prevence až po stíhání a zaměří se na podporu obětí na úrovni EU i na mezinárodní úrovni.

V boji proti **převaděčství migrantů** bude Komise stát v čele společně s klíčovými partnery prostřednictvím nové Globální aliance pro boj proti převaděčství migrantů, ve spolupráci s Europolem, Eurojustem a Frontexem, a to i v online dimenzi. Je třeba neprodleně přijmout a provést legislativní návrhy Komise týkající se boje proti převaděčství[72]. Kromě toho Komise v návaznosti na přijetí **souboru nástrojů pro dopravce**[73] zintenzivnila navazování kontaktů se zahraničními orgány a dopravci a bude i nadále spolupracovat s leteckým průmyslem a organizacemi civilního letectví[74] s cílem zvýšit informovanost o převaděčství migrantů leteckou dopravou[75].

Trestná činnost proti životnímu prostředí v dlouhodobém měřítku ohrožuje životní prostředí, veřejné zdraví a ekonomiku. Komise bude podporovat členské státy při provádění směrnice o trestněprávní ochraně životního prostředí[76] a posilovat operativní sítě a opatření v této oblasti[77]. Zásadní je důsledné prosazování práva. Nedávno přijatá Úmluva Rady Evropy o trestněprávní ochraně životního prostředí[78] navíc pomůže zajistit silné a srovnatelné úsilí při potírání trestné činnosti proti životnímu prostředí v Evropě i mimo ni.

Reakce trestního soudnictví

Kriminalita a terorismus mohou mít dopad na každého, a proto je nezbytné podporovat a chránit práva **obětí**, aby se snížila újma a zvýšila celková bezpečnost a důvěra v úřady. V návaznosti na směrnici o právech obětí Komise vypracuje novou **Strategii EU pro práva obětí**.

Systémy trestního soudnictví EU potřebují účinné nástroje k řešení vznikajících hrozeb. Za tímto účelem Komise zřídila **Fórum na vysoké úrovni o budoucnosti trestního soudnictví v EU**. Toto fórum sdružuje členské státy, Evropský parlament, instituce a jiné subjekty EU a další relevantní zainteresované strany. Jeho cílem je diskutovat o způsobech, jak zajistit, aby naše systémy trestního soudnictví zůstaly účinné, spravedlivé a odolné vůči vyvíjejícím se výzvám, a zároveň posílit justiční spolupráci a zvýšit vzájemnou důvěru, a to i prostřednictvím digitalizace[79].

Klíčová opatření

Komise:

[71] Směrnice (EU) 2024/1712 ze dne 13. června 2024, kterou se mění směrnice 2011/36/EU o prevenci obchodování s lidmi, boji proti němu a o ochraně obětí (Úř. věst. L, 2024/1712, 24.6.2024).
[72] COM(2023) 755 final a COM(2023) 754 final.
[73] Soubor nástrojů zaměřený na využívání komerčních dopravních prostředků pro usnadňování nelegální migrace do EU.
[74] Včetně Mezinárodní organizace pro civilní letectví (ICAO).
[75] Komise rovněž podpoří finalizaci nařízení o opatřeních vůči dopravcům, kteří usnadňují nebo vykonávají obchodování s lidmi nebo převaděčství migrantů, COM(2021) 753 final.
[76] Směrnice Evropského parlamentu a Rady (EU) 2024/1203 ze dne 11. dubna 2024 o trestněprávní ochraně životního prostředí (Úř. věst. L, 2024/1203, 30.4.2024).
[77] Síť EU pro provádění a prosazování práva v oblasti životního prostředí (IMPEL), Evropská síť státních zástupců pro životní prostředí (ENPE), síť EnviCrimeNet a Fórum soudců EU pro životní prostředí (EUFJE).
[78] Výbor expertů na trestněprávní ochranu životního prostředí (PC-ENV) – Evropský výbor pro trestní problematiku.
[79] Zejména zřízením systému komunikace v oblasti e-justice prostřednictvím online výměny dat (eCODEX) a Evropského informačního systému rejstříků trestů pro státní příslušníky třetích zemí (ECRIS-TCN).

- **v roce 2026 předloží legislativní návrh modernizovaných pravidel pro boj proti organizované trestné činnosti**
- **v roce 2025 předloží legislativní návrh na revizi právního rámce pro prekurzory drog**
- **v roce 2025 předloží legislativní návrh společných trestněprávních norem proti nedovolenému obchodu s palnými zbraněmi**
- **posoudí potřebu revize směrnic o pyrotechnických výrobcích a výbušninách pro civilní použití**
- **posoudí potřebu dalšího posílení evropského vyšetřovacího příkazu a evropského zatýkacího rozkazu**
- **v roce 2026 předloží novou Strategii EU pro boj proti obchodování s lidmi**
- **v roce 2026 předloží novou Strategii EU pro práva obětí**
- **do roku 2027 předloží Akční plán EU na ochranu dětí před trestnou činností**
- **v roce 2025 předloží Akční plán EU proti obchodu s drogami**
- **v roce 2026 předloží Akční plán EU proti nedovolenému obchodu s palnými zbraněmi**
- **od roku 2025 bude postupně rozšiřovat Alianci přístavů EU**
- **v roce 2026 přijme pokyny k ochraně nezletilých osob podle aktu o digitálních službách**
- **v roce 2026 předloží Akční plán EU proti kyberšikaně**

Členské státy se vyzývají, aby:

- **do konce roku 2026 plně transponovaly nová pravidla pro vymáhání a konfiskaci majetku a plně využívaly jejich potenciál**
- **zavedly správní přístup v boji proti pronikání trestné činnosti**
- **vytvořily partnerství veřejného a soukromého sektoru proti praní peněz**
- **transponovaly a v plném rozsahu prováděly směrnici o prevenci a potírání násilí vůči ženám a domácího násilí**

Evropský parlament a Rada se vyzývají, aby:

- **přikročily k jednání o nařízení, kterým se stanoví pravidla pro předcházení pohlavnímu zneužívání dětí a boj proti němu, a o směrnici o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti materiálům pohlavního zneužívání dětí**
- **dokončily jednání o směrnici o boji proti korupci**

6. Boj proti terorismu a násilnému extremismu

Zavedeme ucelenou agendu boje proti terorismu, abychom zabránili radikalizaci, zabezpečili online prostor i veřejný prostor, omezili kanály financování a dokázali reagovat na případné útoky.

Hrozba terorismu v EU je i nadále vysoká. Úzce souvisí s vedlejšími účinky geopolitických událostí, nových technologií a nových způsobů financování terorismu. Musíme zajistit, aby EU měla dostatečné zdroje k předvídání hrozeb, prevenci radikalizace (offline i online), ochraně občanů a veřejného prostoru před útoky a k účinné reakci, když k nim dojde. V roce 2025 bude předložena **nová Agenda EU pro předcházení terorismu a násilnému extremismu a boj proti nim**, v níž budou stanovena budoucí opatření EU. V souladu s touto novou agendou podepíší EU a západní Balkán v roce 2025 nový **Společný akční plán** pro předcházení terorismu a násilnému extremismu a boj proti nim.

Prevence radikalizace a ochrana osob online

Podobně jako boj proti organizované trestné činnosti začíná boj proti terorismu a násilnému extremismu **řešením jeho základních příčin**. **Znalostní centrum EU pro prevenci radikalizace** posílí svou podporu odborníkům z praxe a tvůrcům politik pomocí nového **uceleného souboru nástrojů prevence**, který umožní včasnou identifikaci a intervence zaměřené na zranitelné osoby, zejména na nezletilé. K radikalizaci často dochází ve věznicích, a tak Komise vydá nová doporučení, aby podpořila členské státy při řešení této problematiky.

Teroristé a násilní extremisté využívají online platformy k šíření teroristického a škodlivého obsahu, shromažďování finančních prostředků a náboru nových členů. Na internetu jsou alarmujícím tempem radikalizováni zranitelní uživatelé, zejména nezletilí. V boji proti šíření teroristického obsahu online se osvědčilo **nařízení proti teroristickému obsahu online**, které umožňuje rychlé odstranění nejodpornějších a nejnebezpečnějších materiálů[80]. Komise v současnosti vyhodnocuje jeho fungování a posoudí, jak nejlépe tento rámec posílit.

Krizový protokol EU pro společnou a rychlou reakci donucovacích orgánů a technologického průmyslu v souvislosti s teroristickým útokem bude změněn tak, aby byla zajištěna škálovatelnost a flexibilita reakce na rostoucí online rozměr teroristických útoků. Hlavním nástrojem dobrovolné spolupráce s technologickým průmyslem v oblasti boje proti teroristickému a škodlivému obsahu online bude i nadále Internetové fórum EU. Kromě toho se Komise zapojuje do mezinárodních iniciativ, jako je nadace Christchurch Call a Globální internetové fórum pro boj proti terorismu (GIFCT).

Boj proti financování terorismu

Teroristé financují své aktivity pomocí kampaní skupinového financování, kryptoaktiv, neobank nebo online platebních platforem. Donucovací orgány musí tyto finanční toky odhalovat a vyšetřovat. To vyžaduje prostředky, nástroje a odborné znalosti. Klíčovou roli hraje **síť finančních vyšetřovatelů pro boj proti terorismu**. Komise prozkoumá možnost vytvoření **nového celounijního systému pro sledování financování terorismu**, který by zahrnoval transakce v rámci EU a SEPA, převody kryptoaktiv a online a bezhotovostní platby a který by doplnil Dohodu mezi EU a USA o Programu sledování financování terorismu (TFTP).

Rozpočet EU musí být **chráněn před zneužitím k podpoře radikálních/extremistických názorů** v členských státech. Revidované **finanční nařízení** nyní zahrnuje jako důvod pro vyloučení z financování EU odsouzení za „vyzývání k diskriminaci, nenávisti nebo násilí“. Komise bude i nadále zkoumat, jak by bylo možné tento soubor nástrojů v plném rozsahu nejlépe využít, a to i při výběru potenciálních příjemců. Ochrana rozpočtu EU závisí také na silné spolupráci a sdílení informací s vnitrostátními orgány, institucemi a jinými subjekty EU.

Ochrana před útoky

Kromě investic do prevence radikalizace je důležitou součástí ochrany občanů omezení prostředků, které teroristům a zločincům umožňují páchat útoky. Je třeba přijmout opatření jak v oblasti nástrojů, které teroristé používají, tak v oblasti ochrany cílů ohrožených útokem.

Kromě opatření týkajících se palných zbraní Komise rovněž **přezkoumá pravidla** týkající se **prekurzorů výbušnin**, aby zahrnovala vysoce rizikové chemické látky. Nejčastějším cílem teroristických útoků, zejména pro osamělé aktéry, zůstává **veřejný prostor**. V zájmu ochrany občanů před újmou bude posílen **poradenský program EU pro ochranu bezpečnosti**, který na žádost členských států provádí hodnocení zranitelnosti veřejného prostoru, kritické

[80] Do 31. prosince 2024 bylo vydáno 1 426 příkazů k odstranění teroristického obsahu nebo k zablokování přístupu k němu, přičemž velká většina z nich se týkala džihádistického teroristického obsahu, ale také pravicového teroristického obsahu.

infrastruktury a vysoce rizikových akcí a je financován z rozpočtu EU v rámci Fondu pro vnitřní bezpečnost. EU bude usilovat o navýšení dostupných finančních prostředků na ochranu veřejného prostoru. Komise nabízí podporu orgánům členských států a soukromým subjektům prostřednictvím specializovaných pokynů a nástrojů, jako je Znalostní centrum pro ochranu veřejného prostoru[81], a od roku 2020 již na tuto podporu ochrany veřejného prostoru uvolnila 70 milionů EUR.

Komise rovněž prozkoumá možnost zavedení požadavků na organizace, aby zvážily nebo přijaly bezpečnostní opatření na veřejně přístupných místech, a to ve spolupráci s místními orgány a soukromými partnery

Vzhledem ke zjevné zranitelnosti se bude činnost Komise v oblasti ochrany židovské komunity i nadále řídit **Strategií EU pro boj proti antisemitismu a podporu židovského života (2021–2030)**. Komise rovněž zajistí, aby byly k dispozici vhodné nástroje na podporu členských států v boji proti **nenávisti vůči muslimům**.

Stále větší bezpečnostní výzvu představuje využívání **dronů** ke špionáži a útokům. Komise vypracuje **harmonizovanou metodiku testování protidronových systémů**, zřídí **Centrum excelence pro protidronovou obranu** a posoudí potřebu harmonizovat právní předpisy a postupy členských států[82].

Zahraniční terorističtí bojovníci

K identifikaci zahraničních teroristických bojovníků, kteří se vracejí do EU nebo do ní vstupují na jejích vnějších hranicích, jsou zapotřebí údaje o osobách představujících teroristickou hrozbu. Za tímto účelem Komise společně s Europolem posílí **spolupráci s klíčovými třetími zeměmi, aby získala biografické a biometrické údaje o osobách, které by mohly představovat teroristickou hrozbu**, včetně zahraničních teroristických bojovníků, které pak mohou být vloženy do Schengenského informačního systému v plném souladu s platnými právními rámci EU a členských států. Je proto nezbytné, aby členské státy využívaly všechny stávající nástroje. To zahrnuje vkládání všech relevantních informací do **Schengenského informačního systému**, posílení biometrických kontrol a provádění povinných systematických kontrol všech osob na vnějších hranicích EU[83]. Kromě toho budou orgánům ochrany hranic členských států při identifikaci a posuzování rizika podezřelých cest potenciálních zahraničních teroristických bojovníků i nadále nápomocny **společné ukazatele rizik (CRI)** vyvinuté Frontexem.

Kromě toho Komise společně s Eurojustem posoudí možnost ukládat tyto důkazy do Databáze důkazů o nejzávažnějších mezinárodních zločinech zřízené Eurojustem, aby si členské státy zachovaly přístup k **důkazům z bojišť** shromážděným vyšetřovacím týmem OSN pro prosazování odpovědnosti za trestné činy spáchané organizací Dá'iš/ISIL (UNITAD) pro účely stíhání zahraničních teroristických bojovníků. Justiční orgány členských států budou pro rychlou identifikaci přeshraničních vazeb v případech terorismu také moci využívat nový evropský **justiční rejstřík pro boj proti terorismu**.

Klíčová opatření
Komise:

[81] Znalostní centrum pro ochranu veřejného prostoru.
[82] V návaznosti na soubor klíčových opatření ve sdělení z roku 2023 o boji proti potenciálním hrozbám, které představují drony, COM(2023) 659 final.
[83] V plném souladu se Schengenským hraničním kodexem a nařízením o prověřování.

- **v roce 2025 přijme novou Agendu EU pro předcházení terorismu a násilnému extremismu a boj proti nim**
- **v roce 2025 podepíše se západním Balkánem nový Společný akční plán pro předcházení terorismu a násilnému extremismu a boj proti nim**
- **společně se Znalostním centrem EU vyvine nový ucelený soubor nástrojů prevence**
- **v roce 2026 vyhodnotí uplatňování nařízení proti teroristickému obsahu online**
- **v roce 2025 změní krizový protokol EU**
- **v roce 2026 předloží legislativní návrh na revizi nařízení o uvádění prekurzorů výbušnin na trh a o jejich používání**
- **prozkoumá možnost vytvoření nového celounijního systému pro sledování financování terorismu**

Členské státy se vyzývají, aby:

- **posílily biometrické kontroly a prováděly povinné systematické kontroly na vnějších hranicích EU**
- **plně využívaly evropský justiční rejstřík pro boj proti terorismu**

7. EU jako silný globální hráč v oblasti bezpečnosti

V zájmu zvýšení bezpečnosti EU posílíme operativní spolupráci prostřednictvím partnerství s klíčovými regiony, jako jsou naši partneři v procesu rozšíření a sousedství, Latinská Amerika a Středomoří. Bezpečnostní zájmy EU budou zohledněny v rámci mezinárodní spolupráce, a to i využíváním nástrojů EU.

Poslední roky ukázaly, že vnější a vnitřní bezpečnost EU je neoddělitelně spjata. Ruská útočná válka proti Ukrajině, konflikt v Gaze, situace v Sýrii a vznikající konflikty po celém světě mají vážné vedlejší účinky na vnitřní bezpečnost EU. **EU musí aktivně hájit své bezpečnostní zájmy**, aby mohla čelit dopadům globální nestability na svou vnitřní bezpečnost, a to prostřednictvím řešení vnějších hrozeb, narušování pašeráckých tras a ochrany koridorů strategického zájmu, jako jsou obchodní trasy. Zároveň bude EU i nadále silným spojencem partnerských zemí a bude spolupracovat na posílení globální bezpečnosti a budování vzájemné odolnosti vůči hrozbám.

V posledních letech podnikla EU k posílení své bezpečnostní spolupráce významné kroky. S partnerskými zeměmi uzavřela dohody o operativní spolupráci donucovacích a justičních orgánů a další typy ujednání. Aktivně usiluje o uzavření dalších mezinárodních dohod v souladu se směrnicemi Rady pro jednání a vyvíjí iniciativy pro budování kapacit, při čemž jsou jí nápomocny instituce a jiné subjekty EU. Pro posílení bezpečnosti s partnerskými zeměmi má také zásadní význam Nástroj pro sousedství a rozvojovou a mezinárodní spolupráci – Globální Evropa.

Základním kamenem pro posílení globální bezpečnosti je **mezinárodní řád založený na pravidlech**. Pro posílení tohoto úsilí jsou zásadní bezpečnostní dialogy, včetně tematických dialogů. Pro rozvoj účinných bezpečnostních řešení má zásadní význam provádění **Strategického kompasu pro bezpečnost a obranu** spolu s dvoustrannými a mnohostrannými rámci spolupráce, jako jsou dohody o stabilizaci a přidružení a dohody o přidružení, a spolupráce s organizacemi, jako je OSN a NATO. EU bude i nadále hrát svou úlohu na mnohostranných fórech[84] a posílí svou spolupráci s relevantními mezinárodními a regionálními

[84] Globální fórum pro boj proti terorismu, Globální koalice proti Dá'iš, Globální internetové fórum pro boj proti terorismu (GIFCT), nadace Christchurch Call, Globální koalice pro řešení hrozeb spojených se syntetickými drogami.

organizacemi a rámci, včetně NATO, OSN, Rady Evropy, Interpolu, skupiny G7, OBSE a občanské společnosti.

Regionální spolupráce

Prioritní pokračování neochvějné podpory **Ukrajiny** ze strany EU a posílení bezpečnosti a odolnosti **zemí procesu rozšíření EU** je politickým a geostrategickým imperativem. Podpora bezpečnosti EU musí jít ruku v ruce s **urychlenou integrací kandidátských zemí** do **bezpečnostní architektury EU**, současně s upevňováním jejich regionální spolupráce. Komise využije politiku rozšíření EU k podpoře schopnosti kandidátských a potenciálních kandidátských zemí EU reagovat na hrozby, k posílení operativní spolupráce a výměny informací a k zajištění souladu se zásadami, právními předpisy a nástroji EU. Pro posílení bezpečnosti v kandidátských i potenciálních kandidátských zemích mají zásadní význam Nástroj předvstupní pomoci (NPP III), jakož i nástroje pro Ukrajinu, Moldavsko a západní Balkán.

EU bude do bezpečnostní architektury EU rovněž dále integrovat **partnery v sousedství**. Prostřednictvím **nového Paktu pro Středomoří** a připravovaného **Strategického přístupu k Černému moři** bude Unie usilovat o další budování regionální spolupráce a dvoustranných strategických komplexních partnerství s bezpečnostním rozměrem, v případě potřeby s pravidelnými dialogy na vysoké úrovni o otázkách bezpečnosti. Bude posílena operativní spolupráce se severní Afrikou, **Blízkým východem a Zálivem**, zejména v oblasti boje proti terorismu, praní peněz, nedovolenému obchodu s palnými zbraněmi a výroby drog a obchodu s nimi, zejména s kaptagonem.

Aby bylo možné řešit nárůst teroristické a trestné činnosti a jejích možných vedlejších účinků v **subsaharské Africe, zejména v oblasti Sahelu, Afrického rohu a západní Afriky**, posílí EU podporu Africké unie, regionálních hospodářských společenství a zemí v regionu. V souladu se Strategií EU pro námořní bezpečnost[85] posílí EU spolupráci v **Guinejském zálivu, Rudém moři a Indickém oceánu** v boji proti pašování a pirátství, a to podporou vnitroafrické a regionální spolupráce a s pomocí koordinované námořní přítomnosti EU (CMP) a Centra pro námořní analýzu a operace – narkotika) (MAOC-N).

S **Latinskou Amerikou a Karibikem** posílí EU operativní spolupráci s cílem rozbít a stíhat vysoce rizikové zločinecké sítě a narušit nezákonné činnosti a pašerácké trasy a rozšíří rámce spolupráce, jako je EU-CLASI (Latinskoamerický výbor pro vnitřní bezpečnost) a mechanismus EU-CELAC pro koordinaci a spolupráci v oblasti drog. Mezi priority bude patřit odolnost logistických uzlů a partnerství a přístupy založené na sledování toku peněz. EU bude dále podporovat rozvoj Policejního společenství amerického kontinentu (AMERIPOL), které se má stát regionální obdobou Europolu, a posilovat justiční spolupráci mezi členskými státy a tímto regionem. EU bude rovněž spolupracovat s **jižní a střední Asií** na řešení společných bezpečnostních výzev souvisejících s terorismem, obchodováním s nelegálním zbožím včetně drog, obchodováním s lidmi a převaděčstvím migrantů.

Kromě toho bude EU podporovat rámce regionální spolupráce ve třetích zemích, aby jim dále pomáhala zastavit nelegální obchodování u zdroje v souladu se zásadou sdílené odpovědnosti za celý zločinecký dodavatelský řetězec. Dále bude EU přispívat k posílení bezpečnosti logistických uzlů v zahraničí tím, že bude koordinovat **společné inspekce v přístavech třetích zemí**.

[85] JOIN(2023) 8 final.

Operativní spolupráce

Strategie **Global Gateway** bude podporovat udržitelné a vysoce kvalitní infrastrukturní projekty v oblasti digitálních technologií, klimatu a energetiky, dopravy, zdravotnictví, vzdělávání a výzkumu. Do budoucích investic v rámci strategie Global Gateway bude Komise nyní v případě potřeby začleňovat i bezpečnostní aspekty. To bude zahrnovat iniciativy, které mají zásadní význam pro strategickou autonomii EU a jejích partnerských zemí, jako jsou infrastrukturní projekty, jejichž součástí jsou bezpečnostní hodnocení a opatření ke zmírnění rizik.

Komise bude usilovat o další **dohody o spolupráci s Europolem a Eurojustem mezi EU a třetími zeměmi**, zejména se zeměmi Latinské Ameriky.

Kromě toho je jedním z nejúčinnějších prostředků posílení operativní spolupráce proaktivní účast zemí mimo EU v **EMPACT**. EU bude dále podporovat, aby se do tohoto rámce zapojily i třetí země, zejména z regionů západního Balkánu, východního sousedství, subsaharské Afriky, severní Afriky, Blízkého východu, Latinské Ameriky a Karibiku. Dalším nástrojem k posílení spolupráce se třetími zeměmi v oblasti boje proti trestné činnosti jsou operativní pracovní skupiny mezi členskými státy koordinované Europolem, jichž se mohou účastnit i třetí země. Cílem Komise je rovněž dokončit jednání o mezinárodní dohodě mezi **EU a Interpolem**[86], která zajistí jednotnější přístup ke globálním bezpečnostním hrozbám a boji proti nadnárodní trestné činnosti.

V rámci přístupu „Tým Evropa“ musí být Unie přítomna v terénu. Zásadní roli při zajišťování toho, aby vnější činnost Unie byla dobře informovaná, koordinovaná a pohotová, hrají odborní pracovníci Unie a členských států. Aby se tento přístup posunul na vyšší úroveň, posílí Komise s podporou vysoké představitelky pro zahraniční věci a bezpečnostní politiku **styčné sítě** a usnadní nasazení regionálních **styčných důstojníků Europolu a Eurojustu** v souladu s operativními potřebami členských států.

EU bude usilovat o užší operativní spolupráci donucovacích a justičních orgánů, podporovat sdílení informací v reálném čase a společné operace prostřednictvím **společných vyšetřovacích týmů** ve třetích zemích s podporou Europolu a Eurojustu. Komise bude rovněž podporovat členské státy při zřizování **společných středisek pro syntézu informací** sdružujících odborníky a místní donucovací orgány ve strategických třetích zemích.

Nástroje společné zahraniční a bezpečnostní politiky (SZBP)

K lepší identifikaci a řešení vnějších hrozeb pro vnitřní bezpečnost EU budou rovněž plně využity **mise společné bezpečnostní a obranné politiky (SBOP)** v souladu s jejich mandáty stanovenými Radou. Vysoká představitelka pro zahraniční věci a bezpečnostní politiku a Komise budou za účelem budování kapacit třetích zemí podporovat akce SBOP pomocí specializovaných nástrojů financování a prozkoumají všechny vhodné možnosti financování.

Zavedeným nástrojem SZBP, který se používá také v boji proti terorismu, jsou **omezující opatření EU**. Na základě návrhů vysoké představitelky pro zahraniční věci a bezpečnostní politiku, členských států nebo Komise by Rada mohla posoudit, jak dosáhnout toho, aby stávající autonomní omezující opatření EU (seznam teroristů EU) byla účinnější, operativnější a pružnější. Kromě toho by mohlo být posouzeno, zda by v souladu s cíli SZBP neměla být zvážena další omezující opatření zaměřená na zločinecké sítě.

[86] Rozhodnutí Rady (EU) 2021/1312 ze dne 19. července 2021 a rozhodnutí Rady (EU) 2021/1313 ze dne 19. července 2021.

Vízová politika a výměna informací

Klíčovým nástrojem spolupráce se třetími zeměmi a ochrany našich hranic je vízová politika EU, neboť reguluje vstup do EU a stanoví jeho podmínky. Prostřednictvím připravované Strategie EU v oblasti vízové politiky Komise do **vízové politiky EU** plně začlení **bezpečnostní aspekty**. Komise bude spolupracovat se spolunormotvůrci na přijetí návrhu revize a zefektivnění mechanismu pro pozastavení zrušení vízové povinnosti, zejména pro specifické případy zneužití bezvízového režimu[87]. Třetí země budou vyzvány ke sdílení informací o osobách, které mohou představovat bezpečnostní hrozbu, a tyto informace budou zaneseny do informačních systémů a databází EU.

V zájmu dosažení koordinace politik a úsilí na vyšší úrovni, které umožní účinnější, rychlejší a hladší spolupráci, bude Komise usilovat o vytvoření **ujednání o toku údajů** a prozkoumá způsoby, jak **posílit výměnu informací** pro účely prosazování práva a správy hranic s důvěryhodnými třetími zeměmi v souladu se základními právy a pravidly ochrany údajů.

Klíčová opatření

Komise:

- **uzavře mezinárodní dohody o spolupráci s Europolem a Eurojustem mezi EU a prioritními třetími zeměmi**
- **bude podporovat účast partnerských zemí v EMPACT za účelem boje proti organizované trestné činnosti a terorismu**
- **bude podporovat instituce a jiné subjekty EU při vytváření a posilování pracovních ujednání s partnerskými zeměmi**
- **dále zohlední bezpečnostní aspekty ve vízové politice EU prostřednictvím připravované Vízové strategie**
- **posílí výměnu informací s důvěryhodnými třetími zeměmi pro účely prosazování práva a správy hranic**

Komise ve spolupráci s vysokou představitelkou pro zahraniční věci:

- **bude plně využívat civilní mise společné bezpečnostní a obranné politiky (SBOP)**
- **do roku 2027 začne koordinovat společné inspekce v přístavech třetích zemí**

Komise ve spolupráci s vysokou představitelkou pro zahraniční věci a členskými státy:

- **posílí styčné sítě a spolupráci v rámci přístupu „Tým Evropa“**
- **od roku 2025 bude zřizovat společné operační týmy a společná střediska pro syntézu informací ve třetích zemích**

Evropský parlament a Rada se vyzývají, aby:

- **dokončily jednání o revizi mechanismu pro pozastavení zrušení vízové povinnosti**

8. Závěr

Ve světě nejistoty je potřeba posílit schopnost Unie předvídat bezpečnostní hrozby, předcházet jim a reagovat na ně.

Nestačí pouze reagovat na krize, když nastanou. Musíme mít dokonalý přehled o vyvíjejících se hrozbách. A musíme zajistit, aby naše nástroje a kapacity tomuto úkolu odpovídaly.

[87] COM(2023) 642.

Ucelený soubor opatření podrobně popsaných v této strategii pomůže vytvořit Unii, která bude ve světě silnější: Unii, která je schopna předvídat, plánovat a postarat se o své vlastní bezpečnostní potřeby, která dokáže účinně reagovat na hrozby pro svou vnitřní bezpečnost a pohnat pachatele k odpovědnosti a která chrání svou otevřenou, svobodnou a prosperující společnost a demokracii.

To vyžaduje změnu našeho myšlení o vnitřní bezpečnosti. Budeme se snažit přispět k rozvoji nové bezpečnostní kultury EU, v níž budou bezpečnostní aspekty zohledněny ve všech našich právních předpisech, politikách a programech – od jejich vzniku až po jejich provedení. A kde nám spolupráce napříč oblastmi politik umožňuje učinit průlomové kroky.

To není úkolem pouze jednoho orgánu, vlády nebo aktéra. Je to společné úsilí Evropy.