EURÓPSKA
KOMISIA

V Bruseli 15. 5. 2024
COM(2024) 198 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE

o siedmej správe o pokroku vo vykonávaní Stratégie EÚ pre bezpečnostnú úniu

I ÚVOD

V júli 2020 prijala EÚ svoju Stratégiu EÚ pre bezpečnostnú úniu na roky 2020 – 2025[1]. Táto stratégia, navrhnutá na vrchole pandémie ochorenia COVID-19, sa stavia proti čoraz zložitejšej bezpečnostnej situácii s hybridnými a teroristickými hrozbami zameranými na bezpečnosť európskych občanov a podnikov vo fyzickom, ako aj kybernetickom priestore. Reakcia EÚ na tieto výzvy vychádzala z holistického celospoločenského prístupu k bezpečnosti, ktorý sa zameriaval na odstránenie bariér medzi rôznymi bezpečnostnými politikami a prepojenie bodov v rámci celého európskeho bezpečnostného ekosystému.

Po štyroch rokoch sa geopolitický, hospodársky a bezpečnostný kontext v rámci EÚ a v jej susedstve výrazne a trvalo zmenil. Riziká, ktorým dnes čelíme, sú veľmi odlišné od tých, ktoré dominovali pri vytváraní Stratégie EÚ pre bezpečnostnú úniu. Pandémia ochorenia COVID-19 zdôraznila to, ako sa naše spoločnosti a hospodárstva spoliehajú na informačné a komunikačné siete, ako aj na prepojené produkty, a na potrebu zaistiť ich kybernetickú bezpečnosť vzhľadom na rýchlo sa rozvíjajúcu a mimoriadne prispôsobivú počítačovú kriminalitu.

Miera teroristickej hrozby na európskej pôde je stále vysoká, pričom niekoľko členských štátov nedávno zvýšilo svoje hodnotenie vnútroštátnej hrozby na najvyššiu úroveň. Ohrozenie stability organizovanou trestnou činnosťou sa naďalej zintenzívňuje, pričom presun veľkej časti obchodu a ľudskej interakcie do online priestoru otvára nové možnosti pre páchanie trestnej činnosti. Keďže v dôsledku nestability v susedstve EÚ sa milióny ľudí stali zraniteľnejšími, prevádzačstvo a obchodovanie s ľuďmi sa stali hlavným predmetom záujmu tých, ktorí majú zisk z trestnej činnosti vykorisťovaním iných. Zneužívanie migrantov na našich vonkajších hraniciach poukázalo na nové, hybridné formy hrozieb, ktorých cieľom je v spojení s dezinformačnými kampaňami rozdeliť európske spoločnosti a nabúrať ich dôveru. Potenciálne zneužívanie nových technológií, ako je umelá inteligencia, zo strany aktérov s nekalými úmyslami, či už na účely páchania počítačovej trestnej činnosti alebo na manipuláciu s informáciami, napokon prináša nové bezpečnostné výzvy pre naše demokracie, najmä v roku, ktorý sa vyznačuje veľkými volebnými procesmi v celej Európe.

Vnútorná a vonkajšia bezpečnosť sú prepojené. Ruská útočná vojna voči Ukrajine priniesla nárast kybernetických útokov[2] a odhalila potenciálnu zraniteľnosť niektorých kritických infraštruktúr EÚ. Súčasná situácia na Blízkom východe a bezprecedentný rozsah násilia v regióne zintenzívnili výzvy spojené s udržaním vnútornej bezpečnosti EÚ, pričom sa zvýšilo riziko teroristických útokov, či už zo strany samostatne konajúcich páchateľov alebo organizovaných skupín, podporovaných pokusmi o šírenie teroristického obsahu prostredníctvom online platforiem a sietí.

V tejto meniacej sa panoráme hrozieb sa vízia stanovená v Stratégii EÚ pre bezpečnostnú úniu ukázala ako mimoriadne dôležitá. Aj keď nemožno eliminovať všetky riziká, zraniteľné miesta je možné riešiť a Stratégiou EÚ pre bezpečnostnú úniu sa poskytol pevný rámec na vybudovanie schopnosti EÚ riešiť existujúce a vznikajúce hrozby jednotne a so zlepšenými kolektívnymi mechanizmami konania. Cieľom tejto siedmej správy o pokroku v oblasti bezpečnostnej únie je poskytnúť prehľad o vykonávaní stratégie od jej prijatia v roku 2020. Hoci sa Komisia zaoberala všetkými bodmi, ktoré boli pôvodne zdôraznené v Stratégii EÚ pre bezpečnostnú úniu, s cieľom reagovať na meniace sa bezpečnostné výzvy boli do nej začlenené nové iniciatívy. Na zaistenie účinnej ochrany občanov EÚ pred bezpečnostnými hrozbami má

[1] COM(2020) 605.
[2] ENISA Panoráma hrozieb 2023, s. 10 – 11.

teraz zásadný význam, aby boli dokončené dosiaľ nedoriešené spisy, ktoré ešte čakajú na schválenie Parlamentom a Radou, a aby členské štáty presadzovali a vykonávali schválené právne predpisy.

II LEPŠIE CHRÁNENÁ A ODOLNEJŠIA FYZICKÁ A DIGITÁLNA INFRAŠTRUKTÚRA

II.1. Kritická infraštruktúra

Občania, podniky a orgány v EÚ sa spoliehajú na kritickú infraštruktúru, o ktorú sa opierajú základné služby, ako sú dodávky energie, zásobovanie vodou a potravinami, doprava a telekomunikácie. Od poskytovania týchto služieb závisí každodenný život občanov a dlhodobé zdravie hospodárstva. Geopolitický kontext, v ktorom kritická infraštruktúra funguje v EÚ, je však veľmi nestály. Situácia sa ešte zhoršila útočnou vojnou Ruska voči Ukrajine, ako aj zvýšenými hybridnými útokmi a sabotážou plynovodu Nord Stream a poškodením plynovodov baltskej prípojky.

Od začiatku mandátu tejto Komisie prijala EÚ rôzne opatrenia na zvýšenie ochrany kritickej infraštruktúry a odolnosti subjektov, ktoré ju prevádzkujú, s cieľom vyhnúť narušeniu základných služieb alebo zmierniť vplyv tohto narušenia. EÚ posilnila právny rámec na riešenie súčasných a budúcich online a offline rizík, od kybernetických útokov po prírodné katastrofy, prijatím **smernice o odolnosti kritických subjektov** (ďalej len „smernica CER“)[3] a revidovanej **smernice o bezpečnosti sietí a informačných systémov** (ďalej len „smernica NIS2“)[4]. Smernicami sa po ich transpozícii členskými štátmi zabezpečí lepšie zohľadnenie rizík a zraniteľných miest, ktoré majú vplyv na subjekty v celom rade kľúčových sektorov[5] . Na urýchlenie vykonávania smernice CER slúžilo odporúčanie Rady[6] ako základ pre vykonávanie záťažových testov so subjektmi, ktoré prevádzkujú kritickú infraštruktúru, a to najprv v sektore energetiky, kde výsledky teraz analyzuje Komisia.

Z nedávnych udalostí takisto vyplynulo, že v prípade incidentu je potrebné urýchlene konať na úrovni EÚ. Komisia navrhla[7] **odporúčanie Rady o koncepcii**, ktorým sa stanovuje koordinácia na úrovni EÚ s cieľom reagovať na pokusy o narušenie kritickej infraštruktúry so značným cezhraničným významom. **Nástrojom núdzovej pomoci pre jednotný trh** sa poskytnú prostriedky na zabezpečenie nepretržitého fungovania vnútorného trhu počas krízy.

Komisia takisto prijala opatrenie na zvýšenie odolnosti kritickej infraštruktúry na **sektorovej úrovni**, pričom vychádzala zo základných scenárov stanovených horizontálnymi právnymi predpismi. V **odvetví energetiky** pomôže práca na vytvorení sieťového predpisu o osobitných odvetvových pravidlách týkajúcich sa aspektov kybernetickej bezpečnosti pri cezhraničných tokoch elektriny, aby bola elektrizačná sústava EÚ odolnejšia a bezpečnejšia. Komisia takisto oznámila **akčný plán v oblasti veternej energie** na posilnenie kybernetickej odolnosti veterných zariadení. V **odvetví dopravy** Komisia pokračovala v práci na systéme inšpekcií bezpečnostnej ochrany letectva a námornej dopravy, pričom vykonala viac ako 100 inšpekcií

[3] Smernica (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov.

[4] Smernica (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii.

[5] Medzi sektory, na ktoré sa vzťahujú smernice NIS2 a CER, patrí energetika, doprava, bankovníctvo, infraštruktúra finančného trhu, digitálna infraštruktúra, zdravotníctvo, pitná voda, odpadová voda, verejná správa, vesmír a výroba, spracovanie a distribúcia potravín.

[6] Po návrhu Komisie COM(2022) 551 bolo prijaté odporúčanie Rady 2023/C 20/01.

[7] COM(2023) 526.

v oblasti letectva a 60 inšpekcií v oblasti námornej dopravy. Pokiaľ ide o **námornú bezpečnosť**, v októbri 2023 bola schválená revidovaná stratégia námornej bezpečnosti Európskej únie[8] spolu s jej akčným plánom na lepšiu ochranu kritickej námornej infraštruktúry a lodí pred fyzickými a kybernetickými hrozbami. Komisia takisto vyvíja **spoločné prostredie na výmenu informácií** s cieľom uľahčiť cezhraničnú a medzisektorovú výmenu informácií medzi námornými orgánmi. V rámci preskúmania nariadenia o **transeurópskej dopravnej sieti**[9] sa stanovili členským štátom nové požiadavky na ochranu pred rizikom s cieľom zabezpečiť, aby kľúčová dopravná infraštruktúra Únie bola účinne chránená. Po hĺbkovom posúdení rizika **odvetvia infraštruktúry pripojiteľnosti** EÚ s členskými štátmi a agentúrou ENISA Komisia vydala niekoľko odporúčaní na zvýšenie kybernetickej bezpečnosti a odolnosti, napríklad vo februári 2024[10] stanovila opatrenia na zlepšenie bezpečnosti infraštruktúry podmorských káblov, ktoré sú nevyhnutné pre naše komunikačné siete. V oznámení o riadení **klimatických rizík** sa určili hlavné kategórie opatrení vrátane lepšieho využívania dostupných satelitných údajov a služieb na posilnenie odolnosti kritickej infraštruktúry[11].

Vo **vesmírnom sektore** zahŕňa **stratégia EÚ v oblasti kozmického priestoru pre bezpečnosť a obranu**[12], prijatá v marci 2023, opatrenia na zvýšenie odolnosti systémov a služieb vesmírneho sektora a na rozvoj ďalších vesmírnych služieb EÚ s dvojakým použitím. Pokiaľ ide o **vodné systémy**, **príručka týkajúca sa plánu zabezpečenia dostupnosti vody** zahŕňa bezpečnostné opatrenia na boj proti nepriateľským akciám namiereným na fyzickú a kybernetickú integritu systémov dodávky vody a úmyselnú kontamináciu prenášanú vodou[13]. Vo **finančnom sektore** sa **aktom o digitálnej prevádzkovej odolnosti (DORA)**[14] posilňuje digitálna odolnosť subjektov finančného sektora EÚ zefektívnením a aktualizáciou existujúcich pravidiel. A napokon v **sektore zdravotníctva**, ktorý je súčasťou európskej zdravotnej únie[15], **Úrad EÚ pre pripravenosť a reakcie na núdzové zdravotné situácie (HERA)** podporuje výskum a vývoj, výrobu a poskytovanie zdravotníckych protiopatrení. Okrem toho sa rozširuje modul krízového riadenia systému včasného varovania a reakcie EÚ s cieľom podporiť koordináciu závažných ohrození zdravia a systémov zdravotnej starostlivosti a zabezpečiť nepretržitú koordináciu ohrození zdravia v rámci EÚ a na celosvetovej úrovni. V marci 2024 bolo vymenovaných prvých šesť referenčných laboratórií EÚ pre verejné zdravie a do konca roka 2024 bude dokončený a vyskúšaný plán prevencie, pripravenosti a reakcie Únie, ktorý sa pripravuje.

II.2. Kybernetická bezpečnosť

Panoráma kybernetických hrozieb sa v uplynulých rokoch výrazne zhoršila, čo dokazuje dramatický nárast útokov na dodávateľské reťazce a zneužívanie zraniteľných miest v softvéri, operačných systémoch pre mobilné zariadenia alebo osobné počítače a virtuálnych súkromných sieťach. Kybernetické útoky pribúdajú[16] a sú zamerané na ťažký priemysel, informačné služby,

[8] JOIN(2023) 8.

[9] Predbežná dohoda z 24. apríla 2024 o nariadení Európskeho parlamentu a Rady o usmerneniach Únie pre rozvoj transeurópskej dopravnej siete.

[10] C(2024) 1181.

[11] COM(2024) 91.

[12] JOIN(2023) 9.

[13] Archív publikácií JRC – *Water Security Plan Implementation Manual for Drinking Water Systems* (Príručka pre vykonávanie plánu zabezpečenia dostupnosti vody pre systémy pitnej vody).

[14] Nariadenie (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora.

[15] Oznámenie o európskej zdravotnej únii.

[16] ENISA Panoráma hrozieb 2023, s. 10 – 11.

vládu a zdravotníctvo. Výzvou aj naďalej zostáva ransomvér, a to nielen z hľadiska počtu útokov, ale aj z hľadiska narastajúcej kolúzie zločineckých skupín a štátnych aktérov motivovaných záujmami nad rámec finančných ziskov[17]. Vzhľadom na tieto narastajúce a vyvíjajúce sa kybernetické hrozby EÚ podnikla významné kroky na zvýšenie kybernetickej bezpečnosti v členských štátoch, posilnenie bezpečnosti dodávateľských reťazcov a produktov, posilnenie solidarity na úrovni EÚ a posilnenie kapacít na lepšie odhaľovanie kybernetických bezpečnostných hrozieb a incidentov, ich prípravu a reakciu na ne.

Súčasný mandát položil pevný základ pre pokračujúce úsilie EÚ o ochranu svojej digitálnej infraštruktúry. **Revíziou smernice NIS** sa výrazne rozšírila jej pôsobnosť tak, aby zahŕňala všetky stredné a veľké subjekty pôsobiace v 18 kritických sektoroch so sprísnenými požiadavkami na kybernetickú bezpečnosť, povinným oznamovaním incidentov a zákonom ustanovenou európskou štruktúrou koordinácie kybernetických kríz. Medzi ďalšie úspechy patrí dosiahnutá dohoda o **akte o kybernetickej odolnosti**[18] **a** prijatie **nariadenia EÚ o digitálnej identite**[19], ktoré výrazne posilnia našu celkovú kybernetickú bezpečnosť. Aktom o kybernetickej odolnosti sa zavedú povinné požiadavky na špecificky navrhnutú a štandardnú kybernetickú bezpečnosť pre hardvér a softvér počas celého životného cyklu produktu, čím sa zabezpečí, že produkty budú dodávané na trh bez toho, aby sa prejavovali známymi zraniteľnosťami. Nariadenie EÚ o digitálnej identite uľahčí rozvoj digitálneho jednotného trhu na základe dôveryhodných služieb a bude kľúčovým prvkom v úsilí o riešenie phishingových útokov a zlepšenie autentifikácie a správy prístupu. Medzitým 1. augusta 2025 nadobudnú účinnosť nové pravidlá v rámci **smernice o rádiových zariadeniach**, v ktorých sa výrobcom bezdrôtových zariadení stanovujú povinnosti zlepšiť ich úroveň kybernetickej bezpečnosti, súkromia a ochrany pred podvodmi.

Akt o kybernetickej solidarite[20] výrazne zmení situáciu z hľadiska odhaľovania kybernetických hrozieb, pripravenosti a reakcie na incidenty na úrovni EÚ. Stanovuje sa v ňom európsky systém varovania pred kybernetickobezpečnostnými hrozbami, ktorý sa bude skladať z celoeurópskej siete kybernetických centier, s cieľom vybudovať koordinované detekčné kapacity EÚ a spoločnú situačnú informovanosť. Mechanizmus na riešenie kybernetických núdzových situácií posilní pripravenosť a zlepší kapacity členských štátov v oblasti reakcie a obnovy. V záujme podpory reakcie na významné a rozsiahle kybernetické incidenty a podpory počiatočnej obnovy sa vytvorí rezerva EÚ pre kybernetickú bezpečnosť, ktorá bude k dispozícii členským štátom, inštitúciám EÚ a tretím krajinám pridruženým k programu Digitálna Európa.

Európske centrum kompetencií v oblasti kybernetickej bezpečnosti, ktoré by sa malo tento rok stať plne autonómnym, zvýši kapacity a konkurencieschopnosť Európy v oblasti kybernetickej bezpečnosti, ochráni jej hospodárstvo a spoločnosť pred kybernetickými útokmi a posilní jej technologickú suverenitu prostredníctvom spoločných investícií do strategických projektov v oblasti kybernetickej bezpečnosti.

Prijatie vôbec prvého európskeho **systému certifikácie kybernetickej bezpečnosti**[21]**,** so spoločnými kritériami EÚ, je ďalším dôležitým krokom k vytvoreniu prostredia na vnútornom trhu, ktorému môžu podniky a spotrebitelia dôverovať. V pracovnom programe Únie pre

[17] Pozri napríklad: https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime

[18] Predbežná dohoda bola dosiahnutá 30. novembra 2023. Očakáva sa, že účinnosť nadobudne v roku 2024.

[19] Predbežná dohoda bola dosiahnutá 8. novembra 2023.

[20] COM(2023) 209.

[21] C(2024) 560, prijaté 31. januára 2024.

európsku certifikáciu kybernetickej bezpečnosti[22] prijatom vo februári 2024 sa určujú strategické priority pre budúce európske systémy certifikácie kybernetickej bezpečnosti. Akt o kybernetickej bezpečnosti bol zmenený tak, aby umožňoval systémy certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby, ktoré Komisia bude požadovať od agentúry ENISA, keď tento akt nadobudne účinnosť. Pracuje sa na ďalších systémoch, ako je európsky systém certifikácie kybernetickej bezpečnosti pre cloudové služby, ktoré pomôžu používateľom prijímať informované rozhodnutia o nakupovaných službách. Čím je úroveň citlivosti údajov a požadovaného uistenia vyššia, tým prísnejšie požiadavky by sa v týchto systémoch mali uplatňovať.

EÚ medzitým podnikla kroky na posilnenie **kybernetickej bezpečnosti inštitúcií, orgánov, úradov a agentúr EÚ**, zaviedla rámec pre riadenie, správu a kontrolu kybernetických rizík, posilnila úlohu tímu reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT-EU) a zriadila novú Medziinštitucionálnu radu pre kybernetickú bezpečnosť na monitorovanie a podporu jeho vykonávania. Prioritne by sa však mal riešiť nedostatočný pokrok v rokovaniach o súbežnom návrhu o informačnej bezpečnosti, ktorý je nevyhnutný na dokončenie spoľahlivého legislatívneho rámca pre inštitúcie, agentúry a orgány EÚ, a tým prispieť k bezpečnej európskej správe.

Nad rámec intenzívnej legislatívnej činnosti z uplynulých rokov Komisia pracovala na zintenzívnení **operačnej spolupráce s členskými štátmi.** Zavedenie prvých cezhraničných sietí centier bezpečnostných operácií, ako aj pomoc poskytnutá členským štátom prostredníctvom podpornej činnosti ENSIA vo výške 35 miliónov eur v rámci programu Digitálna Európa počas uplynulých dvoch rokov ukázali, ako sa EÚ môže usilovať o zaistenie bezpečnosti svojich občanov tým, že bude združovať zdroje na posilnenie kapacít kybernetickej bezpečnosti.

S cieľom zaistiť hospodársku bezpečnosť a otvorenú strategickú autonómiu EÚ takisto zaujala proaktívny prístup k **riešeniu kybernetických rizík vo vznikajúcich technológiách**. V rámci stratégie EÚ v oblasti hospodárskej bezpečnosti sa v súvislosti s kritickými technológiami, ako sú umelá inteligencia, pokročilé polovodiče, biotechnológie a kvantové technológie vykonávajú spoločné posúdenia rizík[23]. Na ochranu údajov a zabezpečenie citlivej komunikácie vydala Komisia odporúčanie[24], v ktorom vyzvala členské štáty, aby vypracovali a vykonali Plán koordinovaného prechodu na postkvantovú kryptografiu v celej EÚ. Odporúčaním sa členské štáty nabádajú, aby podporovali vývoj príslušných postkvantových šifrovacích algoritmov a noriem, ktoré sa majú vykonávať v celej Únii.

Vykonávanie súboru nástrojov EÚ pre kybernetickú bezpečnosť 5G[25] je kľúčom k zabezpečeniu dôveryhodnosti a kybernetickej bezpečnosti sietí a technológií 5G a sietí a technológií ďalších generácií s nimi spojených. V súlade s týmto súborom nástrojov sa Komisia bude snažiť o to, aby jej medziinštitucionálna komunikácia nebola vystavená pôsobeniu mobilných sietí, ktoré využívajú vysokorizikoví dodávatelia, a aby sa jej posúdenie premietlo do všetkých príslušných programov a nástrojov financovania EÚ[26]. Prístup EÚ ku kybernetickej bezpečnosti v súčasnosti nezahŕňa len prevenciu a ochranu kritickej

[22] SWD(2024) 38.
[23] C(2023) 6689.
[24] C(2024) 2393.
[25] Skupina pre spoluprácu v oblasti bezpečnosti sietí a informačných systémov 1/2020, *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* (Kybernetická bezpečnosť sietí 5G – súbor nástrojov EÚ s opatreniami na zmiernenie rizika).
[26] C(2023) 4049.

infraštruktúry, ale aj **krízové riadenie** vrátane vytvorenia a formalizácie **Európskej siete styčných organizácií pre kybernetické krízy (EU-CyCLONe)**. Rozvojom ekosystému zainteresovaných strán a sietí pre krízové riadenie sa zvýšila pripravenosť EÚ na kolektívnu reakciu v prípade veľkého kybernetického incidentu. Dobrá koordinácia medzi rôznymi úrovňami (technická, prevádzková a politická) a silná synergia medzi rôznymi komunitami v oblasti kybernetickej bezpečnosti si vyžadujú pravidelné cvičenia a interakcie naprieč sektormi, posúdenia rizík, záťažové testy a dokumentáciu, ktorá je jasná, aktuálna a ktorú správne chápu všetci aktéri.

Bezpečnosť a konkurencieschopnosť EÚ závisia od dostupnosti odbornej kvalifikovanej pracovnej sily v oblasti kybernetickej bezpečnosti. EÚ však čelí výraznému nedostatku odborníkov v oblasti kybernetickej bezpečnosti, čo zvyšuje riziká pre EÚ, jej členské štáty, podniky a občanov vyplývajúce z incidentov v oblasti kybernetickej bezpečnosti, ktoré sa nedajú rýchlo identifikovať alebo sa nestretnú s primeranou a včasnou reakciou[27]. Tento problém pomôže vyriešiť zriadenie **Akadémie zručností v oblasti kybernetickej bezpečnosti** tým, že zlúči existujúce iniciatívy odbornej prípravy týkajúcej sa kybernetických zručností a zlepší ich koordináciu. Zvyšujúci sa počet záväzkov akadémii ukazuje ochotu priemyslu a akademickej obce stať sa hlavnými prispievateľmi pri povzbudzovaní väčšieho počtu odborníkov vrátane mladých žien, aby sa zapojili do oblasti kybernetickej bezpečnosti.

Novou **politikou EÚ v oblasti kybernetickej obrany** sa stanovujú prostriedky na zlepšenie koordinácie medzi civilnými komunitami v oblasti kybernetickej bezpečnosti a vojenským/obranným ekosystémom a prepojenia medzi týmito dvoma oblasťami sa v budúcnosti pravdepodobne rozšíria. Touto politikou sa zároveň umožňuje EÚ a jej členským štátom posilniť ich schopnosť chrániť, odhaľovať, brániť a odrádzať, pričom sa náležitým spôsobom využíva celý rad možností obrany, ktoré majú civilné a vojenské komunity k dispozícii pre širšiu bezpečnosť a obranu EÚ, v súlade s medzinárodným právom. V rámci novej politiky sa zdôrazňuje potreba užšej spolupráce medzi verejným a súkromným sektorom a navrhujú sa spôsoby, ako to dosiahnuť.

EÚ v akcii

Agentúra ENISA od svojho zriadenia vypracovala 70 správ o situačnej informovanosti, v ktorých sa analyzovalo viac ako 4 000 incidentov. Vybavila 22 hovorov týkajúcich sa incidentov veľkého rozsahu. ENISA spolu s Komisiou zorganizovala niekoľko teoretických cvičení s kybernetickou tematikou, z ktorých v poslednom sa testovala pripravenosť Európskej siete styčných organizácií pre kybernetické krízy (EU-CyCLONe), ktorá spája vnútroštátne orgány členských štátov zodpovedné za riadenie kybernetických kríz. Takéto cvičenia zlepšujú koordináciu, a tým zmierňujú vplyv potenciálnych budúcich útokov v EÚ.

V rámci programu Digitálna Európa vyčleňuje Komisia rozpočet vo výške 84 miliónov eur na posilnenie opatrení na podporu kybernetickej bezpečnosti podľa nových právnych predpisov EÚ vrátane aplikovania umelej inteligencie a iných podporných technológií pre centrá bezpečnostných operácií, ako aj prechod Európy na postkvantovú kryptografiu. Európske centrum kompetencií v oblasti kybernetickej bezpečnosti pomôže zabezpečiť, aby tieto projekty boli prospešné pre podniky, MSP a orgány verejnej správy v členských štátoch a pridružených krajinách.

[27] ENISA, *Foresight Cybersecurity Threats for 2030 – Update 2024*(Prognóza kybernetických bezpečnostných hrozieb do roku 2030 – Aktualizácia z roku 2024).

III BOJ PROTI TERORIZMU A RADIKALIZÁCII

III.1. Protiteroristické opatrenia

Hrozba terorizmu zostáva akútna a riziká sú ovplyvnené konfliktami mimo EÚ. Podľa Europolu[28] členské štáty v roku 2022 nahlásili 28 dokončených, neúspešných alebo zmarených útokov, čo je nárast v porovnaní s rokom 2021 (18 útokov), ale výrazne menej ako 56 útokov nahlásených v roku 2020. Zvýšené napätie v niektorých komunitách v členských štátoch od útoku Hamasu zo 7. októbra 2023 bolo zaznamenané pri troch teroristických útokoch (Arras vo Francúzsku 13. októbra, Brusel 16. októbra a Paríž 2. decembra 2023). Zároveň niektoré členské štáty čelia významnej hrozbe násilného pravicového extrémizmu. Podľa hlásení sú oslavovanie terorizmu, ako aj nenávistné prejavy, najmä vo forme antisemitizmu a nenávisti voči moslimom, v EÚ od 7. októbra 2023 na vzostupe[29].

V rámci Stratégie EÚ pre bezpečnostnú úniu bol prijatý súbor opatrení a nástrojov na podporu členských štátov v boji proti terorizmu. Prijatím **programu boja proti terorizmu pre EÚ**[30] v decembri 2020 sa EÚ poskytli nástroje na lepšie predvídanie teroristických hrozieb, predchádzanie týmto hrozbám, ochranu pred nimi a reakciu na ne. Smernicu o boji proti terorizmu[31], ktorá bola prijatá v roku 2017, teraz vykonávajú všetky členské štáty, pričom sa kriminalizuje výcvik a cestovanie na účely terorizmu, ako aj financovanie terorizmu. Nedostatky v transpozícii smernice vo viacerých členských štátoch sa riešia prostredníctvom postupov v prípade nesplnenia povinnosti, pričom sa zorganizovalo niekoľko seminárov, aby sa zabezpečilo, že vykonaním tohto právneho predpisu sa dosiahne jeho plný účinok.

Niektorí **zahraniční teroristickí bojovníci** sa vrátili do EÚ, ale značný počet zostáva v táboroch a vo väzniciach na severovýchode Sýrie. Zatiaľ čo primárnu zodpovednosť nesú členské štáty, spolupráca na úrovni EÚ pomohla členským štátom riešiť problémy, ako je stíhanie tých, ktorí spáchali teroristické trestné činy, predchádzanie nezistenému vstupu do schengenského priestoru pomocou systematických kontrol v Schengenskom informačnom systéme s plným využitím jeho funkcie a reintegrácia a rehabilitácia vracajúcich sa zahraničných teroristických bojovníkov. Pri koordinácii týchto vyšetrovaní a trestných stíhaní zohrávali kľúčovú úlohu agentúry Europol, ako aj Eurojust.

Kľúčovým prvkom v boji proti terorizmu je zabránenie prístupu teroristov k prostriedkom na vykonanie útoku. Možnosť prístupu teroristov k zbraniam v EÚ ovplyvnia nové **právne predpisy o strelných zbraniach**. Nové právne predpisy navrhnuté s cieľom obmedziť dostupnosť **prekurzorov výbušnín**, ktoré by teroristi mohli použiť na výrobu bômb, nadobudli účinnosť vo februári 2021[32]. Na základe prístupu, ktorý sa používa na reguláciu prístupu k prekurzorom výbušnín, Komisia vykonala posúdenie vplyvu na reguláciu prístupu k **vysokorizikovým chemickým látkam.** Rýchly pokrok v oblasti umelej inteligencie a biotechnológie navyše znižuje prekážky prístupu k nebezpečným chemickým látkam a patogénom, čím sa zvyšuje riziko chemických a biologických udalostí.

S cieľom **zvýšiť pripravenosť** Komisia buduje európske strategické rezervy kapacít prostredníctvom rescEU a HERA, aby dokázala reagovať na chemické, biologické, rádiologické a jadrové hrozby. Týmito strategickými rezervami sa zabezpečuje dostupnosť

[28] Europol 2023, Správa EÚ o situácii a trendoch v oblasti terorizmu z roku 2023.
[29] Pozri na lokalite: isdglobal.org, 31. októbra 2023; isdglobal.org, 2. novembra 2023.
[30] COM(2020) 795.
[31] Smernica (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu.
[32] Nariadenie (EÚ) 2019/1148 z 20. júna 2019 o uvádzaní prekurzorov výbušnín na trh a ich používaní.

protiopatrení vrátane vybavenia na ochranu pred účinkami incidentov. EÚ pokračovala v posilňovaní rámca EÚ na **predchádzanie praniu špinavých peňazí a financovaniu terorizmu a boj proti nim a** dôsledne monitoruje vykonávanie, aby zabezpečila, že právne predpisy prispejú k efektívnejšiemu odhaľovaniu prostriedkov určených na financovanie teroristických organizácií. S cieľom podporiť vyšetrovania súvisiace s financovaním terorizmu Komisia v roku 2021 zriadila aj **sieť protiteroristických finančných vyšetrovateľov**. Sieť, ktorej predsedá Komisia, podporuje výmenu informácií medzi vyšetrovateľmi z členských štátov o technikách a skúsenostiach v oblasti boja proti financovaniu terorizmu.

Prioritou programu boja proti terorizmu je **ochrana ľudí a verejných priestranstiev**. Prostredníctvom programu poradcov EÚ pre ochrannú bezpečnosť je k dispozícii viac ako 100 špeciálne vyškolených národných odborníkov a odborníkov Komisie, ktorí môžu na žiadosť orgánu členského štátu a s financovaním Komisie vykonávať misie posúdenia zraniteľnosti s cieľom pomôcť udržiavať verejné priestranstvá, vysokorizikové udalosti a kritické infraštruktúry v EÚ bezpečné pred teroristickými hrozbami. Ako sa uvádza v spoločnom oznámení Komisie a vysokého predstaviteľa zo 6. decembra 2023[33] s názvom „Nenávisť tu nemá miesto: Európa zjednotená proti nenávisti“, zvýšili sa finančné prostriedky na ochranu verejných priestranstiev a bohoslužobných miest všetkých vierovyznaní. Od roku 2020 sa prostredníctvom **Fondu pre vnútornú bezpečnosť** poskytuje rozpočet vo výške 30 miliónov eur na program PROTECT, ktorý zahŕňa osobitné zameranie na ochranu bohoslužobných miest vrátane synagóg a mešít: ďalších 5 miliónov eur pomáha riešiť osobitné hrozby rastúceho antisemitizmu. Komisia spolupracuje s občianskou spoločnosťou v boji proti nenávistným prejavom, napríklad prostredníctvom Európskej panelovej diskusie občanov o boji proti nenávisti v spoločnosti.

Drony sú čoraz bežnejším a dostupnejším nástrojom, ktorý sa môže používať na legitímne, ale aj na škodlivé účely vrátane útokov na verejné priestory, jednotlivcov a kritickú infraštruktúru. V októbri 2023 Komisia prijala oznámenie o boji proti hrozbám, ktoré predstavujú nespolupracujúce drony určené na civilné použitie[34]. Medzi kľúčové opatrenia, ktoré sa už vykonali, patrí zriadenie expertnej skupiny pre obranu proti dronom, ktorá bude poskytovať poradenstvo na politickej a prevádzkovej úrovni, ako aj osobitné posúdenie rizika týkajúce sa hrozby, ktorú predstavujú nespolupracujúce bezpilotné lietajúce prostriedky pre civilné letectvo a letiskové zariadenia. Komisia takisto vykonala **komplexné mapovanie rizík leteckej bezpečnosti**, aby zhodnotila existujúce a vznikajúce riziká a zraniteľné miesta s cieľom aktualizovať základný režim bezpečnostnej ochrany letectva na letiskách v EÚ[35].

III.2. Predchádzanie radikalizácii a boj proti nej

predchádzanie radikalizácii je prvým krokom k zamedzeniu teroristických útokov. Komisia posilnila svoju podporu členským štátom na pomoc pri predchádzaní tomu, aby boli občania vystavení škodlivému extrémistickému a teroristickému obsahu online aj offline, a to aj vo väzniciach. Prostredníctvom siete na zvyšovanie povedomia o radikalizácii Komisia spája 6 500 odborníkov (tvorcov politík, orgánov na presadzovanie práva, výskumných pracovníkov) z celej Európy s cieľom vypracovať osvedčené postupy na riešenie násilného extrémizmu. Od júna 2024 bude sieť na zvyšovanie povedomia o radikalizácii integrovaná do znalostného centra EÚ pre prevenciu radikalizácie. Prostredníctvom **znalostného centra EÚ** sa EÚ zameriava na odstránenie bariér medzi príslušnými tvorcami politík, odborníkmi a výskumnými pracovníkmi, pričom poskytuje hĺbkové štúdie, prognostické scenáre, podporu reakcie na

[33] JOIN(2023) 51.
[34] COM/2023/659.
[35] SWD(2023) 37.

geopolitický vývoj, odbornú prípravu v oblasti strategickej komunikácie, ako aj nástroje na vývoj politík a postupov zameraných proti radikalizácii. Komisia prijala aj odporúčanie o procesných právach podozrivých a obvinených osôb, na ktoré sa vzťahuje väzba, a o materiálnych podmienkach obmedzenia osobnej slobody[36], čo zahŕňa opatrenia na riešenie otázky radikalizácie vo väzniciach.

EÚ pracuje aj na predchádzaní zahraničnému vplyvu a financovaniu, ktorým sa podporujú radikálne/extrémistické názory v členských štátoch. Komisia naďalej zostáva obozretná, aby zabránila využívaniu finančných prostriedkov EÚ na podporu akéhokoľvek projektu, ktorý je nezlučiteľný s európskymi hodnotami, alebo ktorý sa venuje nezákonnej agende. Revidované nariadenie o rozpočtových pravidlách[37] v súčasnosti obsahuje odsúdenie za „podnecovanie k nenávisti“ ako dôvod na vylúčenie z financovania EÚ. V januári 2024 vydala Komisia nové usmernenia pre manažérov finančných programov o dôsledkoch porušovania hodnôt EÚ.

Dezinformácie určené na podnecovanie nenávisti a teroristický obsah sa šíria online vrátane obrázkov vytvorených umelou inteligenciou a môžu inšpirovať ku skutkom násilného extrémizmu. Kľúčovým nástrojom na zabránenie šíreniu teroristického obsahu online je **nariadenie o riešení šírenia teroristického obsahu online**[38], ktorým sa poskytovateľom hostingových služieb ukladá povinnosť odstrániť teroristický obsah alebo k nemu zablokovať prístup do jednej hodiny od prijatia príkazu na odstránenie od orgánov členských štátov. Komisia vo svojej hodnotiacej správe prijatej vo februári 2024 uviedla, že nariadenie účinne zamedzuje šírenie teroristického obsahu online. Príslušné orgány na vydávanie príkazov na odstránenie dosiaľ vymenovalo 23 členských štátov a od júna 2022 do apríla 2024 bolo vydaných približne 500 príkazov na odstránenie. Zároveň sa nedostatky v transpozícii nariadenia vo viacerých členských štátoch riešia prostredníctvom postupu v prípade nesplnenia povinnosti.

Komisia zároveň uverejnila súbor usmernení pre učiteľov a pedagógov týkajúcich sa boja proti dezinformáciám a podpory digitálnej gramotnosti prostredníctvom vzdelávania a odbornej prípravy.

Čo je nezákonné offline, musí to byť nezákonné aj online. Rozhodujúcim krokom v tomto smere je presadzovanie **aktu o digitálnych službách**[39] uplatniteľného od 17. februára 2024, pričom všetky online platformy majú povinnosť bojovať proti nezákonnému obsahu. Ďalším prvkom súboru nástrojov EÚ na boj proti terorizmu je **jednotka EÚ pre nahlasovanie internetového obsahu agentúry Europol**, ktorá odkazuje na teroristický obsah na viac ako 300 platformách a zvyšuje informovanosť o teroristickej propagande a o opatreniach proti nej. **Internetové fórum EÚ** takisto podporuje technický priemysel pri zmierňovaní extrémistického obsahu a v súčasnosti sa zaoberá rizikom teroristického zneužívania generatívnej umelej inteligencie, čím dopĺňa legislatívny vývoj, najmä akt o umelej inteligencii.[40]. Po útoku v meste Christchurch v marci 2019 internetové fórum EÚ schválilo krízový protokol EÚ s cieľom zabezpečiť spoluprácu medzi orgánmi presadzovania práva a priemyslom po kríze.

III.3. Ochrana obetí terorizmu

[36] Odporúčanie Komisie (EÚ) 2023/681 z 8. decembra 2022.
[37] Predbežná politická dohoda bola dosiahnutá 7. decembra 2023.
[38] Nariadenie (EÚ) 2021/784 z 29. apríla 2021 o riešení šírenia teroristického obsahu online.
[39] Nariadenie (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami (akt o digitálnych službách).
[40] Predbežná politická dohoda bola dosiahnutá 8. decembra 2023.

V januári 2020 zriadila Komisia Centrum odborných znalostí EÚ pre **obete terorizmu**, ktoré poskytuje odborné znalosti, usmernenia a podporu vnútroštátnym orgánom a organizáciám na podporu obetí. Centrum EÚ pomáha zabezpečiť, aby sa pravidlá EÚ o obetiach terorizmu správne uplatňovali, pričom podporuje výmenu osvedčených postupov a delenie sa o odborné znalostí.

EÚ v akcii

V roku 2022 bolo dokončených, neúspešných alebo zmarených 28 teroristických útokov. V roku 2022 bolo v členských štátoch zatknutých 380 osôb za trestné činy súvisiace s terorizmom. Financovania terorizmu sa týkalo 14 z nich, pričom všetky súviseli s džihádistickým terorizmom. **Eurojust** podporil opatrenia v 203 prípadoch vrátane práce 8 spoločných vyšetrovacích tímov. Podľa nariadenia o predchádzaní šíreniu teroristického obsahu online bolo od júna 2022 vykonaných 350 príkazov na odstránenie.

S podporou Komisie členské štáty zaviedli nástroje na posúdenie rizík, špeciálne režimy obmedzenia osobnej slobody, rehabilitačné a reintegračné programy, odbornú prípravu pre väzenských a probačných pracovníkov, štruktúry na výmenu informácií a multidisciplinárnu spoluprácu pri riadení bývalých páchateľov trestnej činnosti po prepustení.

Hodnota nariadenia o riešení šírenia teroristického obsahu online sa potvrdila napríklad tým, že sa umožnilo rýchle odstránenie teroristického obsahu po útoku, ktorého sa 7. októbra 2023 dopustil Hamas voči Izraelu.

IV BOJ PROTI ORGANIZOVANEJ TRESTNEJ ČINNOSTI

Organizovaná trestná činnosť je hrozbou pre európskych občanov, podniky, štátne inštitúcie, ako aj hospodárstvo ako celok. Zločinecké siete sú zapojené do trestnej činnosti rôzneho druhu vrátane obchodovania s drogami, organizovanej majetkovej trestnej činnosti, trestných činov proti životnému prostrediu, podvodov, prevádzačstva a obchodovania s ľuďmi. Rozšírenejším používaním internetu a online služieb sa ešte viac rozvinula počítačová kriminalita a rodovo-motivované kybernetické násilie. Narušenie spôsobené ruskou útočnou vojnou voči Ukrajine okrem toho vytvorilo nový priestor, ktorý organizované zločinecké skupiny rýchlo využívajú. Páchatelia trestnej činnosti jednoducho operujú online a cezhranične, čo vytvára potrebu konzistentných opatrení na európskej a nadnárodnej úrovni. V **stratégii EÚ na boj proti organizovanej trestnej činnosti na roky 2021 – 2025**[41], ktorú Komisia prijala v apríli 2021, sa zdôrazňuje význam rozkladania štruktúr organizovanej trestnej činnosti so zameraním na jednotlivcov na vrchole zločineckých organizácií, najmä na tie skupiny, ktoré predstavujú najväčšie riziko pre bezpečnosť Európy.

IV.1. Počítačová kriminalita

Technologický vývoj síce prináša dôležité a rýchle zlepšenia pre našu spoločnosť, zároveň však umožňuje páchateľom počítačovej kriminality využívať bezhraničnú povahu digitálneho sveta. V období od mája 2021 do júna 2022 bolo nahlásených 3 640 ransomvérových útokov proti podnikom a inštitúciám v EÚ a v roku 2023 celkové platby za ransomvér prvýkrát prekročili 1 miliardu EUR[42]. Zločiny siahajúce od rozsiahlych kybernetických útokov až po činnosti, pri ktorých sa využíva malvér, špionážny softvér, phishing a spam narúšajú fungovanie digitálnych a fyzických infraštruktúr a vážne ovplyvňujú životy ľudí. Na boj proti týmto trestným činom

[41] COM(2021) 170.

[42] ENISA, *Threat landscape for ransomware attacks* (Panoráma hrozieb v prípade ransomvérových útokov).

prijala EÚ množstvo legislatívnych a nelegislatívnych opatrení na podporu cezhraničnej spolupráce na úrovni EÚ a na medzinárodnej úrovni.

V roku 2021 sa EÚ pripojila k **Medzinárodnej iniciatíve v oblasti boja proti ransomvéru**, ktorá spája úsilie viac ako 50 partnerov z EÚ a tretích krajín, aby sa aktéri **ransomvéru** zodpovedali za svoje trestné činy a odopreli im bezpečné útočisko. Iniciatíva pomáha zabrániť aktérom ransomvéru profitovať z nezákonných príjmov, narušať ich aktivity a postaviť ich pred súd.

Na celom svete bolo len v roku 2023 nahlásených viac ako sto miliónov fotiek a videí znázorňujúcich **sexuálne zneužívanie detí**, pričom mnohé ďalšie nahlásené neboli, čo dokazuje, ako znepokojivo a nebezpečne sa tento fenomén šíri. Deti, ktoré trávia viac času online, sa stávajú náchylnejšími na grooming, čo vedie k nárastu materiálu súvisiaceho s vykorisťovaním, ktorý samy vytvárajú. V súlade so **Stratégiou EÚ pre účinnejší boj proti sexuálnemu zneužívaniu detí**[43] a **komplexnou stratégiou EÚ v oblasti práv dieťaťa**[44] Komisia prijala návrh, ktorým sa stanovujú pravidlá predchádzania sexuálnemu zneužívaniu detí a boja proti nemu[45] a ktorým sa poskytovateľom online služieb ukladajú nové povinnosti. Ak sa predchádzaním nezníži významné riziko, mohlo by sa poskytovateľom služieb nariadiť, aby odhaľovali, oznamovali, odstraňovali a blokovali obsah zobrazujúci sexuálne zneužívanie detí online. Návrhom by sa zriadilo aj **špecializované centrum EÚ** s cieľom uľahčiť vykonávanie nariadenia. Platnosť dočasných právnych predpisov prijatých s cieľom umožniť poskytovateľom online služieb pokračovať v dobrovoľnom odhaľovaní a nahlasovaní sexuálneho zneužívania detí online bola predĺžená do 3. apríla 2026, aby sa získal dostatočný čas na nájdenie dohody o dlhodobom nariadení. Túto iniciatívu doplnil návrh na aktualizáciu **smernice o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti materiálu obsahujúcemu sexuálne zneužívanie detí z roku 2011**[46]. Revidovanými pravidlami sa rozširuje vymedzenie trestných činov, najmä s cieľom udržať krok s narastajúcou online trestnou činnosťou, a zavádzajú sa vyššie sankcie a špecifickejšie požiadavky na predchádzanie a pomoc obetiam.

Odhaduje sa, že polovica všetkých mladých žien zažíva **rodovo motivované kybernetické násilie**[47]**. Smernicou o boji proti násiliu na ženách a domácemu násiliu**, ktorá bola prijatá v máji 2024, sa kriminalizujú niektoré formy násilia, ktoré neúmerne postihujú ženy, najmä zdieľanie intímnych obrázkov bez predchádzajúceho súhlasu (vrátane deepfake), kybernetické nebezpečné prenasledovanie, kybernetické obťažovanie a mizogýnne nenávistné prejavy. Touto smernicou sa takisto posilní prístup obetí k spravodlivosti.

IV.2. Obchodovanie s drogami

Nezákonný obchod s **drogami** je jednou z najvýznamnejších bezpečnostných hrozieb, ktorým dnes EÚ čelí. Hodnota obchodov na maloobchodnom trhu s drogami v EÚ sa odhaduje najmenej na 30 mld. eur ročne[48]. Záchyty kokaínu v EÚ dosahujú rekordné úrovne[49]. Rastú obavy z výroby a šírenia syntetických drog v Európe a z prepojenia obchodovania s drogami

[43] COM(2020) 607 – prijaté v júli 2020.
[44] COM(2021) 142 – prijaté v marci 2021.
[45] COM(2022) 209 – prijaté v máji 2022.
[46] COM(2024) 60 – prijatá v apríli 2024.
[47] Výskumná služba Európskeho parlamentu (EPRS), *Combating gender-based violence: Cyberviolence, European added value assessment* (Boj proti rodovo motivovanému násiliu: kybernetické násilie, Posúdenie európskej pridanej hodnoty), 2021.
[48] Europol, 2024.
[49] V roku 2021 bolo zadržaných 303 ton kokaínu. Európska správa o drogách 2023, EMCDDA.

s násilím[50]. V **protidrogovom programe a akčnom pláne EÚ na boj proti drogám na roky 2021 – 2025**[51] sa stanovujú konkrétne opatrenia na zintenzívnenie činnosti na úrovni EÚ vrátane prebiehajúceho úsilia o posilnenie medzinárodnej spolupráce v oblasti obchodovania s drogami a transformácie Európskeho monitorovacieho centra pre drogy a drogovú závislosť na **Agentúru EÚ pre drogy**[52]. Agentúra začne svoju činnosť v júli 2024.

Program sa doplnil o **plán EÚ** prijatý Komisiou v októbri 2023[53], v ktorom sa stanovujú dodatočné opatrenia na boj proti obchodovaniu s drogami a organizovanej trestnej činnosti vrátane zriadenia novej **Európskej aliancie prístavov** na zvýšenie odolnosti prístavov proti prenikaniu trestnej činnosti, a to posilnením práce colných orgánov, orgánov presadzovania práva, verejných a súkromných subjektov v prístavoch v celej EÚ. Výsledkom vykonávania plánu bolo aj tematické schengenské hodnotenie, v ktorom sa hodnotili schopnosti členských štátov v oblasti policajnej spolupráce, ochrany vonkajších hraníc a riadenia IT systémov na boj proti obchodovaniu s drogami, pričom sa určilo 40 najlepších postupov.

IV.3. Nezákonné obchodovanie s tovarom

Nezákonné obchodovanie s tovarom je vysoko ziskové podnikanie a náklady pre spoločnosť nepochádzajú len z chýbajúcich príjmov, ale aj v podobe nebezpečenstva pre zdravie a bezpečnosť občanov, čo si vyžaduje koordinovanú reakciu vlád, orgánov presadzovania práva a súkromných subjektov.

Nedovolené obchodovanie so zbraňami podnecuje organizovanú trestnú činnosť v rámci EÚ, ako aj v jej susedstve. V EÚ je v rukách civilistov odhadom 35 miliónov nedovolených strelných zbraní. V Schengenskom informačnom systéme sa uvádza zhruba 630 000 odcudzených alebo stratených zbraní. S rozvojom nových technológií, ako je 3D tlač, nachádza nedovolené obchodovanie so zbraňami nové spôsoby, ako uniknúť kontrolám. Spolu s **akčným plánom EÚ na boj proti nedovolenému obchodovaniu so strelnými zbraňami na roky 2020 – 2025**[54] teraz všetky členské štáty transponovali **smernicu o strelných zbraniach**[55] do svojich vnútroštátnych právnych predpisov, čo prináša podstatné zlepšenia bezpečnosti tým, že sa sťažuje zákonné získanie najnebezpečnejších zbraní. Rada a Európsky parlament takisto dosiahli dohodu o revidovaných **pravidlách o vývozných povoleniach a opatreniach týkajúcich sa dovozu a tranzitu strelných zbraní**[56] s cieľom zlepšenia vysledovateľnosti civilných strelných zbraní so širším zameraním na digitalizáciu.

Nedovolené obchodovanie s kultúrnymi statkami je takisto lukratívnym odvetvím pre organizované zločinecké skupiny a v niektorých prípadoch aj pre účastníkov konfliktu a teroristov[57]. Komisia prijala v decembri 2022 akčný plán EÚ na posilnenie boja proti **nedovolenému obchodovaniu s kultúrnymi objektmi**[58] vrátane dialógu so zainteresovanými

[50] Začiatkom roku 2024 boli zabití dvaja dôstojníci v Barbate (Španielsko) podozrivými obchodníkmi s drogami a v Bruseli (Belgicko) došlo k niekoľkým streľbám spojeným s drogovým násilím, pričom niekoľko osôb bolo zranených a usmrtených.

[51] COM(2020) 606.

[52] Nariadenie (EÚ) 2023/1322 z 27. júna 2023 o Agentúre Európskej únie pre drogy (EUDA).

[53] COM(2023) 641.

[54] COM(2020) 608.

[55] Smernica (EÚ) 2021/555 o kontrole nadobúdania a držania zbraní.

[56] COM(2022) 480.

[57] Pozri napríklad rezolúcie Bezpečnostnej rady OSN č. 2199 (2015), č. 2253 (2015), č. 2322 (2016), č. 2347 (2017), č. 2462 (2019) a č. 2617 (2021); Rímsku deklaráciu ministrov kultúry krajín G20 z 30. júla 2021.

[58] COM(2022) 800.

stranami s cieľom podporiť spravodlivý a renomovaný trh s umením, ktorý chráni kultúrne dedičstvo.

IV.4. Prevádzačstvo a obchodovanie s ľuďmi

Odhaduje sa, že služby prevádzačov využíva viac ako 90 % migrantov, ktorí prichádzajú do EÚ bez povolenia. Zisky z prevádzačstva sa celosvetovo odhadujú na 4,7 – 6 miliárd eur ročne, zatiaľ čo úmrtia v dôsledku tohto zločineckého obchodovania sa len v Stredozemnom mori od roku 2014 odhadujú na viac ako 28 000.

Na zvýšenie úsilia proti **prevádzačstvu** navrhla Komisia aktualizovať súčasný legislatívny rámec[59] navrhovanou smernicou, ktorej cieľom je zabezpečiť efektívnejšie prenasledovanie a stíhanie prevádzačov, a navrhovaným nariadením na zintenzívnenie koordinácie EÚ posilnením **Európskeho centra boja proti prevádzačstvu** v Europole a zlepšením výmeny informácií medzi zodpovednými orgánmi. Komisia vyzýva Európsky parlament a Radu, aby čo najskôr dosiahli dohodu o týchto dokumentoch. Komisia súbežne začala 28. novembra 2023 **Globálnu alianciu na boj proti prevádzačstvu** s **výzvou na akciu**, ktorá sa v súčasnosti realizuje s príslušnými zainteresovanými stranami. V apríli 2024 Komisia usporiadala podujatie zamerané na vytvorenie komunity zainteresovaných strán a príslušných orgánov s cieľom riešiť problém využívania digitálnych služieb pri prevádzačstve. Komisia takisto podporuje orgány presadzovania práva a súdne orgány kľúčových tretích krajín s cieľom zvýšiť ich kapacitu na vyšetrovanie a stíhanie organizovaných skupín prevádzačov a obchodovania s ľuďmi.

Mnohé zločinecké siete zapojené do prevádzačstva sú zapojené aj do **obchodovania s ľuďmi**. Europol odhaduje celosvetové zisky z obchodovania s ľuďmi na viac ako 29,4 miliardy eur ročne[60]. Väčšinu obetí tvoria ženy a dievčatá, ale na vzostupe je aj obchodovanie s mužmi, najmä na účely pracovného vykorisťovania. V apríli 2021 sa poskytol v stratégii EÚ v oblasti boja proti obchodovaniu s ľuďmi na roky 2021 – 2025[61] komplexný rámec opatrení. Nedávno revidovaná smernica o boji proti obchodovaniu s ľuďmi sa vzťahuje na nové formy vykorisťovania (vykorisťovanie prostredníctvom náhradného materstva, núteného manželstva a nezákonnej adopcie), posilňuje nástroje pre orgány presadzovania práva a súdne orgány a vyžaduje od členských štátov, aby ukladali tresty osobám, ktoré vedome využívajú služby závislé od obetí obchodovania s ľuďmi. Eurojust v spolupráci s koordinátorom EÚ pre boj proti obchodovaniu s ľuďmi zriadil osobitnú skupinu špecializovaných prokurátorov na boj proti obchodovaniu s ľuďmi.

IV.5. Trestné činy proti životnému prostrediu

Trestné činy proti životnému prostrediu často spôsobujú nezvratné a dlhodobé škody na zdraví ľudí, ako aj na ekosystémoch a životnom prostredí. Sú vysoko lukratívne a často zahŕňajú organizovanú trestnú činnosť, ale je ťažké ich odhaliť a trestne stíhať. Trestné činy proti životnému prostrediu sú treťou najväčšou trestnou činnosťou na svete, pokiaľ ide o príjmy, pričom nezákonné konanie a zisky sa každoročne a v súčasnosti výrazne zvyšujú[62].

Kým zisky z trestnej činnosti súvisiace s týmto trestným činom sa odhadujú na 200 miliárd eur ročne s výraznými negatívnymi vplyvmi na hospodárstvo, škody na našom životnom prostredí, biodiverzite, ľudskom zdraví a bezpečnosti sú nevyčísliteľné. Opatrenia na zakročenie proti

[59] COM(2023) 754 a COM(2023) 755.
[60] Štúdia o hospodárskych, sociálnych a ľudských nákladoch spojených s obchodovaním s ľuďmi v EÚ (2020).
[61] COM(2021) 171.
[62] *Organized crime groups pushing environmental security to tipping point* (Organizované zločinecké skupiny posúvajú environmentálnu bezpečnosť do kritického bodu) (interpol.int)

trestným činom proti životnému prostrediu na úrovni EÚ boli posilnené prostredníctvom **novej smernice o trestných činoch proti životnému prostrediu**[63], ktorou sa rozširuje rozsah trestných činov určených na vyšetrovanie a trestné stíhanie a stanovujú sa v nej konkrétne druhy a úrovne sankcií pre fyzické a právnické osoby, ktoré spáchali trestné činy proti životnému prostrediu. Prijali sa ďalšie opatrenia, a to prijatím nariadenia o preprave odpadu a účinnejším zameraním sa na nezákonnú ťažbu dreva zavedením nových pravidiel o výrobkoch, ktoré nespôsobujú odlesňovanie. Okrem toho sa revidovaným **akčným plánom EÚ na boj proti obchodovaniu s voľne žijúcimi druhmi živočíchov a rastlín** aktualizujú priority EÚ s cieľom lepšie predchádzať a riešiť základné príčiny tohto javu.

IV.6. Hospodárske a finančné trestné činy

Pranie špinavých peňazí a financovanie terorizmu predstavujú závažné ohrozenie integrity hospodárstva a finančného systému EÚ, ako aj bezpečnosti jej občanov. Europol odhaduje, že približne 1 % ročného hrubého domáceho produktu EÚ sa spája s podozrivou finančnou činnosťou[64].

EÚ sa dohodla na nových pravidlách na **predchádzanie praniu špinavých peňazí a financovaniu terorizmu**, na zlepšenie prevencie a odhaľovania pokusov páchateľov trestnej činnosti prať nezákonné príjmy alebo financovať teroristické aktivity prostredníctvom finančného systému Únie[65], pričom sa v nich stanovujú priamo uplatniteľné požiadavky na súkromné subjekty na úrovni celej Únie vrátane vykonávania náležitej starostlivosti vo vzťahu ku klientovi a ohlasovania podozrení. Úlohy a právomoci vnútroštátnych orgánov dohľadu a finančných spravodajských jednotiek sa posilnia a zosúladia, aby sa zabezpečilo, že zodpovedné orgány budú svoje úlohy vykonávať účinnejšie a spolupracovať efektívnejšie. Jasnými pravidlami sa okrem toho posilňuje preventívna funkcia konečných užívateľoch výhod a bankových registrov. Zriadi sa **nový Úrad pre boj proti praniu špinavých peňazí a financovaniu terorizmu**, ktorý bude mať priame právomoci v oblasti dohľadu nad najrizikovejšími cezhraničnými subjektmi vo finančnom sektore a bude poskytovať prevádzkovú podporu pre spoločnú analýzu cezhraničných prípadov zo strany finančných spravodajských jednotiek.

Okrem nových pravidiel boja proti praniu špinavých peňazí bude dôležitým nástrojom v boji proti závažnej a organizovanej trestnej činnosti nedávno prijatá **smernica o vymáhaní majetku a konfiškácii**, ktorou sa zavádzajú prísnejšie opatrenia na konfiškáciu nezákonných ziskov zo širokého spektra trestných činov. Úrady pre vyhľadávanie majetku budú mať mandát na identifikáciu, vyhľadávanie a zaistenie majetku pochádzajúceho z trestnej činnosti. Tieto pravidlá v kombinácii s nedávno prijatou **smernicou o kriminalizácii porušení reštriktívnych opatrení Únie**, ktorou sa harmonizuje vymedzenie pojmov a sankcie za takéto trestné činy v celej Únii, umožnia zároveň vyhľadávanie, zaistenie, správu a konfiškáciu výhod, ktoré získali zločinecké subjekty, a to prostredníctvom porušovania sankcií Únie.

IV.7. Boj proti korupcii

Korupcia prináša veľké spoločenské škody, oslabuje verejné inštitúcie, ich realizáciu verejných politík a služieb a dôveru občanov v demokratické inštitúcie. Korupcia v súkromnom sektore oslabuje jednotný trh a dáva nové príležitosti organizovanej trestnej činnosti.

[63] Smernica 2008/99/ES o ochrane životného prostredia prostredníctvom trestného práva.
[64] Finančná spravodajská skupina Europolu, *„Od podozrenia k činu“* (2017).
[65] COM(2021) 420, COM(2021) 421, COM(2021) 422 a COM(2021) 423.

Na riešenie rizík a výziev spojených s korupciou navrhla Komisia[66] **smernicu o boji proti korupcii** s cieľom posilniť pravidlá kriminalizujúce korupčné trestné činy a harmonizáciu sankcií v celej EÚ. Európsky parlament prijal svoju pozíciu vo februári 2024. Aby sa zabezpečilo, že v EÚ nebudú žiadne miesta na ukrytie korupcie, Komisia vyzýva Radu, aby pokročila v diskusiách a podporila ciele návrhu Komisie.

Osobitné pravidlá na ochranu rozpočtu EÚ pred trestnými činnosťami vrátane korupcie sú stanovené v **smernici o ochrane finančných záujmov**[67]. Spolu s navrhovanou protikorupčnou smernicou je nevyhnutné dôkladné vykonávanie tohto opatrenia, aby boli financie EÚ chránené pred podvodmi a korupčnými aktivitami. Komisia v tom zohráva svoju úlohu, ak je to potrebné, prostredníctvom postupu v prípade nesplnenia povinnosti. Kľúčovú úlohu v tomto zohráva úrad OLAF a **Európska prokuratúra**, ktorá vyšetruje nezrovnalosti a stíha trestné činy poškodzujúce finančné záujmy Únie[68]. Nová **protikorupčná sieť EÚ**[69], ktorá slúži ako fórum pre všetky zainteresované strany v EÚ na výmenu osvedčených postupov, príležitostí, nápadov a plánov ďalšej práce, sa prvýkrát stretla v septembri 2023.

IV.8. Ochrana obetí trestných činov

Obete všetkých druhov trestných činov si zasluhujú podporu a pozornosť. Komisia už dosiahla väčšinu opatrení v rámci svojej prvej **stratégie EÚ v oblasti práv obetí (2020 – 2025)**[70]. Komisia 12. júla 2023 navrhla smernicu, ktorou sa mení **smernica o právach obetí**[71] z roku 2012, aby sa ďalej posilnili práva všetkých obetí trestných činov v EÚ, najmä práva najzraniteľnejších obetí.

EÚ v akcii

Europol 5. apríla 2024 zverejnil správu s prvým mapovaním najnebezpečnejších zločineckých sietí ako kľúčový výstup plánu EÚ na boj proti obchodovaniu s drogami a organizovanej trestnej činnosti. Zo zistení vyplýva, že najväčšiu hrozbu predstavuje 821 vysokorizikových zločineckých sietí, ktoré tvoria spolu 25 000 členov. V EÚ pôsobí viac ako 10 rokov 34 % vysokorizikových zločineckých sietí, 76 % z nich je prítomných alebo pôsobí až v 7 krajinách a ich členovia zastupujú 112 národností.

V rámci zásahu proti cezhraničnej trestnej činnosti („operácia Mobile 6“) 400 príslušníkov orgánov presadzovania práva z 25 krajín zaistilo 505 ukradnutých áut, 2 000 autosúčiastok, 16 člnov, 32 vonkajších motorov a 248 sfalšovaných dokumentov. Bolo zastavených 209 údajných prevádzačov. V rokoch 2022 a 2023 vykonala Európska prokuratúra rozsiahle vyšetrovanie, ktoré sa týkalo viac ako 30 krajín, organizovaných zločineckých skupín podozrivých zo zodpovednosti za cezhraničné podvody s DPH, ktorých výška sa odhaduje na 2,2 miliardy eur (operácia Admiral).

[66] COM(2023) 234.
[67] Smernica (EÚ) 2017/1371 z 5. júla 2017 o boji proti podvodom, ktoré poškodzujú finančné záujmy Únie, prostredníctvom trestného práva. Od decembra 2021 začala Komisia 19 postupov v prípade nesplnenia povinnosti pre nedodržiavanie smernice o ochrane finančných záujmov.
[68] Poľsko sa formálne pripojilo k Európskej prokuratúre vo februári 2024.
[69] JOIN(2023) 12.
[70] COM(2020) 258.
[71] COM(2023) 424.

V ZAISTENIE BEZPEČNOSTI NAŠICH HRANÍC A PODPORA PRESADZOVANIA PRÁVA A JUSTIČNEJ SPOLUPRÁCE

V priestore bez kontrol na vnútorných hraniciach by príslušníci polície v jednom členskom štáte mali mať prístup k informáciám, aké majú k dispozícii ich kolegovia v inom členskom štáte. Normou musí byť účinná spolupráca. Preto je nevyhnutné posilniť nástroje, ktoré majú orgány presadzovania práva a súdne orgány v celej EÚ k dispozícii na účely výmeny informácií a cezhraničnej spolupráce.

Ako sa zdôrazňuje v správe o stave Schengenu 2024[72], neustále posilňovanie **schengenského priestoru**, riešenie nedostatkov zistených pri hodnoteniach a zameranie kolektívneho úsilia na koordinovanejšiu správu schengenského priestoru prispieva nielen k voľnému pohybu, ale aj k bezpečnosti občanov v celej Európe. Základom dobrého fungovania schengenského priestoru sú tri piliere: účinné riadenie vonkajších hraníc EÚ, posilnenie vnútorných opatrení, ktoré nahradia absenciu kontrol na vnútorných hraniciach, a to najmä v oblasti policajnej spolupráce, bezpečnosti a riadenia migrácie, a zabezpečenie spoľahlivej pripravenosti a riadenia[73].

Riadenie vonkajších hraníc sa posilní novými právnymi predpismi o preverovaní[74] neoprávnených príchodov. Nové vymedzenie zneužívania migrantov[75] pomôže riešiť vykorisťovanie migrantov pri hybridných útokoch na vonkajšej hranici EÚ, ako to bolo napríklad na hraniciach s Bieloruskom v roku 2021. Účinné riadenie migrácie s plynulým postupom na hraniciach[76] posilní schengenský priestor tým, že sa zabezpečí užšia spolupráca a rozdelenie zodpovednosti medzi členskými štátmi. Kódex schengenských hraníc po jeho prijatí prinesie väčšiu koordináciu EÚ a lepšie pripraví členské štáty na riešenie vznikajúcich problémov na spoločnej vonkajšej hranici EÚ a v rámci schengenského priestoru, zatiaľ čo agentúry EÚ budú naďalej pomáhať členským štátom udržiavať vysokú úroveň vnútornej bezpečnosti v schengenskom priestore.

Balík v oblasti policajnej spolupráce[77] ponúkol veľkú modernizáciu dostupných nástrojov na zlepšenie cezhraničných operácií, poskytol jasné kanály a časové rámce na výmenu informácií medzi silami presadzovania práva v členských štátoch a posilnil úlohu **Europolu**. Revidované pravidlá o **automatizovanej výmene** okrem toho pomôžu vyplniť medzery v informáciách, podporiť predchádzanie, odhaľovanie a vyšetrovanie trestných činov v EÚ. Významný pokrok sa dosiahol aj vo vývoji účinných nástrojov na zabezpečenie plynulého cestovania leteckou dopravou do EÚ, z EÚ a v rámci nej, pričom sa posilnila kapacita orgánov na odhaľovanie bezpečnostných hrozieb, a to revíziou právneho rámca na používanie **vopred poskytovaných informácií o cestujúcich**.

Pokiaľ ide o terorizmus, zmenou **nariadenia o Eurojuste** týkajúcou sa digitálnej výmeny informácií v prípadoch terorizmu prijatou v roku 2023[78] sa prostredníctvom justičného registra

[72] COM(2024)173.

[73] V marci 2024 sa Bulharsko a Rumunsko stali členmi schengenského priestoru, ktorí plne uplatňujú schengenské *acquis*, a kontrola vnútorných hraníc na vzdušných a námorných hraniciach boli zrušené.

[74] COM(2020) 612.

[75] COM(2020) 613.

[76] Nariadenie, ktorým sa stanovuje spoločné konanie o medzinárodnej ochrane v Únii, COM(2016) 467 a COM(2020) 614

[77] COM(2021) 780, COM(2021) 782 a COM(2021) 784.

[78] Nariadenie (EÚ) 2023/2131, pokiaľ ide o digitálnu výmenu informácií v prípadoch terorizmu.

na boj proti terorizmu zefektívni výmena informácií medzi zodpovednými vnútroštátnymi orgánmi a Eurojustom.

Trestné stíhanie páchateľov počítačovej kriminality si vyžaduje konkrétne formy dôkazov, pričom sa dosiahol zásadný pokrok pri posilňovaní cezhraničnej spolupráce pri **výmene elektronických dôkazov**. Očakáva sa, že Druhým dodatkovým protokolom k Budapeštianskemu dohovoru Rady Európy[79] sa zintenzívni boj proti počítačovej kriminalite tým, že sa posilnia možnosti justičných orgánov zhromažďovať elektronické dôkazy o trestnom čine (napríklad vytvorením spoločných vyšetrovacích tímov). V rámci vnútorných pravidiel EÚ pre **elektronické dôkazy**[80], prijatých v roku 2023, sa zavedie nový systém na získavanie elektronických dôkazov v trestnom konaní tým, že umožnia orgánom presadzovania práva a justičným orgánom priamo oslovovať súkromných poskytovateľov služieb so sídlom v inom členskom štáte.

Umelá inteligencia sa stala všestranným a kľúčovým komponentom v technológiách, ktoré majú k dispozícii subjekty presadzovania práva a iné subjekty vnútornej bezpečnosti; zároveň by jej nasadením na tento účel mali rešpektovať základné práva. Umelú inteligenciu môžu však využívať aj páchatelia počítačovej kriminality na organizovanie sofistikovaných kybernetických útokov a iných škodlivých činností. **Nariadenie o umelej inteligencii (akt o umelej inteligencii)** je prvým krokom k regulácii používania umelej inteligencie v rámci EÚ, pričom poskytuje prvky ochrany pre zodpovedné používanie systémov umelej inteligencie v tejto oblasti a zároveň chráni základné práva a bezpečnosť občanov. Úrad pre umelú inteligenciu bude podporovať vykonávanie aktu, pričom zabezpečí rešpektovanie jeho záruk a procedurálnych požiadaviek. Komisia prispeje k vypracovaniu vhodných usmernení na podporu presadzovania práva a iných subjektov bezpečnosti, pokiaľ ide o vhodné a efektívne využívanie umelej inteligencie pri ich činnosti.

Hoci práca na **kritickom komunikačnom systéme EÚ** pokračuje, nové nariadenie, ktorým sa zriaďuje platforma spolupráce spoločných vyšetrovacích tímov[81], poskytuje zúčastneným stranám bezpečné prostriedky na výmenu dôkazov a informácií, účinnú komunikáciu a ľahkú spoluprácu s tretími krajinami.

So zvýšením cezhraničnej trestnej činnosti v EÚ čoraz častejšie dochádza k situáciám, keď má viacero členských štátov právomoc viesť trestné stíhanie v tej istej veci. Nové pravidlá **o odovzdávaní trestného konania** pomôžu predchádzať neefektívnej duplicite konaní a vyhýbať sa prípadom beztrestnosti v prípade odmietnutia odovzdania na základe európskeho zatykača a zabezpečia náležité rešpektovanie práv podozrivých a obetí. Efektívna cezhraničná justičná spolupráca si vyžaduje bezpečnú, spoľahlivú a časovo efektívnu komunikáciu medzi súdmi. Teraz to bude možné vďaka **balíku o digitálnej justícii**. Orgány budú môcť navzájom komunikovať a vymieňať si údaje súvisiace s prípadmi v občianskych, obchodných a trestných veciach prostredníctvom bezpečných a spoľahlivých digitálnych kanálov. Uľahčí sa tým boj proti trestnej činnosti a kľúčové bude urýchlené vykonávanie zo strany členských štátov.

---

79 Prijaté Výborom ministrov 17. novembra 2021.

80 Nariadenie (EÚ) 2023/1543 z 12. júla 2023 o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie a smernica (EÚ) 2023/1544 z 12. júla 2023, ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní.

81 Nariadenie (EÚ) 2023/969 z 10. mája 2023, ktorým sa zriaďuje platforma spolupráce na podporu fungovania spoločných vyšetrovacích tímov.

EÚ v akcii

V roku 2022 boli výsledkom platformy EMPACT:

- 9 922 zatknutí
- identifikácie 4 019 obetí obchodovania s ľuďmi
- zatknutia 3 646 prevádzačov
- zabavenia majetku a zaistených peňazí vo výške viac ako 180 miliónov eur
- zabavenia viac ako 62 ton drog

VI PREPOJENIE MEDZI VNÚTORNOU A VONKAJŠOU BEZPEČNOSŤOU: BEZPEČNOSŤ V EÚ, JEJ SUSEDSTVE A V PARTNERSKÝCH KRAJINÁCH

Rastúce prepojenie medzi vnútornou a vonkajšou bezpečnosťou sa vzhľadom na súčasný geopolitický kontext stalo evidentnejším až v posledných rokoch. EÚ je bezpečnejšia, keď sú bezpečnejší aj jej partneri. Len v roku 2023 sa vynaložilo približne 700 miliónov eur na pomoc kapacitám tretích krajín a posilnenie našej spolupráce s nimi v oblasti boja proti terorizmu a predchádzania násilnému extrémizmu a boja proti nemu, pričom 72 % bolo venovaných Afrike vzhľadom na rastúcu nestabilitu a prítomnosť teroristických skupín v regióne Sahel. To je päťnásobok výdavkov spred 10 rokov. Spolupráca v oblasti presadzovania práva s tretími krajinami bola medzitým začlenená do všetkých operatívnych akčných plánov platformy EMPACT.

Komisia konala rýchlo, aby predišla hrozbám vnútornej bezpečnosti vyplývajúcim z útočnej vojny Ruska voči **Ukrajine,** pričom zabezpečila maximálnu opatrnosť, pokiaľ ide o zneužívanie konfliktu a tokov tých, ktorí hľadajú bezpečnosť v Európe, zo strany organizovaných zločineckých skupín a skupín obchodujúcich s ľuďmi. Útvary Komisie a ESVČ sa s koordinátorom EÚ pre boj proti terorizmu dohodli s Ukrajinou na vytvorení štruktúrovaného dialógu o vnútornej bezpečnosti, a to aj v oblastiach, ako je obchodovanie so strelnými zbraňami a riadenie hraníc. Dialóg v oblasti kybernetiky medzi EÚ a Ukrajinou spolu s koordinovanou politickou, technickou, finančnou a materiálnou podporou zo strany EÚ pomohol Ukrajine posilniť jej kybernetickú odolnosť. Ohlásená kancelária EÚ pre inovácie v oblasti obrany v Kyjeve bude pôsobiť ako most medzi začínajúcimi podnikmi a inovátormi z EÚ a ukrajinským priemyslom a ozbrojenými silami, a to aj v oblasti kybernetickej obrany. Pomôže pri prenose prelomových technologických riešení, ktoré môžu mať vplyv priamo na bojisku.

Trestnoprávnym a bezpečnostným dôsledkom inváze Ruska na Ukrajinu a množstvu hybridných a kybernetických hrozieb je takisto vo veľkej miere vystavená **Moldavská republika**. Útvary Komisie v júli 2022 zriadili v spolupráci s ESVČ podporné centrum EÚ pre vnútornú bezpečnosť a riadenie hraníc s Moldavskou republikou. EÚ podporuje Moldavsko v tom, aby zlepšilo svoju odolnosť a schopnosť čeliť hybridným a kybernetickým hrozbám, a to aj prostredníctvom vykonávania odporúčaní obnoveného prieskumu týkajúceho sa hybridných rizík a prostredníctvom partnerskej misie EÚ v Moldavskej republike.

Bezpečnosť partnerov zo západného Balkánu je vzhľadom na ich blízkosť úzko spojená s vnútornou bezpečnosťou EÚ a spolupráca v oblasti presadzovania práva medzi EÚ a **krajinami západného Balkánu** sa počas tohto mandátu naďalej zintenzívňuje. Spoločný

akčný plán boja proti terorizmu podpísaný so všetkými partnermi zo západného Balkánu v roku 2018 napreduje s dobrým pokrokom a v krajinách, kde bola väčšina opatrení dokončená, teda v Severnom Macedónsku, Albánsku a Čiernej Hore, boli podpísané aktualizované mechanizmy. EÚ takisto pokračuje v posilňovaní kolektívnej kybernetickej odolnosti partnerov zo západného Balkánu prostredníctvom operačnej a technickej podpory, odbornej prípravy a zapojenia regiónu do mechanizmov kybernetickej bezpečnosti EÚ.

Potenciálny vplyv na vnútornú bezpečnosť EÚ vrátane výrazného nárastu incidentov v niektorých členských štátoch má aj súčasná situácia na **Blízkom východe**. Sieť finančných vyšetrovateľov na boj proti terorizmu umožnila členským štátom vymieňať si informácie o prípadoch súvisiacich s činnosťami Hamasu v oblasti získavania finančných prostriedkov v EÚ, čím vyšetrovateľom poskytla lepšie pochopenie, ako takéto hrozby riešiť.

Vzhľadom na vývoj v **Afganistane**, v koordinácii s Komisiou, vysokým predstaviteľom, predsedníctvom a kľúčovými agentúrami EÚ vypracoval koordinátor EÚ pre boj proti terorizmu akčný plán boja proti terorizmu pre Afganistan, ktorý Rada schválila v októbri 2021. EÚ sa naďalej angažuje v Afganistane a posilňuje svoju úlohu v širšom regióne prostredníctvom posilnenej spolupráce v otázkach bezpečnosti s **krajinami Strednej Ázie** a dialógu o boji proti terorizmu s **Pakistanom**.

EÚ posilnila spoluprácu s krajinami **Latinskej Ameriky a Karibiku,** najmä pokiaľ ide o boj proti organizovanému zločinu, obchodovaniu s drogami a financovaniu terorizmu.

Základom prístupu EÚ je **viacstranná spolupráca**. EÚ úzko spolupracuje s OSN, najmä s Úradom OSN pre boj proti terorizmu a výkonným riaditeľstvom Výboru pre boj proti terorizmu. EÚ takisto spolupracuje s viac ako 40 subjektmi OSN, ktoré tvoria globálny pakt OSN pre koordináciu boja proti terorizmu. Od septembra 2022 EÚ spolupredsedá Globálnemu fóru pre boj proti terorizmu s Egyptom, ktoré predstavuje viacstranné fórom na podporu civilných aspektov boja proti terorizmu a násilnému extrémizmu so silným zameraním na Afriku. EÚ je zároveň nevojenským partnerom globálnej koalície na boj proti Dá'iš a aktívne spolupracuje s NATO, Interpolom a OBSE. V oblasti boja proti praniu špinavých peňazí a terorizmu a financovaniu šírenia zbraní Komisia aktívne prispieva k práci Finančnej akčnej skupiny. Angažovanosť v globálnej koalícii na boj proti Dá'iš je dôležitou súčasťou zahraničnej politiky EÚ v reakcii na terorizmus/násilný extrémizmus a súvisiace hrozby.

EÚ výrazne prehĺbila a rozšírila svoju **spoluprácu s NATO**, najmä v oblastiach, ako je odolnosť, kritická infraštruktúra, zdravotná bezpečnosť, boj proti kybernetickým a hybridným hrozbám vrátane dezinformácií, vojenská mobilita, vesmír, vznikajúce prelomové technológie a klíma a obrana. V januári 2022 sa začal štruktúrovaný dialóg o odolnosti, ktorý posilnila osobitná skupina EÚ – NATO pre odolnosť kritickej infraštruktúry. V júni 2023 táto osobitná skupina zverejnila správu, v ktorej sa mapujú súčasné bezpečnostné výzvy pre kritickú infraštruktúru v štyroch kľúčových sektoroch (energetika, doprava, digitálna infraštruktúra a vesmír). Vykonávanie odporúčaní pre ďalšiu spoluprácu medzi EÚ a NATO obsiahnutých v správe rýchlo napreduje so zameraním na cvičenia, civilno-vojenskú koordináciu a spoluprácu so súkromným sektorom.

Revidované vykonávacie usmernenia **súboru nástrojov kybernetickej diplomacie EÚ** umožňujú rozvoj trvalých, prispôsobených, súdržných a koordinovaných stratégií proti vytrvalým aktérom kybernetických hrozieb, čím sa lepšie riešia výzvy pokračujúcich hrozieb nižšej úrovne v šedej zóne a činností, ktoré pochádzajú od vytrvalých aktérov kybernetických hrozieb. EÚ pokračuje v práci na zvyšovaní kybernetickej odolnosti, podpore partnerov

a presadzovaní rámca OSN pre zodpovedné správanie v kybernetickom priestore a na zabezpečení digitálnej infraštruktúry prostredníctvom Global Gateway. EÚ zintenzívnila **spoluprácu v oblasti kybernetickej bezpečnosti s NATO** prostredníctvom cieleného štruktúrovaného dialógu **a s medzinárodnými partnermi**. Dialóg so Spojenými štátmi, ktorého výsledkom je spoločný akčný plán EÚ a USA pre kybernetickú bezpečnosť, spoločná technická práca na mapovaní a porovnávaní právnych predpisov a úsilie v oblasti normalizácie, je dobrým príkladom konkrétnej spolupráce EÚ s partnermi na podporu globálnej kybernetickej bezpečnosti. V roku 2023 EÚ takisto obnovila kybernetické dialógy s Japonskom a Indiou a začala prvý so Spojeným kráľovstvom, čo umožňuje výmenu informácií o panoráme hrozieb, budovaní kybernetických kapacít a spolupráci na viacstranných a regionálnych fórach.

V posledných rokoch nadviazala EÚ **dialógy o boji proti terorizmu** s kľúčovými partnerskými krajinami a mnohostrannými organizáciami vrátane OSN, Austrálie, Egypta, Indie, Pakistanu, Saudskej Arábie, Turecka a USA. EÚ má takisto sieť 20 odborníkov v oblasti bezpečnosti/boja proti terorizmu rozmiestnených v delegáciách EÚ po celom svete na podporu cieľov zahraničnej a bezpečnostnej politiky EÚ týkajúcich sa boja proti terorizmu a násilnému extrémizmu. Komisia pokračuje v práci na odstraňovaní teroristického obsahu online z internetu, pričom dodržiava základné slobody v duchu Výzvy na činnosť z Christchurch[82]. V rámci vykonávania dohody o obchode a spolupráci sa v decembri 2023 a vo februári 2024 uskutočnilo prvé kolo dialógov medzi EÚ a Spojeným kráľovstvom o kybernetickom terorizme a boji proti nemu.

V súvislosti s **obchodovaním s drogami** bolo výsledkom stretnutia na vysokej úrovni v rámci mechanizmu koordinácie a spolupráce v oblasti drog EÚ – CELAC vo februári 2024 prijatie deklarácie[83], v ktorej sa určili priority spolupráce na nasledujúcich päť rokov. EÚ prispieva k práci globálnej koalície na riešenie hrozieb, ktoré predstavujú syntetické drogy, ktorú začali Spojené štáty americké. Európske monitorovacie centrum pre drogy a drogovú závislosť zvyšuje spoluprácu s Kolumbiou, Ekvádorom a Čile prostredníctvom uzatvorenia pracovných dohôd.

V boji proti závažnej a organizovanej trestnej činnosti sú nevyhnutné účinné **opatrenia na vymáhanie a konfiškáciu majetku pochádzajúceho z trestnej činnosti** na globálnej úrovni. Komisia sa zaviazala, že zabezpečí spoločný prístup EÚ v nadchádzajúcich rokovaniach o dodatkovom protokole k Varšavskému dohovoru Rady Európy **o** praní špinavých peňazí, vyhľadávaní, zaistení a konfiškácii ziskov z trestnej činnosti a o financovaní terorizmu, ktorý je potrebné aktualizovať, s prihliadnutím na rýchlo sa vyvíjajúce kriminálne prostredie a medzinárodný vývoj. Komisia prijala v apríli 2024 odporúčanie pre rozhodnutie, ktorým sa požaduje, aby Rada poverila Komisiu rokovať o protokole v mene EÚ.

V kontexte **hybridných hrozieb**, ktorých zložitosť a sofistikovanosť narastajú, má vykonávanie Strategického kompasu EÚ pre bezpečnosť a obranu zásadný význam. Útvary Komisie a Európska služba pre vonkajšiu činnosť prispeli k vytvoreniu súboru nástrojov EÚ na boj proti hybridným hrozbám, ktorý poskytuje rámec pre koordinovanú reakciu na hybridné kampane a spája všetky príslušné interné a externé nástroje a opatrenia. Operačný protokol EÚ na boj proti hybridným hrozbám aktualizovaný v apríli 2023 pomáha zabezpečiť účinné uplatňovanie procesov a nástrojov v reakcii na hybridné hrozby počas celého cyklu krízového riadenia. Zriaďujú sa tímy rýchlej reakcie EÚ na hybridné hrozby s cieľom poskytovať

[82] Výzva na činnosť z Christchurch, ktorú začali Francúzsko a Nový Zéland v roku 2019.

[83] Mechanizmus koordinácie a spolupráce v oblasti drog EÚ – CELAC – deklarácia z La Paz, 22. februára 2024.

krátkodobú prispôsobenú pomoc pri boji proti hybridným hrozbám v členských štátoch EÚ a partnerských krajinách.

Strategické a koordinované využívanie **manipulácie s informáciami a zasahovania zo zahraničia** predstavuje jasnú hrozbu pre našu bezpečnosť a bezpečnosť našich partnerov, keďže polovica sveta smeruje k volebným urnám v roku 2024. V uplynulých rokoch EÚ zintenzívnila svoju činnosť v boji proti manipulácii s informáciami a zasahovaniu zo zahraničia a zriadila pracovnú skupinu Komisie pre strategickú komunikáciu, ktorá má pomôcť urýchliť reakcie, pričom sa opierala o akčný plán pre európsku demokraciu a o vykonávanie strategického kompasu pre bezpečnosť a obranu EÚ.

Pokusy o zahraničné zasahovanie jednoznačne potvrdili obvinenia z korupcie prostredníctvom platieb tretích krajín politikom v EÚ. Riziko cudzieho zasahovania je obzvlášť intenzívne v období pred voľbami do Európskeho parlamentu. S cieľom zjednodušiť výmenu informácií pred voľbami, Rada v apríli 2024 aktivovala dojednania o integrovanej politickej reakcii na krízu (ďalej len „IPCR“).

V **strategickom kompase EÚ a analýze hrozieb** sa uznáva, že zmena klímy a zhoršovanie životného prostredia majú rastúci vplyv v oblastiach mieru, bezpečnosti a obrany. Tieto faktory v kombinácii s nedostatkom vody predstavujú hrozbu pre nestabilné prostredie v susedstve EÚ a môžu viesť ku krízam súvisiacim s vysídľovaním, vnútorným nepokojom alebo medzištátnym sporom. V júni 2023 Komisia a vysoký predstaviteľ pre zahraničné veci a bezpečnostnú politiku prijali spoločné oznámenie o prepojení medzi klímou a bezpečnosťou[84].

V decembri 2023 sa v balíku **opatrení v oblasti obrany demokracie** stanovilo, ako používať normy týkajúce sa transparentnosti na zastupovanie záujmov na ochranu demokracií EÚ pred rizikom skrytého zasahovania[85], a vysvetlila sa práca EÚ v boji proti dezinformáciám, ako je napríklad intenzívna výmena informácií medzi inštitúciami v reálnom čase, využívanie sietí na overovanie faktov a intenzívna práca s kľúčovými platformami prostredníctvom Kódexu postupov proti šíreniu dezinformácií a v súčasnosti aktu o digitálnych službách.

EÚ v akcii

V globalizovanom svete, kde sú závažná trestná činnosť a terorizmus čoraz viac nadnárodné, je spolupráca a výmena informácií medzi orgánmi presadzovania práva a justičnými orgánmi tretích krajín nevyhnutná.

Europol a Eurojust podpísali dohody o spolupráci s tretími krajinami s cieľom zlepšiť výmenu informácií v boji proti terorizmu a organizovanej trestnej činnosti. V júli 2023 nadobudla platnosť dohoda medzi EÚ a Novým Zélandom o výmene osobných údajov s Europolom a s Europolom sa rokuje o dohodách s Bolíviou, Brazíliou, Mexikom, Peru a Ekvádorom.

Eurojust uľahčuje justičnú spoluprácu v boji proti závažnej trestnej činnosti aj s tretími krajinami prostredníctvom 13 dohôd o spolupráci, s medzinárodnými justičnými sieťami prostredníctvom pracovných dohôd a v rámci siete tvoriacej viac ako 70 jurisdikcií na celom svete a prostredníctvom kontaktných miest. Do Eurojustu je vyslaných 12 styčných

[84] JOIN(2023) 19.
[85] COM(2023) 637.

prokurátorov z tretích krajín. Prebiehajú rokovania o dohodách o medzinárodnej justičnej spolupráci s Eurojustom s Brazíliou, Argentínou a Kolumbiou.

Agentúra ENISA takisto posilnila svoju spoluprácu a medzinárodný vplyv a nedávno podpísala pracovné dohody s ukrajinskými a americkými agentúrami pôsobiacimi v oblasti kybernetickej bezpečnosti.

VII VYKONÁVANIE BEZPEČNOSTNEJ ÚNIE

Správne vykonávanie bezpečnostnej únie je spoločnou zodpovednosťou, kde musí každý aktér zohrávať svoju úlohu. Komisia podporuje stratégie členských štátov, ich politiky, právne predpisy, organizáciu a budovanie kapacít s cieľom realizovať prácu bezpečnostnej únie, a to aj prostredníctvom Nástroja technickej podpory.

VII.1. Postupy v prípade nesplnenia povinnosti

Zatiaľ čo sa v práve EÚ v súčasnosti upevnili nové spoľahlivé pravidlá na lepšiu ochranu občanov EÚ, za včasnú transpozíciu, vykonávanie a uplatňovanie takýchto pravidiel sú zodpovedné členské štáty. Úroveň vykonávania právnych predpisov EÚ členskými štátmi v oblasti bezpečnostnej únie je väčšinou uspokojivá, v tejto citlivej oblasti však nie je priestor pre slabé miesta.

Komisia si vždy, keď je to potrebné, plní svoju povinnosť využiť postupy v prípade nesplnenia povinnosti a členské štáty postupuje Súdnemu dvoru Európskej únie, aby riešil prípady porušenia práva EÚ. Vďaka úzkej spolupráci medzi Komisiou a členskými štátmi bolo vyriešených mnoho postupov v prípade nesplnenia povinnosti, ktoré sa začali v rámci Stratégie EÚ pre bezpečnostnú úniu.

VII.2. Úloha agentúr a orgánov EÚ

Agentúry a orgány EÚ v oblasti spravodlivosti, vnútorných vecí a kybernetickej bezpečnosti zohrávajú kľúčovú úlohu pri vykonávaní *acquis* EÚ v oblasti bezpečnosti, ktoré sa s rozširovaním ich povinností neustále zväčšuje. Táto spolupráca viedla ku konkrétnym výsledkom, ako ukazuje napríklad **platforma EMPACT,** ktorá uľahčuje štruktúrovanú multidisciplinárnu spoluprácu členských štátov s podporou všetkých inštitúcií, orgánov a agentúr EÚ. V rámci operácií platformy EMPACT, ktoré sa uskutočňujú aj prostredníctvom osobitných operačných jednotiek, sa koordinuje úsilie členských štátov a operačných partnerov v boji proti zločineckým sieťam a závažnej trestnej činnosti.

Agentúra **ENISA** zohráva kľúčovú úlohu pri posilňovaní kapacít EÚ na predchádzanie kybernetickým útokom, ich odhaľovanie, odrádzanie od nich a reagovanie na ne, pričom podporuje kybernetickú odolnosť, chráni našu komunikáciu a údaje a udržuje online spoločnosť a hospodárstvo v bezpečí. Prostredníctvom odborného poradenstva a podpory v otázkach kybernetickej bezpečnosti, a to aj prostredníctvom správ o situačnej informovanosti a posúdení rizík, uľahčuje spoluprácu a výmenu informácií medzi členskými štátmi, inštitúciami EÚ a inými zainteresovanými stranami. Jej úlohy boli posilnené v súlade s novými pravidlami kybernetickej bezpečnosti. Medzi niektoré príklady prínosu agentúry ENISA ku kybernetickej bezpečnosti je nedávna aktualizácia prehľadu o kybernetickej bezpečnosti a odolnosti volieb alebo správa o osvedčených postupoch riadenia kybernetických kríz.

Európske centrum kompetencií v oblasti kybernetickej bezpečnosti je spoločne so sieťou národných koordinačných centier novým rámcom Európy, ktorý podporuje inovácie

a priemyselnú politiku v oblasti kybernetickej bezpečnosti. Po úplnom zriadení budú centrum a sieť prijímať strategické investičné rozhodnutia a združovať zdroje na zlepšenie a posilnenie technologických a priemyselných kybernetickobezpečnostných kapacít. Centrum tak bude zohrávať kľúčovú úlohu pri plnení cieľov programov Digitálna Európa a Horizont Európa v oblasti kybernetickej bezpečnosti.

Europol má od roku 2022 posilnený mandát na lepšiu podporu členských štátov EÚ v boji proti terorizmu, závažnej a organizovanej trestnej činnosti. Europol je v súčasnosti schopný podporovať členské štáty pri využívaní vznikajúcich technológií a vývoji spoločných technologických riešení. Aktuálne je takisto schopný prijímať údaje priamo od súkromných subjektov (pomáha napríklad riešiť online šírenie materiálu týkajúceho sa sexuálneho zneužívania detí). Okrem toho môže výkonný riaditeľ Europolu teraz navrhnúť vnútroštátne vyšetrovanie v prípade, že má trestný čin v jednom členskom štáte vplyv na spoločný záujem, na ktorý sa vzťahuje politika Únie. Mandátom sa posilňuje aj rámec Europolu pre ochranu údajov a dohľad európskeho dozorného úradníka pre ochranu údajov. Výsledkom nepretržitej práce Europolu sú mnohé úspešné operácie, ako je napríklad prípad Encrochat, ktorý doteraz viedol k viac ako 6 500 zatknutiam na celom svete. Mandátom sa posilňuje aj rámec Europolu pre ochranu údajov a dohľad európskeho dozorného úradníka pre ochranu údajov.

V októbri 2023 vstúpila do platnosti zmena nariadenia o **Eurojuste**, ktorou sa zlepšila schopnosť Eurojustu identifikovať prepojenia medzi vyšetrovaním a stíhaním terorizmu, vytvoriť moderný systém správy prípadov, poskytnúť bezpečný digitálny komunikačný kanál medzi členskými štátmi a Eurojustom a uľahčiť spoluprácu s tretími krajinami. Zmenou sa takisto zabezpečuje, že Eurojust má právomoci na uchovanie, analýzu a ukladanie dôkazov týkajúcich sa hlavných medzinárodných trestných činov.

Od začiatku svojej prevádzkovej činnosti v júni 2021 sa **Európska prokuratúra** ukázala ako nevyhnutná pri vyšetrovaní a stíhaní trestných činov poškodzujúcich finančné záujmy Únie, keď sa dôraz kladie na trestné činy poškodzujúce rozpočet Únie. K 31. decembru 2023 mala Európska prokuratúra 1 927 aktívnych vyšetrovaní, pričom škoda bola odhadnutá na viac ako 19,2 miliardy eur. S počtom 139 obžalôb podaných v roku 2023 začala Európska prokuratúra súdiť pred vnútroštátnymi súdmi viac podozrivých z podvodu v EÚ.

Agentúra **Frontex** bola aktívna aj v bezpečnostných záležitostiach pri plnení svojich úloh súvisiacich s hranicami, najmä v oblasti prevádzačstva, ako aj námornej bezpečnosti a obchodovania s ľuďmi. V januári 2024 agentúry Frontex a Europol podpísali dohodu, v ktorej sa uvádza, ako môžu tieto dve agentúry lepšie koordinovať činnosti, aby sa navzájom dopĺňali, a určiť konkrétne prioritné opatrenia, ktoré sa majú dosiahnuť v krátkodobom a dlhodobom horizonte. V praxi je úlohou agentúry Frontex poskytovať spravodajské informácie pochádzajúce z jej dozoru nad hranicami a ich monitorovania. Úlohou Europolu je na druhej strane poskytovať reakciu orgánov presadzovania práva na organizovanú cezhraničnú trestnú činnosť a terorizmus v rámci EÚ. Agentúra Frontex, **Európska námorná bezpečnostná agentúra** a **Európska agentúra pre kontrolu rybárstva** okrem toho posilnili svoju spoluprácu obnovením trojstrannej dohody o pracovných podmienkach týkajúcich sa funkcií pobrežnej stráže v roku 2021, čím prispeli k zvýšeniu bezpečnosti na mori.

VIII VÝHĽAD DO BUDÚCNOSTI

Množstvo legislatívnych a operačných opatrení prijatých za posledné štyri roky umožnilo EÚ lepšie čeliť bezpečnostným výzvam v porovnaní s tým, ako tomu bolo na začiatku mandátu

tejto Komisie. Neustále sa meniaca panoráma hrozieb však znamená, že treba využiť každú príležitosť na riešenie potenciálnych zraniteľností. **Súčasná stratégia bola prijatá s horizontom do roku 2025. Po tomto dátume bude potrebné pokračovať v práci s neustálou pozornosťou a odhodlaním.**

Koncept bezpečnosti, ktorý sa tradične sústreďuje na armádu a vnútorné záležitosti, musí držať krok s meniacimi sa hrozbami. Riziká a zraniteľnosti sa musia brať do úvahy od hospodárskej bezpečnosti po prerušenia dodávok a pripravenosť na krízy a zahŕňajú prakticky každý sektor našej spoločnosti, od zdravia, životného prostredia/klímy po energetiku a dopravu. Digitálny rozmer je teraz základom všetkých aspektov bezpečnosti a rozdiely medzi online a offline hrozbami postupne prekonáva nová realita, pričom väčšina hrozieb má kybernetický prvok a hybridný charakter. Súčasná situácia zároveň viac ako kedykoľvek predtým ukázala skutočnú spojitosť medzi vnútorným a vonkajším rozmerom bezpečnosti. Preto **je potrebné neustále úsilie, aby sa zabezpečilo, že bezpečnostné aspekty budú súčasťou všetkých politík a** rozhodovacích procesov EÚ.

Európska stratégia hospodárskej bezpečnosti z 20. júna 2023 dopĺňa „celospoločenský“ prístup navrhnutý v Stratégii EÚ pre bezpečnostnú úniu tým, že pridáva strategickú zložku, ktorá sa zameriava na obranu záujmov EÚ, jej členských štátov a občanov pred hrozbami pre naše hospodárstvo resp. pomocou ekonomických prostriedkov. Stanovuje sa v nej rámec na dosiahnutie **hospodárskej bezpečnosti** podporou hospodárskej základne a konkurencieschopnosti EÚ; ochranou pred rizikami; a partnerstvom s čo najširším okruhom krajín s cieľom riešiť spoločné obavy a záujmy, čo bude **kľúčovým prvkom pri úvahách o bezpečnosti EÚ v budúcnosti**.

Nová politika EÚ v oblasti kybernetickej obrany je len jednou oblasťou, ktorá dokazuje potrebu **zlepšiť koordináciu medzi civilnými komunitami a vojenským/obranným ekosystémom**. Prepojenia medzi týmito dvoma oblasťami sa v budúcnosti pravdepodobne rozšíria.

Páchatelia trestnej činnosti sa vo svojich aktivitách rýchlo prispôsobujú a nasadzujú nové technológie. **Skupina na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva**, ktorej spolupredsedá Komisia a predsedníctvo Rady, zvažuje výzvy, ktorým čelia odborníci v oblasti presadzovania práva, najmä pokiaľ ide o prístup k údajom. V budúcich úvahách o bezpečnosti bude potrebné **preskúmať, ako sa môžu pri presadzovaní práva využívať digitálne technológie a** zároveň zabezpečiť plné rešpektovanie základných práv, pokiaľ ide o prístup k údajom v oblastiach, ako je kvantová komunikačná infraštruktúra, umelá inteligencia a moderné technológie na úseku hraničného dozoru.

V rámci budúcich bezpečnostných politík sa bude musieť pokračovať v hľadaní účinných reakcií na vznikajúce riziká. Bude si to vyžadovať prehodnotenie toho, ako by mali inštitúcie a orgány EÚ, ako aj členské štáty, reagovať na výzvy, a zaručiť schopnosť EÚ reagovať v prípade potreby rýchlo. **Treba sa vyhnúť silám a mechanizmom reakcie, ktoré zdvojujú posúdenie rizík alebo komplikujú reakciu na krízu**.

Keďže EÚ naďalej preukazuje svoju schopnosť prispôsobiť sa meniacim sa rizikám, nemalo by sa okrem toho dovoliť, aby sa nové zraniteľnosti vyvinuli prostredníctvom nerovnakého vykonávania už dohodnutých nástrojov. **Účinné vykonávanie a uplatňovanie právnych predpisov na vnútroštátnej úrovni je nevyhnutné.**

Hoci kapacita EÚ bola posilnená rastúcou úlohou agentúr EÚ v oblasti bezpečnosti, **možno ju optimalizovať ďalším posilnením koordinácie a komplementárnosti medzi agentúrami.**. Zvážiť by sa mohlo prehĺbenie spolupráce nielen medzi agentúrami, ktoré tradične pracujú

v bezpečnostných záležitostiach, ako sú Europol, Eurojust a ENISA a takisto Frontex a Európska prokuratúra, ale aj odvetvovými agentúrami vrátane novej Agentúry Európskej únie pre drogy, Úradu pre boj proti praniu špinavých peňazí a financovaniu terorizmu, Agentúry Európskej únie pre bezpečnosť letectva, Európskej námornej bezpečnostnej agentúry a Európskej agentúry pre kontrolu rybárstva.

V Stratégii EÚ pre bezpečnostnú úniu na roky 2020 – 2025 sa konsolidoval súbor bezpečnostných nástrojov EÚ a v súčasnosti poskytuje silný základ na ochranu Európanov v budúcnosti. Opatrenia prijaté vo všetkých oblastiach bezpečnostnej únie budú naďalej nevyhnutné, aby sa zabezpečilo, že EÚ bude schopná prispôsobiť sa, a to aj v prípade výnimočných a neočakávaných hrozieb.