



V Bruseli 18. 10. 2023
COM(2023) 665 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE
o šiestej správe o pokroku pri vykonávaní Stratégie EÚ pre bezpečnostnú úniu

I. Úvod

Komisia pred tromi rokmi prijala Stratégiu EÚ pre bezpečnostnú úniu¹ na roky 2020 – 2025, v ktorej stanovila hlavné priority Únie v oblasti bezpečnosti. Odvtedy sme dosiahli značný pokrok v rámci všetkých štyroch pilierov stratégie – prijali sa kľúčové právne predpisy vzťahujúce sa na všetky možné oblasti od ochrany kritických subjektov až po posilnenie kybernetickej odolnosti. Panoráma bezpečnostných hrozieb v Európe a našom susedstve sa však stále vyvíja. Teroristické útoky na jednej z našich škôl vo Francúzsku a na bruselských uliciach, ktoré sa odohrali v posledných dňoch, nám neúprosne pripomínajú naliehavosť neustáleho prispôsobovania a posilňovania našej bezpečnostnej štruktúry. Ustavične narastá nebezpečenstvo, ktoré predstavujú kybernetické útoky, čo ešte zintenzívňujú aktéri s nekalými úmyslami zapájajúci sa do prebiehajúcich konfliktov. Stále sa znásobujú hybridné hrozby vrátane dezinformácií. Europol označil ruskú útočnú vojnu proti Ukrajine za príčinu značného nárastu kybernetických útokov na ciele EÚ, pričom dochádza k významným politicky motivovaným útokom, ktoré sú koordinované proruskými hackerskými skupinami². Prejavilo sa to zablokovaním prístupu na internet a prerušením prístupu ku kľúčovým službám, akými sú energetické siete³.

Stratégia EÚ pre bezpečnostnú úniu bola navrhnutá s cieľom pripraviť EÚ, aby dokázala lepšie odolávať meniacej sa panoráme hrozieb. V čase, keď sme čelili krízam spôsobeným pandemiou a vojnou sa ukázalo, aký dôležitý je prístup, ktorý sme prijali v stratégii, t. j. naše odhodlanie prepojiť celý bezpečnostný ekosystém EÚ a odstrániť bariéry medzi kybernetickým a fyzickým rozmerom bezpečnosti vrátane boja proti organizovanej trestnej činnosti a terorizmu, ako aj boja proti radikalizácii.

Ostražitosť si však vyžaduje, aby sme neustále skúmali, na čo sa v našom úsilí o zachovanie bezpečnosti občanov zabúda. V stratégii sa stanovujú prioritné oblasti, v ktorých môže Únia priniesť pridanú hodnotu, aby pomohla členským štátom pri posilňovaní bezpečnosti pre všetkých ľudí žijúcich v Európe. Od jej prijatia sa zrealizovali všetky stanovené opatrenia a začlenili sa do nej nové opatrenia s cieľom reagovať na pretrvávajúce bezpečnostné výzvy.

Celkovo Komisia v rámci Stratégie EÚ pre bezpečnostnú úniu predložila 36 legislatívnych iniciatív. V prípade viac ako polovice týchto návrhov sa už uzavreli medziinštitucionálne rokovania, ktoré viedli k prijatiu mnohých nových právnych predpisov, ktoré sú uvedené v tabuľke v prílohe. Niekoľko kľúčových iniciatív, ktoré navrhla Komisia, však ešte stále prerokúva Európsky parlament a Rada. Keďže aktuálne volebné obdobie sa blíži ku koncu (voľby do Európskeho parlamentu sa majú uskutočniť v júni 2024), je potrebné urýchlene pracovať na realizácii týchto zostávajúcich dokumentov, aby občania mohli plne využívať výhody bezpečnostnej únie. Táto šiesta správa o pokroku v oblasti bezpečnostnej únie sa preto zameriava na opísanie tých kľúčových legislatívnych a nelegislatívnych spisov týkajúcich sa bezpečnostnej únie prijatých Komisiou, v prípade ktorých je potrebné vyvinúť väčšie úsilie na ich dokončenie a účinné vykonávanie.

¹ COM(2020) 605.

² Distribuované útoky na vyradenie služby (DDoS): pozri správu Europolu zo série Spotlight s názvom *Cyber-attacks: the apex of crime-as-a-service* (Kybernetické útoky: zločin ako služba na vrchole), 13. septembra 2023.

³ Počas konfliktu na Ukrajine sa intenzívne využívajú malvéry typu *wiper*, aby zničili údaje a systémy, napríklad zablokovaním prístupu k internetu pre tisíce odberateľov v EÚ, ako aj dôležitej nemeckej energetickej spoločnosti, ktorá prišla o prístup k diaľkovému monitorovaniu vyše 5 800 veterných turbín. *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict* (Úloha kybernetiky v ruskej vojne proti Ukrajine: jej dosah a dôsledky pre budúcnosť ozbrojeného konfliktu), štúdia Európskeho parlamentu, september 2023 – PE 702.594.

Pokiaľ ide o už dohodnuté právne predpisy EÚ, ich prínos sa prejaví až po ich zavedení do praxe. Je potrebné zamerať sa na ich správnu a úplnú transpozíciu, vykonávanie a uplatňovanie členskými štátmi. Komisia v roku 2023 naďalej zabezpečovala, aby Stratégia EÚ pre bezpečnostnú úniu plnila svoje ciele, pričom využívala svoje inštitucionálne právomoci na začatie postupu v prípade nesplnenia povinnosti vždy, keď členské štáty netransponovali alebo nesprávne transponovali právne predpisy EÚ.

V tejto správe sú tiež zhrnuté prípady, keď boli opatrenia členských štátov a/alebo agentúr EÚ kľúčové pre plnenie cieľov. Agentúry EÚ zohrávajú mimoriadne dôležitú úlohu pri podpore vykonávania iniciatív týkajúcich sa bezpečnostnej únie, pričom ich povinnosti sa za posledné roky rozšírili. V správe sú uvedené niektoré z hlavných úloh, ktoré im boli pridelené, aby sa členským štátom poskytla posilnená podpora pri vykonávaní kľúčových iniciatív v rámci bezpečnostnej únie.

Geopolitická situácia navyše zdôraznila význam vonkajšej bezpečnosti pre našu vnútornú bezpečnosť. Silnejší vnútorný rámec EÚ v oblasti bezpečnosti je neoddeliteľne prepojený so silnejšími partnerstvami a spoluprácou s tretími krajinami. EÚ sa musí naďalej aktívne venovať tomu, ako môže globálna angažovanosť pomôcť zaistiť bezpečnosť občanov doma.

II. Nadčasové bezpečnostné prostredie

Kybernetická bezpečnosť a odolnosť kritickej infraštruktúry

Únia sa v rámci bezpečnostnej únie zaviazala zaručiť dobrú ochranu všetkým európskym občanom a podnikom, a to online i offline, ako aj k tomu, že bude podporovať otvorený, bezpečný a stabilný kybernetický priestor. Rastúci rozsah, frekvencia a vplyv kybernetických incidentov predstavujú vážnu hrozbu pre fungovanie sietí a informačných systémov, ako aj pre vnútorný trh. Útočná vojna Ruska proti Ukrajine ešte viac túto hrozbu prehĺbila a súčasné geopolitické napätie zhoršujú zásahy množstva kriminálnych a haktivistických aktérov napojených na štát. Sabotáž plynovodu Nord Stream, ku ktorej došlo minulú jeseň, poukázala na to, ako veľmi sú kľúčové sektory, akými sú energetika, digitálna infraštruktúra, doprava a vesmírny sektor, závislé od odolnej kritickej infraštruktúry. Nedávny incident s podmorským plynovodom a dátovým káblom v Estónsku a vo Fínsku demonštruje potrebu vysokej úrovne pripravenosti, aby bolo možné čeliť takýmto situáciám. Hoci príčina poškodenia stále nie je jasná a vyšetrovanie prebieha, povzbudivým prvkom je výmena informácií na rôznych úrovniach medzi členskými štátmi a Komisiou. Tieto narušenia nemali žiaden okamžitý vplyv, pokiaľ ide o internetové pripojenie či bezpečnosť dodávok plynu na európskej alebo miestnej úrovni. Je to znakom dosiahnutého pokroku a posilneného úsilia o pripravenosť v posledných mesiacoch.

Na zabezpečenie ochrany a odolnosti týchto kritickej infraštruktúr je preto potrebný jasný a rozsiahly právny rámec. V tejto súvislosti sa dosiahol zásadný pokrok súbežným prijatím revidovanej smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS 2)⁴ a smernice o odolnosti kritickej subjektov (CER)⁵, ktoré nadobudli účinnosť 16. januára 2023. Teraz sa od členských štátov naliehavo vyžaduje, aby tieto dôležité právne predpisy urýchlili a úplne transponovali, a to najneskôr do 17. októbra 2024, s cieľom zaviesť pevný rámec Únie na ochranu kritickej infraštruktúry Únie pred fyzickými alebo kybernetickými hrozbami.

⁴ Smernica (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a smernica (EÚ) 2018/1972 (smernica NIS 2).

⁵ Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritickej subjektov a o zrušení smernice Rady 2008/114/ES.

V júli 2023 Komisia stanovila v delegovanom nariadení Komisie základné služby v 11 odvetviach, na ktoré sa vzťahuje smernica CER⁶. V ďalšom kroku by členské štáty mali vykonať posúdenia rizík v prípade týchto služieb. V nadväznosti na odporúčanie Rady⁷ z 8. decembra 2022 sa zintenzívnila práca na záťažových testoch na kritickú infraštruktúru, pričom sa začalo v odvetví energetiky, a posilnila sa spolupráca s NATO a s kľúčovými partnerskými krajinami. Výsledkom tejto práce bola správa osobitnej skupiny EÚ – NATO pre odolnosť kritickú infraštruktúru z júna 2023, v ktorej sú zmapované súčasné bezpečnostné výzvy pre kritickú infraštruktúru v štyroch kľúčových odvetviach (energetika, doprava, digitálna infraštruktúra a vesmír) a uvedené odporúčania na posilnenie odolnosti. Odporúčania, ktoré sa okrem iného týkajú posilnenej koordinácie, zdieľania informácií a cvičení, vykonávajú pracovníci EÚ a NATO v rámci štruktúrovaného dialógu o odolnosti.

Komisia zároveň 6. septembra 2023 prijala návrh⁸ odporúčania Rady o koncepcii na posilnenie koordinácie na úrovni EÚ v reakcii na pokusy o narušenie kritickú infraštruktúru so značným cezhraničným významom. Dňa 4. októbra 2023 sa uskutočnilo cvičenie v podobe diskusie o koncepcii na základe scenára s cieľom otestovať, ako by sa uplatňoval v praxi, a poskytnúť podklady pre prebiehajúce rokovania o návrhu v Rade.

Na základe výziev Rady⁹ Komisia, vysoký predstaviteľ a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti vykonávajú hodnotenia rizík a vytvárajú scenáre rizík z hľadiska kybernetickej bezpečnosti. Táto činnosť sa prvotne zameriava na odvetvia telekomunikácií a elektrickej energie. Vďaka zapojeniu všetkých príslušných agentúr a sietí, civilných aj vojenských, sa prvýkrát vytvorilo komplexné a inkluzívne celouijné posúdenie. Ďalej doplní koordinované posúdenia bezpečnostných rizík kritických dodávateľských reťazcov, ktoré sa uskutočňujú v rámci smernice NIS 2, a posúdenia rizík a záťažové testy kritickú infraštruktúru v odvetviach energetiky, digitálnej infraštruktúry komunikácie, dopravy a vesmíru. V záujme koordinácie a súdržnosti by sa tieto činnosti mali vzájomne dopĺňať, aby pomohli vytvoriť štandardný prístup, a mali by usmerňovať vývoj budúcich posúdení. To, či budú tieto činnosti úspešné, bude teraz závisieť od aktívnej účasti členských štátov.

Fungovanie hospodárstiev a spoločností je čoraz závislejšie od služieb a údajov súvisiacich s vesmírom, najmä v oblasti bezpečnosti a obrany. Vesmír je čoraz spornejším strategickým odvetvím a jeho význam pre bezpečnosť vzrástol najmä v dôsledku ruskej invázie na Ukrajinu. V marci 2023 bola prijatá stratégia EÚ v oblasti kozmického priestoru pre bezpečnosť a obranu, aby posilnila naše strategické postavenie a autonómiu vo vesmíre. Kľúčovým opatrením vyplývajúcim z tejto stratégie bude, že Európska komisia v roku 2024 navrhne právny predpis EÚ o vesmíre, ktorým sa upraví bezpečnosť, udržateľnosť a odolnosť/ochrana vesmírnych činností v EÚ.

Pokiaľ ide o vonkajší rozmer, bezpečná infraštruktúra je základom odolnosti svetového hospodárstva a dodávateľských reťazcov¹⁰, a preto je súčasťou stratégie EÚ Global Gateway silný bezpečnostný rozmer. Rovnako je vzhľadom na prepojenia medzi infraštruktúrou EÚ a infraštruktúrou partnerských krajín nevyhnutná ďalšia medzinárodná spolupráca, ktorá posilní globálnu kybernetickú odolnosť a podporí slobodný, otvorený, bezpečný a chránený kybernetický priestor.

⁶ C(2023) 4878.

⁷ Odporúčanie Rady z 8. decembra 2022 o celouijnom koordinovanom prístupe k posilneniu odolnosti kritickú infraštruktúru.

⁸ COM(2023) 526.

⁹ Závery Rady z 23. mája 2022 o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti a výzva z Nevers z 9. marca 2022 na posilnenie spôsobilostí EÚ v oblasti kybernetickej bezpečnosti.

¹⁰ JOIN(2021) 30.

Akt o kybernetickej odolnosti

Pre európsku kybernetickú bezpečnosť má zásadný význam zaistenie toho, aby sa spotrebiteľia a podniky mohli spoliehať na bezpečné digitálne produkty. Komisia sa usilovala riešiť túto potrebu vo svojom návrhu aktu o kybernetickej odolnosti¹¹, ktorý bol prijatý 15. septembra 2022. Zaviedli by sa ním povinné horizontálne požiadavky kybernetickej bezpečnosti pre produkty s digitálnymi prvkami počas piatich rokov alebo celého ich životného cyklu (podľa toho, čo je kratšie). Vytvorili by sa ním podmienky pre návrh a vývoj bezpečných produktov s digitálnymi prvkami tým, že by sa zaistilo, aby sa na trh uvádzali hardvérové a softvérové produkty s čo najmenším počtom zraniteľností. Išlo by o kľúčový míľnik pri sprísňovaní európskych noriem kybernetickej bezpečnosti vo všetkých odvetviach a pravdepodobne by sa stal medzinárodným referenčným bodom, ktorý by poskytoval jasné výhody pre odvetvie kybernetickej bezpečnosti Únie na svetových trhoch. Európsky parlament a Rada prijali svoje príslušné pozície v júli 2023 a rokovania by mali rýchlo napredovať.

Pri zvyšovaní dôvery v produkty a služby IKT zohráva kľúčovú úlohu aj certifikácia kybernetickej bezpečnosti, ktorá spotrebiteľom, podnikom a orgánom umožňuje prijímať informované rozhodnutia s primeranou úrovňou kybernetickej bezpečnosti. Práca na certifikácii kybernetickej bezpečnosti napreduje, pričom systém certifikácie kybernetickej bezpečnosti EÚ založený na spoločných kritériách sa posudzuje v rámci postupu výboru. Kandidátsky systém certifikácie bezpečnosti cloudových služieb EÚ (EUCS) v súčasnosti pripravuje Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) a diskutuje sa o ňom v rámci európskej skupiny pre certifikáciu kybernetickej bezpečnosti. Intenzívna spolupráca s expertmi z rôznych odvetví, so spotrebiteľmi a s poskytovateľmi by mala viesť k vhodnému právnemu a technickému prístupu, na základe ktorého sa zaistia potrebné bezpečnostné záruky v súlade s právom Únie, medzinárodnými záväzkami a povinnosťami vyplývajúcimi z členstva vo WTO. Navyše ENISA pripravuje kandidátsky systém EU5G a peňaženku digitálnej identity EÚ. Na zvýšenie celkovej bezpečnosti produktov IKT, služieb IKT a procesov IKT je nevyhnutné spoločné úsilie všetkých členských štátov.

Nariadenia v oblasti informačnej bezpečnosti a kybernetickej bezpečnosti pre inštitúcie, orgány, úrady a agentúry EÚ

Navrhané nariadenia upravujúce kybernetickú bezpečnosť a informačnú bezpečnosť pre inštitúcie Únie, ktoré boli spoločne predložené v marci 2022, napredujú rôznym tempom. V júni minulého roka bola dosiahnutá politická dohoda týkajúca sa nariadenia o kybernetickej bezpečnosti, ktorá umožňuje posilniť kybernetickú bezpečnosť všetkých inštitúcií, orgánov, úradov a agentúr EÚ, pričom odráža význam, ktorý EÚ prikladá rýchlemu vykonaniu tohto návrhu. V tejto situácii je mimoriadne znepokojujúce, že súbežný návrh o informačnej bezpečnosti, ktorý je nevyhnutný na dokončenie pevného legislatívneho rámca pre inštitúcie, orgány, úrady a agentúry EÚ, napreduje nečakane pomaly. Oba návrhy by sa mali prijať pred voľbami do Európskeho parlamentu, aby európska administratíva bola v súčasnom geopolitickom kontexte dôveryhodná a odolná. Vďaka minimálnemu súboru pravidiel a noriem pre informačnú bezpečnosť pre všetky inštitúcie, orgány, úrady a agentúry EÚ by mali všetky zúčastnené strany istotu a zabezpečila by sa jednotná ochrana pred vyvíjajúcimi sa hrozbami pre utajované aj neutajované skutočnosti EÚ. Tieto nové pravidlá by spoločne poskytli stabilný základ pre bezpečnú výmenu informácií medzi inštitúciami, orgánmi, úradmi a agentúrami EÚ a s členskými štátmi, pričom by sa zaviedli štandardizované postupy a opatrenia na ochranu informačných tokov. Tieto pravidlá reagujú na viaceré výzvy Rady na posilnenie odolnosti inštitúcií, orgánov, úradov a agentúr EÚ a na lepšiu ochranu rozhodovacieho procesu Únie pred škodlivým zasahovaním.

¹¹ COM(2022) 454.

Akt o kybernetickej solidarite

Navrhovaný akt o kybernetickej solidarite¹², ktorý Komisia prijala 18. apríla 2023 a ktorý je založený na už existujúcom silnom strategickom, politickom a legislatívnom rámci, by ďalej posilnil odhaľovanie kybernetických hrozieb, odolnosť a pripravenosť na všetkých úrovniach ekosystému kybernetickej bezpečnosti Únie. Tieto ciele by sa realizovali prostredníctvom troch hlavných opatrení:

1. zavedenie **európskeho kybernetického štítu** s cieľom vybudovať a posilniť spoločné spôsobilosti týkajúce sa odhaľovania a situačnej informovanosti. Tvorili by ho vnútroštátne centrá bezpečnostných operácií a cezhraničné centrá bezpečnostných operácií;
2. vytvorenie **mechanizmu na riešenie kybernetických núdzových situácií** s cieľom podporiť členské štáty pri príprave na významné a rozsiahle kybernetické incidenty, pri reakcii na ne a pri okamžitom zotavení sa z nich. Podpora reakcie na incidenty by zahŕňala rezervu EÚ na účely kybernetickej bezpečnosti, ktorú by mali k dispozícii aj európske inštitúcie, orgány, úrady a agentúry Únie a tretie krajiny pridružené k programu Digitálna Európa, ak sa to stanovuje v ich dohode o pridružení k programu Digitálna Európa;
3. vytvorenie **európskeho mechanizmu preskúmania kybernetických incidentov**, ktorý bude slúžiť na skúmanie a posudzovanie konkrétnych významných alebo rozsiahlych incidentov. Správu o preskúmaní incidentu by koordinovala a pripravovala agentúra ENISA.

V Rade a Európskom parlamente sa začali diskusie. Uzavretie rokovaní pred skončením súčasného mandátu Európskeho parlamentu by výrazne posilnilo úsilie o ochranu občanov a podnikov v celej Únii.

Akadémia zručností v oblasti kybernetickej bezpečnosti

Vzhľadom na nárast kybernetických hrozieb EÚ naliehavo potrebuje odborníkov so zručnosťami a s kompetenciami na predchádzanie kybernetickým útokom, ich odhaľovanie, odrádzanie od nich a na ochranu EÚ pred takýmito útokmi. Odhaduje sa, že v oblasti kybernetickej bezpečnosti je v súčasnosti potrebných 883 000 odborníkov, kým v roku 2022 sa počet neobsadených pracovných miest pohyboval v rozmedzí od 260 000 do 500 000. Všetky skupiny obyvateľstva by sa mali nabádať, aby pomohli vyplniť túto medzeru, no konkrétne v roku 2022 tvorili ženy len 20 % absolventov odboru kybernetickej bezpečnosti a 19 % špecialistov na informačné a komunikačné technológie. V rámci Európskeho roka zručností 2023 Komisia 18. apríla 2023 prijala iniciatívu¹³ s cieľom zriadiť Akadémiu zručností v oblasti kybernetickej bezpečnosti, ktorá by riešila nedostatok odborníkov v oblasti kybernetickej bezpečnosti a ktorú členské štáty uvítali¹⁴. Akadémia zručností v oblasti kybernetickej bezpečnosti by spojila existujúce iniciatívy týkajúce sa kybernetických zručností a zlepšila by ich koordináciu. Komisia vyzýva členské štáty, regionálne a miestne orgány, ako aj európske verejné subjekty, aby prijali osobitné stratégie alebo iniciatívy týkajúce sa kybernetických zručností alebo aby začlenili kybernetické zručnosti do príslušných stratégií alebo iniciatív so širším rozsahom pôsobnosti (napr. kybernetická bezpečnosť, digitálne zručnosti, zamestnanosť atď.). Na zníženie nedostatku kybernetických zručností a súvisiaceho nedostatku pracovnej sily v Európe bude takisto nevyhnutné zapojenie súkromných zainteresovaných strán.

¹² COM(2023) 209.

¹³ COM(2023) 207.

¹⁴ Závery Rady z 22. mája 2023 o politike EÚ v oblasti kybernetickej obrany.

Drony

Ďalšou rastúcou hrozbou pre verejné priestory a kritické infraštruktúry je používanie dronov na nekalé účely. K incidentom s dronmi dochádza čoraz častejšie v rámci Únie aj mimo nej a riešenia na obranu proti dronom sú kľúčovým nástrojom orgánov presadzovania práva a iných verejných orgánov v Únii, ako aj súkromných prevádzkovateľov kritickej infraštruktúry. Oprávnené používanie dronov zároveň významne prispieva k súbežnej zelenej a digitálnej transformácii¹⁵. Ako bolo oznámené v stratégii v oblasti dronov 2.0 prijatej v novembri 2022, Komisia dnes prijíma oznámenie o tom, ako bojovať proti potenciálnym hrozbám, ktoré predstavujú drony, a to spolu s dvoma príručkami s praktickými usmerneniami ku kľúčovým technickým aspektom¹⁶. Cieľom iniciatívy je ponúknuť komplexný a harmonizovaný politický rámec so spoločným výkladom zavedených pravidiel na boj proti hrozbám, ktoré môžu predstavovať drony, a prispôbiť sa podľa potreby rýchlemu technologickému vývoju. V snahe zabezpečiť jeho úplné vykonávanie sa členské štáty a príslušní súkromní prevádzkovatelia vyzývajú, aby úzko spolupracovali s Komisiou.

Bezpečnosť v námornej a leteckej doprave

Nezákonné činnosti, ako je pirátstvo, ozbrojené lúpeže na mori, prevádzachstvo a obchodovanie s ľuďmi, so zbraňami a s drogami, ako aj terorizmus, sú naďalej výzvami pre ochranu námornej dopravy a zhoršujú ich vyvíjajúce sa hrozby vrátane hybridných a kybernetických útokov. Komisia a vysoký predstaviteľ prijali 10. marca 2023 spoločné oznámenie o aktualizácii stratégie námornej bezpečnosti EÚ¹⁷, ktorá by sa teraz mala vykonávať v súlade s aktualizovaným akčným plánom.

V oblasti bezpečnostnej ochrany letectva Komisia 2. februára 2023 prijala pracovný dokument útvarov Komisie *Working towards an enhanced and more resilient aviation security policy*¹⁸ (Práca na posilnenej a odolnejšej politike bezpečnostnej ochrany letectva), ktorý obsahuje ambiciózne program na 1. modernizáciu regulačnej architektúry bezpečnostnej ochrany letectva; 2. podporu vývoja a zavádzania inovativejších riešení a 3. aktualizáciu základnej úrovne bezpečnostnej ochrany letectva tak, aby letiská Únie mohli v plnej miere využívať nové a špičkové technológie na riešenie hrozieb s najvyššou prioritou. Do dvoch rokov je potrebné vykonať štrnásť hlavných opatrení.

Komisia vyzýva Európsky parlament a Radu, aby čo najskôr ukončili rokovania o týchto dokumentoch, a to v každom prípade pred skončením mandátu súčasného Európskeho parlamentu:

- návrh aktu o kybernetickej odolnosti,
- návrh aktu o kybernetickej solidarite,
- návrh nariadenia o informačnej bezpečnosti pre inštitúcie, orgány, úrady a agentúry EÚ.

Komisia vyzýva členské štáty, aby:

- sa usilovali o transpozíciu smernice o odolnosti kritických subjektov, ako aj o záťažové testovanie kritickej infraštruktúry v odvetví energetiky,
- prijali odporúčanie Rady o koncepcii koordinovanej reakcie na narušenia kritickej infraštruktúry so značným cezhraničným významom,

¹⁵ COM(2022) 652.

¹⁶ COM(2023) 659.

¹⁷ JOIN(2023) 8.

¹⁸ SWD(2023) 37.

- plne a urýchlene transponovali smernicu NIS 2 s cieľom posilniť kybernetickú bezpečnosť kľúčových a dôležitých subjektov,
- sa aktívne zapájali do vykonávania posúdení kybernetickobezpečnostných rizík a tvorby scenárov rizík pre kritickú infraštruktúru a dodávateľské reťazce,
- nadviazali na Akadémiu zručností v oblasti kybernetickej bezpečnosti prostredníctvom intenzívnej angažovanosti na európskej úrovni a špecializovaných vnútroštátnych stratégií alebo iniciatív v oblasti kybernetických zručností, pričom zapoja kľúčové zainteresované strany vrátane regionálnych a miestnych orgánov,
- spolupracovali s príslušnými súkromnými prevádzkovateľmi a Komisiou s cieľom zabezpečiť vykonávanie všetkých opatrení uvedených v oznámení o boji proti potenciálnym hrozbám zo strany dronov,
- vykonávali akčný plán stratégie námornej bezpečnosti EÚ a pravidelne podávali správy o dosiahnutých výsledkoch,
- vykonali 14 hlavných opatrení určených na posilnenie bezpečnostnej ochrany letectva.

III. Riešenie vyvíjajúcich sa hrozieb

Nové geopolitické napätie je jasným dôkazom toho, že bezpečnostné výzvy pre EÚ sa nielen zväčšujú, ale sú čoraz premenlivejšie, a prehlbuje ich hybridná povaha mnohých hrozieb. Bezpečnosť musí reagovať aj na zmeny v spoločnosti a technológiách. Pandémia COVID-19 priniesla viac príležitostí pre páchatel'ov počítačovej trestnej činnosti a zaznamenali sme počas nej najmä zvýšenú hrozbu výskytu materiálu obsahujúceho sexuálne zneužívanie detí online. Páchatelia trestnej činnosti a aktéri s nekalými úmyslami sú vždy pripravení zneužiť technologický vývoj. Vzhľadom na takéto často komplexné a viacrozmerné hrozby sú potrebné silné a jednotné opatrenia EÚ.

Nariadenie o boji proti sexuálnemu zneužívaniu detí

Z hodnotenia hrozieb internetovej organizovanej trestnej činnosti Europolu vyplynulo, že v roku 2022 ďalej stúpalo sexuálne vykorisťovanie a zneužívanie detí, pokiaľ ide o frekvenciu a závažnosť, pričom páchatelia naďalej využívali technické možnosti maskovania svojich činností a totožnosti¹⁹. Ukázalo sa, že súčasný systém založený na dobrovoľnom zisťovaní a oznamovaní spoločnosťami nie je na ochranu detí dostatočný. Dočasné nariadenie umožňuje dobrovoľné zisťovanie a oznamovanie spoločnosťami za predpokladu, že je to zákonné podľa všeobecného nariadenia o ochrane údajov. Platnosť tohto nariadenia končí v auguste 2024. V máji 2022 Komisia navrhla nariadenie²⁰ na riešenie zneužívania online služieb na účely sexuálneho zneužívania detí. Navrhovaný rámec kladie veľký dôraz na prevenciu. Spoločnosti by boli povinné posudzovať riziko sexuálneho zneužívania detí prostredníctvom svojich systémov a prijímať preventívne opatrenia. Len v prípade významného rizika by vnútroštátne súdy alebo nezávislé správne orgány mohli ako krajné opatrenie vydať poskytovateľom služieb ciele príkazy na zistenie. Nové nezávislé centrum EÚ by uľahčilo úsilie poskytovateľov služieb tým, že by fungovalo ako centrum odborných znalostí, poskytovalo spoľahlivé informácie o identifikovanom materiáli, prijímalo a analyzovalo oznámenia poskytovateľov

¹⁹ Europol (2023), Hodnotenie hrozieb internetovej organizovanej trestnej činnosti (IOCTA), 2023.

²⁰ COM(2022) 209.

o sexuálnom zneužívaní detí online s cieľom identifikovať chybné oznámenia, ako aj poskytovalo podporu obetiam. Je nevyhnutné, aby sa čo najskôr prijali a zaviedli nové pravidlá v záujme ochrany detí pred ďalším zneužívaním, zabránenia opätovnému výskytu materiálu online a postavenia páchatel'ov pred súd. V Rade a Parlamente prebiehajú rokovania s cieľom dosiahnuť dohodu o tomto dokumente pred skončením mandátu Parlamentu.

Smernica o boji proti násiliu na ženách a domácejmu násiliu

Kybernetické násilie na ženách, a to aj v súvislosti s domácim násilím, sa objavilo ako nová forma tohto násilia, ktorá sa prostredníctvom internetu a IT nástrojov šíri aj za hranicami jednotlivých členských štátov. V marci 2022 Komisia navrhla smernicu na riešenie násilia na ženách a domáceho násilia vrátane osobitných pravidiel týkajúcich sa kybernetického násilia a opatrení na odstránenie nedostatkov v oblasti ochrany, prístupu k spravodlivosti a prevencie. Jej včasné prijatie a vykonávanie by členským štátom poskytlo dodatočné nástroje na boj proti tejto forme trestnej činnosti. Spoluzákonodarcovia začali medziinštitucionálne rokovania v júli 2023 a usilujú sa ich ukončiť pred skončením súčasného mandátu Európskeho parlamentu.

Kybernetická bezpečnosť 5G

Bezpečnosť sietí 5G je hlavnou prioritou Komisie a neoddeliteľnou súčasťou jej Stratégie EÚ pre bezpečnostnú úniu. Siete 5G predstavujú ústrednú infraštruktúru, ktorá tvorí základ širokej škály služieb nevyhnutných pre fungovanie vnútorného trhu a pre dôležité spoločenské a hospodárske funkcie. Orgány členských štátov EÚ zastúpené v skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti s podporou Komisie a agentúry ENISA uverejnili 15. júna 2023 druhú správu o pokroku pri vykonávaní súboru nástrojov EÚ pre kybernetickú bezpečnosť 5G. V správe sa uvádza, že 24 členských štátov prijalo alebo pripravuje legislatívne opatrenia, ktorými sa vnútroštátnym orgánom udelia právomoci posudzovať dodávateľov a vydávať obmedzenia, a desať členských štátov takéto obmedzenia uložilo. Sú však potrebné ďalšie opatrenia, aby sa zabránilo zraniteľnostiam Únie ako celku, keďže by to mohlo mať vážny negatívny vplyv na bezpečnosť jednotlivých používateľov a spoločností v celej Únii a na kritickú infraštruktúru Únie. Súbor nástrojov musia bezodkladne zaviesť všetky členské štáty. V ten istý deň Komisia prijala oznámenie o vykonávaní súboru nástrojov členskými štátmi a o svojej vlastnej korporačnej komunikácii a činnostiach financovania zo strany Únie. Upozornilo sa tým na vážne obavy v súvislosti s rizikami pre bezpečnosť EÚ, ktoré predstavujú dodávatelia zariadení mobilných komunikačných sietí Huawei a ZTE. V tejto súvislosti Komisia prijíma opatrenia, aby zabránila vystaveniu svojej korporačnej komunikácie mobilným sieťam, ktoré ako dodávateľov využívajú spoločnosti Huawei a ZTE. Obstarávania nebudú zahŕňať nové služby pripojenia využívajúce zariadenia od daných dodávateľov a Komisia bude spolupracovať s členskými štátmi a telekomunikačnými operátormi s cieľom zabezpečiť, aby sa títo dodávatelia postupne vyradili z existujúcich služieb pripojenia na pracoviskách Komisie. Komisia takisto skúma, ako toto rozhodnutie zohľadniť v príslušných programoch a nástrojoch financovania Únie v plnom súlade s právom Únie.

Prístup k údajom na účely účinného presadzovania práva

V dnešnom digitálnom veku sa takmer každá trestná činnosť vyznačuje digitálnym prvkom. Technológie a nástroje sa používajú aj na účely trestnej činnosti a patria medzi ne aj tie, ktoré sú potrebné na zaistenie potrieb našej spoločnosti v oblasti kybernetickej bezpečnosti, ochrany údajov a súkromia. V dôsledku toho je čoraz náročnejšie účinne presadzovať právo v celej EÚ s cieľom chrániť verejnú bezpečnosť a predchádzať trestnej činnosti, odhaľovať ju, vyšetrovať a stíhať. Hoci sa na úrovni Únie a na vnútroštátnej úrovni vyvinulo značné úsilie, a to aj prostredníctvom právnych predpisov, ako aj iniciatív zameraných na budovanie kapacít a inovácie, právne a technické výzvy pretrvávajú. Komisia s podporou predsedníctva Rady zriadila skupinu na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva s cieľom poskytnúť platformu na spoluprácu širokej

škále zainteresovaných strán a expertov, aby preskúmali výzvy, ktorým čelia experti v oblasti presadzovania trestného práva (napr. šifrovanie, uchovávanie údajov, 5G a normalizácia). Komisia očakáva, že skupina na vysokej úrovni vypracuje do júna 2024 vyvážené, kvalitné a splniteľné odporúčania, v ktorých zohľadní komplexnosť týchto otázok, a to aj z hľadiska kybernetickej bezpečnosti a ochrany údajov. Členské štáty a zúčastnení experti sa preto vyzývajú, aby sa aktívne zapájali do tohto procesu a pracovali na účinných, zákonných a všeobecne akceptovaných riešeniach.

Hybridné hrozby

V geopolitickom kontexte, v ktorom sú hybridné hrozby čoraz komplexnejšie a sofistikovanejšie, poskytol Strategický kompas pre bezpečnosť a obranu EÚ²¹ (Strategický kompas) spoločné posúdenie hrozieb a výziev, ktorým Únia čelí, ako aj strategický akčný plán. Vzostup škodlivej kybernetickej činnosti štátnych a neštátnych subjektov, a to aj v kontexte vojny proti Ukrajine, ešte viac zdôraznil, že kybernetický priestor predstavuje oblasť zahraničnej a bezpečnostnej politiky. Potenciálne riziká škodlivých činností a dezinformácií si vyžadujú osobitnú ostražitosť vo volebných obdobiach, a to aj v období pred voľbami do Európskeho parlamentu v roku 2024.

Vzhľadom na vysoké riziká účinkov presahovania EÚ naďalej rozvíjala činnosti v oblasti budovania kybernetických kapacít a podporovala partnerstvá s tretími krajinami, a to aj prostredníctvom špecializovaných kybernetických dialógov, aby aktívne prispievala k svojej celkovej odolnosti. Bolo vyvinutých, zrevidovaných a posilnených niekoľko nástrojov na zlepšenie schopnosti Únie účinne riešiť hybridné hrozby, ako sa uvádza v 7. správe o pokroku v oblasti hybridných hrozieb uverejnenej 14. septembra 2023²². Medzi tieto nástroje patrí:

- súbor nástrojov EÚ na boj proti hybridným hrozbám, ktorým sa má zabezpečiť rámec pre koordinovanú a informovanú reakciu na hybridné hrozby a kampane,
- prebiehajúce práce na zriadení tímov rýchlej reakcie EÚ na hybridné hrozby, aby poskytovali krátkodobú podporu prispôbenú členským štátom, partnerským krajinám a misiám a operáciám v rámci spoločnej bezpečnostnej a obrannej politiky (SBOP),
- revidovaný operačný protokol EÚ na boj proti hybridným hrozbám²³, v ktorom sa opisujú procesy a štruktúry Únie zaoberajúce sa hybridnými hrozbami a kampaniami,
- revidované vykonávacie usmernenia k rámcu pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti²⁴ (ďalej len „súbor nástrojov kybernetickej diplomacie“), ktorý umožňuje rozvoj trvalých, prispôbených, súdržných a koordinovaných stratégií proti vytrvalým aktérom kybernetických hrozieb,
- súbor nástrojov proti manipulácii s informáciami a zasahovaniu zo zahraničia s cieľom posilniť existujúce nástroje Únie na predchádzanie takejto manipulácii a zasahovaniu, odrádzanie od nich a reakciu na ne,
- politika EÚ v oblasti kybernetickej obrany²⁵, aby sa posilnili spôsobilosti EÚ v oblasti kybernetickej obrany, zvýšilo situačné povedomie a koordinovala celá škála dostupných možností obrany s cieľom posilniť odolnosť, reagovať na kybernetické útoky a zabezpečiť solidaritu a vzájomnú pomoc.

Členské štáty sa preto vyzývajú, aby pokračovali v spolupráci v tejto oblasti a posilnili ju zabezpečením účinného vykonávania uvedených súborov nástrojov, a to aj prostredníctvom pravidelných cvičení, a dosiahnutím dohody o koncepcii tímov rýchlej reakcie na hybridné hrozby, ktorá poskytne usmernenia pre ďalšie kroky týkajúce sa zriadenia tímov.

²¹ Dokument Rady 7371/22.

²² SWD(2023) 315.

²³ SWD(2023) 116.

²⁴ 10289/23 z 8. júna 2023.

²⁵ JOIN(2022) 49.

Umelá inteligencia v kontexte presadzovania práva

Umelá inteligencia si rýchlo našla svoje miesto v každodennom živote. Vplyvy využívania umelej inteligencie na počítačovú kriminalitu a kybernetickú bezpečnosť ešte nie sú úplne známe, ale jednoznačne budú predstavovať nové výzvy. Hoci umelá inteligencia môže prinášať výhody, ak sa používa bezpečným a kontrolovaným spôsobom, v rukách aktérov s nekalými úmyslami môže byť nebezpečná, a to aj preto, že páchatelom trestnej činnosti pomáha skrývať ich totožnosť pri trestných činoch, ako je terorizmus a sexuálne zneužívanie detí. Orgány preto musia nevyhnutne držať krok s vývojom, aby sa zabránilo zneužívaniu a reagovalo na zneužitie²⁶. V rámci rokovaní o navrhovanom akte o umelej inteligencii sa vyvíja úsilie riešiť tieto otázky a pokročili do rozhodujúcej fázy, pričom spoluzákonodarcovia teraz diskutujú o technických a politických otázkach, na základe ktorých sa určí interakcia s touto technológiou v nadchádzajúcich rokoch. Bude nevyhnutné nájsť vyvážené riešenia, najmä pokiaľ ide o vysokorizikové aplikácie, a to aj v oblasti presadzovania práva.

Komisia vyzýva Európsky parlament a Radu, aby čo najskôr ukončili medziinštitucionálne rokovania o týchto otvorených dokumentoch, a to v každom prípade pred skončením mandátu súčasného Európskeho parlamentu:

- návrh nariadenia o boji proti sexuálnemu zneužívaniu detí,
- návrh smernice o boji proti násiliu na ženách a domácnému násiliu,
- návrh nariadenia, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii).

Komisia vyzýva členské štáty, aby:

- bezodkladne začali úplne vykonávať súbor nástrojov EÚ pre kybernetickú bezpečnosť 5G,
- podporovali prácu skupiny na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva s cieľom formulovať jasné, kvalitné a splniteľné odporúčania na primerané riešenie súčasných a očakávaných výziev,
- v spolupráci s vysokým predstaviteľom podnikli kroky na zabezpečenie účinného vykonávania súboru nástrojov EÚ na boj proti hybridným hrozbám, revidovaného súboru nástrojov kybernetickej diplomacie a súboru nástrojov proti manipulácii s informáciami a zasahovaniu zo zahraničia, a to aj prostredníctvom pravidelných cvičení a pri zohľadnení globálnej vývoja,
- dosiahli dohodu o koncepcii tímov rýchlej reakcie na hybridné hrozby.

IV. Ochrana Európanov pred terorizmom a organizovanou trestnou činnosťou

Neustále existuje riziko, že svetové alebo miestne udalosti vyvolajú nové teroristické činy. Zároveň medzi najzávažnejšie hrozby pre bezpečnosť EÚ patrí organizovaná trestná činnosť a obchodovanie s drogami. V snahe zintenzívniť spoločné úsilie Únie v boji proti týmto hrozbám sa spoločne pracuje na vykonávaní stratégie EÚ na boj proti organizovanej trestnej činnosti²⁷, stratégie EÚ v oblasti boja proti obchodovaniu s ľuďmi²⁸, protidrogového programu

²⁶ Pozri napríklad správu Europolu uverejnenú 17. apríla 2023: *ChatGPT - the impact of Large Language Models on Law Enforcement* (ChatGPT – vplyv veľkých jazykových modelov na presadzovanie práva).

²⁷ COM(2021) 170.

²⁸ COM(2021) 171.

a akčného plánu EÚ na boj proti drogám²⁹ a programu boja proti terorizmu pre EÚ³⁰. Reakcia na znepokojujúco sa zhoršujúcu situáciu, pokiaľ ide o organizovanú trestnú činnosť a obchodovanie s drogami, si však vyžaduje ďalšie zintenzívnenie práce členských štátov a EÚ, aby sa posilnila naša spoločná reakcia na zločinecké siete a poskytovala lepšia ochrana obetiam trestných činov, pričom sa v tom istom čase ako táto správa uverejňuje aj plán EÚ na boj proti obchodovaniu s drogami a organizovanej trestnej činnosti³¹.

Pokiaľ ide o boj proti terorizmu, EÚ posilňuje aj svoj súbor vonkajších nástrojov³² tým, že v plnej miere využíva dialógy na vysokej úrovni o boji proti terorizmu a siet' expertov na boj proti terorizmu/bezpečnosť v delegáciách EÚ, ako aj prostredníctvom účasti na multilaterálnych fórach, a to aj vo funkcii spolupredseda Globálneho fóra pre boj proti terorizmu (GCTF).

Obchodovanie s drogami

S novým mandátom Agentúry EÚ pre drogy, ktorý sa začne uplatňovať od júla 2024, bude mať EÚ viac možností riešiť zložité bezpečnostné a zdravotné problémy s dosahom na milióny ľudí v EÚ a na celom svete. Komisia takisto reviduje³³ nariadenia o drogových prekurzoroch³⁴ s cieľom riešiť hlavné výzvy identifikované v hodnotení z roku 2020³⁵, v ktorom sa zdôraznila potreba riešiť výzvy, ktoré predstavujú dizajnové prekurzory³⁶, v záujme zníženia ponuky nelegálnych drog.

No vzhľadom na bezprecedentný nárast nelegálnych drog dostupných v Európe sa musí v spolupráci s medzinárodnými partnermi zintenzívniť boj proti obchodovaniu s drogami. Na rozloženie zločineckých sietí a lepšiu ochranu obetí trestných činov sú potrebné ďalšie opatrenia zo strany členských štátov a EÚ. Komisia dnes prekladá plán EÚ na boj proti obchodovaniu s drogami a organizovanej trestnej činnosti. Stanovuje sa v ňom 17 opatrení v štyroch prioritných oblastiach: posilniť odolnosť logistických centier pomocou Európskej aliancie prístavov, rozložiť zločinecké siete, zvýšiť úsilie v oblasti predchádzania trestnej činnosti a posilniť spoluprácu s medzinárodnými partnermi. Tieto opatrenia sa majú zrealizovať v rokoch 2024 a 2025.

Strelné zbrane

Nedovolené obchodovanie so strelnými zbraňami podnecuje organizovanú trestnú činnosť v rámci EÚ, ako aj v jej susedstve. V EÚ je v rukách civilistov odhadom až 35 miliónov nedovolených strelných zbraní. V Schengenskom informačnom systéme sa uvádza zhruba 630 000 odcudzených alebo stratených zbraní. Rozvoj rýchleho doručovania balíkov a nových technológií, ako je 3D tlač, umožňuje nové formy nedovoleného obchodovania so strelnými zbraňami, pri ktorých možno uniknúť kontrolám. Riziko šírenia strelných zbraní zvyšuje aj útočná vojna Ruska proti Ukrajine. V októbri 2022 Komisia prijala návrh na aktualizáciu existujúcich právnych predpisov o dovoze, vývoze a tranzite civilných strelných zbraní s cieľom odstrániť medzery v existujúcich pravidlách, ktoré môžu zvýšiť počet pašovaných a odklonených strelných zbraní do EÚ³⁷. V strednodobom horizonte tieto nové pravidlá pomôžu znížiť riziko obchádzania embarga v prípade vývozu strelných zbraní na civilné použitie a zvýšiť kontroly dovozu tohto druhu strelných zbraní z krajín mimo EÚ. Obaja

²⁹ COM(2020) 606.

³⁰ COM(2020) 795.

³¹ COM(2023) 641.

³² Ako sa požaduje v Strategickom kompase a v záveroch Rady o riešení vonkajšieho rozmeru neustále sa vyvíjajúcej hrozby terorizmu a násilného extrémizmu, ktoré boli prijaté v júni 2022.

³³ Drogové prekurzory – právne predpisy EÚ (revidované pravidlá) (europa.eu).

³⁴ Nariadenie (ES) č. 273/2004 o prekurzoroch drog a nariadenie Rady (ES) č. 111/2005, ktorým sa stanovujú pravidlá sledovania obchodu s drogovými prekurzormi medzi Spoločenstvom a tretími krajinami.

³⁵ COM(2020) 768.

³⁶ Opatrenie č. 23 akčného plánu EÚ na boj proti drogám, COM(2020) 606.

³⁷ COM(2022) 480.

spoluzákodarcovia ešte musia prijať svoje pozície k tomuto dokumentu s cieľom dosiahnuť dohodu o tomto dokumente pred skončením mandátu Parlamentu.

Obchodovanie s ľuďmi

Obchodovanie s ľuďmi je obzvlášť závažnou formou organizovanej trestnej činnosti a závažným porušením základných práv. V rámci EÚ sa s obeťami obchoduje najmä na účely sexuálneho a pracovného vykorisťovania, ale aj na účely núteného žobrania, kriminality a iných foriem. Komisia v decembri 2022 navrhla zmeniť smernicu o boji proti obchodovaniu s ľuďmi³⁸ na základe aktualizovaných pravidiel s cieľom riešiť nedostatky v súčasnom právnom rámci. Po prijatí revidovanej smernice by sa do rozsahu pôsobnosti smernice doplnili nútené manželstvo a nezákonná adopcia a zaviedol by sa výslovný odkaz na online rozmer obchodovania s ľuďmi. Zahŕňala by aj povinný sankčný režim pre páchatel'ov a formalizovala by zriadenie národného referenčného mechanizmu s cieľom zlepšiť včasnú identifikáciu a cezhraničné sprostredkovanie pomoci a podpory obeťami. Vedomé využívanie služieb poskytovaných obeťami obchodovania s ľuďmi by sa stalo trestným činom a každoročný zber údajov o obchodovaní s ľuďmi, ktoré má uverejňovať Eurostat, by bol povinný. Rada prijala všeobecné smerovanie v júni 2023, zatiaľ čo Európsky parlament ešte musí prijať svoju pozíciu. Bude nutné rýchlo konať, aby bolo možné dosiahnuť dohodu pred skončením mandátu tohto Parlamentu.

Trestné činy proti životnému prostrediu

Trestné činy proti životnému prostrediu sa stávajú globálnou hrozbou, pričom ich medziročný rast sa odhaduje na 5 až 7 %. Pre organizovanú trestnú činnosť sú lákadlom značné zisky, ktoré možno dosiahnuť, právne medzery medzi členskými štátmi a nízke riziko odhalenia. Podľa Europolu existujú náznaky, že príjmy z týchto činností sa používajú na financovanie terorizmu. Komisia v decembri 2021 prijala návrh na nahradenie smernice z roku 2008 o ochrane životného prostredia prostredníctvom trestného práva. Návrh sa zameriava na spresnenie a aktualizáciu vymedzení kategórií trestných činov proti životnému prostrediu a na vymedzenie účinných, odrádzajúcich a primeraných druhov a úrovní sankcií pre fyzické a právnické osoby. Medzi nové trestné činy patria trestné činy spojené s nezákonným odlesňovaním, porušením právnych predpisov EÚ v oblasti chemických látok, nezákonným čerpaním povrchovej alebo podzemnej vody a nezákonnou recykláciou lodí. Cieľom návrhu je výrazne posilniť reťazec presadzovania práva a cezhraničnú spoluprácu medzi orgánmi členských štátov a agentúrami a orgánmi EÚ. Európsky parlament a Rada prijali svoje príslušné pozície k návrhu a sú v procese rokovaní, ktoré by mali byť schopní uzavrieť do konca roka. Na ďalšie posilnenie prevencie a presadzovania práva je potrebné vykonávať revidovaný akčný plán³⁹ na boj proti obchodovaniu s voľne žijúcimi druhmi živočíchov a rastlín.

Vymáhanie majetku a konfiškácia

Na narušenie organizovanej trestnej činnosti je nevyhnutné pripraviť páchatel'ov trestnej činnosti o ich nezákonné príjmy. Z toho dôvodu Komisia okrem návrhu, ktorým sa orgánom presadzovania práva poskytuje prístup k informáciám o bankových účtoch v celej EÚ⁴⁰ (v súvislosti s ktorým bola politická dohoda dosiahnutá v júni 2023), v máji 2022 predložila aj návrh týkajúci sa vymáhania majetku a konfiškácie⁴¹ s cieľom posilniť spôsobilosti v oblasti vyhľadávania, identifikácie, zaistenia, konfiškácie a správy majetku. Kľúčové ustanovenia návrhu sa týkajú požiadaviek na finančné vyšetrovanie a dodatočných právomocí a nástrojov

³⁸ COM(2022) 732.

³⁹ COM(2022) 581.

⁴⁰ COM(2021) 429.

⁴¹ COM(2022) 245.

úradov pre vyhľadávanie majetku, ako aj účinnejších opatrení na zaistenie a konfiškáciu v prípade širšej škály trestných činov. Jedným z nových trestných činov, na ktorý by sa tieto opatrenia vzťahovali, je porušenie reštriktívnych opatrení Únie. V decembri 2022 Komisia prijala samostatný návrh na harmonizáciu vymedzení trestných činov a sankcií v súvislosti s porušením reštriktívnych opatrení Únie. Účinné vykonávanie a presadzovanie reštriktívnych opatrení Únie zostáva najvyššou prioritou Komisie, čo posilňuje práca osobitnej skupiny pod názvom Freeze and Seize (Zmraziť a zaistiť), ktorú zriadila Komisia v reakcii na ruskú agresiu voči Ukrajine. Pokiaľ ide o oba návrhy, Európsky parlament a Rada prijali svoje pozície s cieľom dosiahnuť dohodu do konca tohto roka.

Balík opatrení proti praniu špinavých peňazí

Pranie špinavých peňazí je spojené v podstate so všetkými trestnými činnosťami, z ktorých plynú príjmy v EÚ⁴², a preto je kľúčovým prvkom v boji proti trestnej činnosti v EÚ. V júli 2021 Komisia predložila ambiciózne návrhy na posilnenie opatrení EÚ na predchádzanie praniu špinavých peňazí a financovaniu terorizmu⁴³ spolu so štyrmi legislatívnymi návrhmi na posilnenie prevencie a odhaľovania pokusov páchatel'ov trestnej činnosti o pranie nezákonných príjmov alebo financovanie teroristických činností prostredníctvom finančného systému. Spoluzákonodarcovia prijali jednu zo štyroch iniciatív z uvedeného balíka, ktorá sa týka zabezpečenia vysledovateľnosti prevodov kryptoaktív, v máji 2023⁴⁴. Toto nariadenie sa začne uplatňovať 30. decembra 2024. K tomuto dátumu budú musieť všetci poskytovatelia služieb kryptoaktív zhromažďovať a uchovávať informácie o pôvodcovi a prijímateľovi prevodov kryptoaktív. Cieľom zvyšných troch návrhov je i) zriadiť nový úrad EÚ pre boj proti praniu špinavých peňazí s cieľom zabezpečiť jednotný vysokokvalitný dohľad na celom vnútornom trhu, a to aj nad najrizikovejšími cezhraničnými subjektmi, pričom sa má podporovať a koordinovať práca finančných spravodajských jednotiek; ii) stanoviť harmonizované pravidlá pre súkromný sektor vrátane zavedenia celounijnového limitu vo výške 10 000 EUR pre veľké hotovostné platby výmenou za služby a tovar a iii) posilniť právomoci a nástroje spolupráce príslušných orgánov. Očakáva sa, že tento balík výrazne posilní schopnosť EÚ bojovať proti praniu špinavých peňazí a chrániť občanov EÚ pred terorizmom a organizovanou trestnou činnosťou. Spoluzákonodarcovia v súčasnosti rokujú o týchto troch zostávajúcich návrhoch s cieľom dosiahnuť dohodu o týchto dokumentoch pred skončením mandátu tohto Parlamentu.

Komisia vyzýva Európsky parlament a Radu, aby čo najskôr ukončili medziinštitucionálne rokovania o týchto otvorených dokumentoch, a to v každom prípade pred skončením mandátu súčasného Európskeho parlamentu:

- návrh smernice o vymáhaní majetku a konfiškácii,
- návrh smernice na harmonizáciu vymedzení trestných činov a sankcií v súvislosti s porušením reštriktívnych opatrení Únie,
- návrh smernice o boji proti obchodovaniu s ľuďmi,
- návrh smernice, ktorou sa zlepši ochrana životného prostredia prostredníctvom trestného práva,
- návrh balíka opatrení v oblasti boja proti praniu špinavých peňazí,

⁴² Europol, *Enterprising criminals – Europe's fight against the global networks of financial and economic crime* (Podnikajúci páchatelia trestnej činnosti – boj Európy proti celosvetovým sieťam finančnej a hospodárskej trestnej činnosti), 2020.

⁴³ COM(2021) 420.

⁴⁴ Nariadenie (EÚ) 2023/1113 z 31. mája 2023 o údajoch sprevádzajúcich prevody finančných prostriedkov a určitých kryptoaktív a o zmene smernice (EÚ) 2015/849.

- návrh na aktualizáciu existujúcich právnych predpisov o dovoze, vývoze a tranzite civilných strelných zbraní.

Komisia vyzýva členské štáty, agentúry a orgány EÚ, aby:

- spolupracovali na vykonávaní 17 opatrení plánu EÚ na boj proti obchodovaniu s drogami a organizovanej trestnej činnosti v rokoch 2023 a 2024.

V. Pevný európsky bezpečnostný ekosystém

V posledných rokoch majú bezpečnostné hrozby čoraz častejšie cezhraničný charakter, čo si vyžaduje ďalšie synergie a užšiu spoluprácu na všetkých úrovniach. Od prijatia Stratégie EÚ pre bezpečnostnú úniu sa zaviedli dôležité iniciatívy na maximalizáciu cezhraničnej spolupráce, konkrétne sa zjednodušili a zmodernizovali dostupné nástroje a postupy na vonkajších hraniciach aj v rámci schengenského priestoru, ako aj posilnila výmena informácií medzi orgánmi presadzovania práva a justičnými orgánmi v záujme lepšieho boja proti organizovanej trestnej činnosti. V tejto súvislosti je účinné vykonávanie rámca interoperability pre výmenu údajov dôležitým pilierom z hľadiska posilnenia bezpečnosti a účinnej európskej reakcie na cezhraničné hrozby pri súčasnom zaručení voľného pohybu v rámci EÚ.

Lepšia výmena informácií v rámci schengenského priestoru: vopred poskytované informácie o cestujúcich (API), záznamy o cestujúcich (PNR) a prümšký rámec II

Dva návrhy týkajúce sa API, ktoré Komisia prijala v decembri 2022⁴⁵, by posilnili vnútornú bezpečnosť Únie tým, že by orgánom presadzovania práva členských štátov poskytli dodatočné nástroje na boj proti závažnej trestnej činnosti a terorizmu. Konkrétne by vopred poskytované informácie o cestujúcich pri letoch vnútri EÚ, ktoré sa používajú spolu s PNR cestujúcich v leteckej doprave, orgánom presadzovania práva členských štátov umožnili výrazne zvýšiť efektívnosť vyšetrení prostredníctvom cielenejších zásahov. Je dôležité, aby sa navrhované pravidlá prijali čo najskôr: tým by sa nielen podporil boj proti organizovanej trestnej činnosti a terorizmu, ale výrazne by sa znížila aj potreba systematických kontrol všetkých cestujúcich v leteckej doprave v prípade dočasného obnovenia kontrol na vnútorných hraniciach, čo by uľahčilo leteckú dopravu a slobodu pohybu. Európska komisia 6. septembra 2023 odporučila Rade, aby povolila rokovania so Švajčiarskom, s Islandom a Nórskom o dohodách o prenose údajov PNR. Prijatím týchto troch odporúčaní by sa podporila jednotná a účinná vonkajšia politika EÚ v oblasti PNR.

Prümské výmeny každodenne využíva polícia na boj proti organizovanej trestnej činnosti, drogám, terorizmu, sexuálnemu vykorisťovaniu a obchodovaniu s ľuďmi. Návrhom nariadenia o automatizovanej výmene údajov na účely policajnej spolupráce („prümšký rámec II“)⁴⁶ sa reviduje existujúci prümšký rámec s cieľom odstrániť nedostatok informácií a posilniť predchádzanie trestným činom, ich odhaľovanie a vyšetrenie v EÚ. Revidované pravidlá automatizovanej výmeny údajov na účely policajnej spolupráce dopĺňajú návrhy týkajúce sa policajnej spolupráce v tomto mandáte, ako aj už prijaté odporúčanie Rady, ktorým sa posilňuje operačná cezhraničná spolupráca, a smernicu o výmene informácií medzi orgánmi presadzovania práva. Rýchle prijatie a vykonávanie týchto súvisiacich nástrojov by zlepšilo, uľahčilo a urýchlilo výmenu údajov medzi orgánmi presadzovania práva a pomohlo by identifikovať páchatel'ov trestnej činnosti.

⁴⁵ COM(2022) 729, COM(2022) 73.

⁴⁶ COM(2021) 784.

Plne interoperabilný systém riadenia hraníc v záujme bezpečného, silného, digitálneho a zjednoteného schengenského priestoru

Dobre fungujúci schengenský priestor bez vnútorných hraníc spočíva vo vzájomnej dôvere medzi členskými štátmi. A preto sú potrebné efektívne kontroly, či už na vonkajších hraniciach Únie, alebo ako alternatívne opatrenia na území členských štátov. Zmenou Kódexu schengenských hraníc⁴⁷, ktorú navrhla Komisia, sa stanovuje, ako môžu členské štáty lepšie využívať alternatívy ku kontrole vnútorných hraníc, čo môže poskytnúť vysokú úroveň bezpečnosti. Prijatie a úplné vykonávanie zmeny Kódexu schengenských hraníc má mimoriadny význam z hľadiska zaistenia vysokej a primeranej úrovne bezpečnosti v rámci schengenského priestoru. Pokračuje sa aj v príprave novej architektúry informačných systémov EÚ s cieľom lepšie podporovať vnútroštátne orgány pri práci na zaistení bezpečnosti a riadení hraníc. Túto architektúru tvorí obnovený Schengenský informačný systém, Európsky systém pre cestovné informácie a povolenia, systém vstup/výstup, aktualizácia vízového informačného systému a rámec interoperability na vzájomné prepojenie systémov, aby sa dosiahla úplná bezpečnosť. Táto nová architektúra by po úplnom dokončení poskytovala vnútroštátnym orgánom komplexnejšie a spoľahlivejšie bezpečnostné informácie. Žiaden z prvkov rámca interoperability nemožno vynechať, čo znamená, že oneskorenie jedného aspektu alebo oneskorenie v jednom členskom štáte vedie k oneskorenému zavedeniu pre všetkých. Oneskorenia v technickom vývoji systému vstup/výstup by sa mali obmedziť na minimum, aby systém vstup/výstup mohol byť čo najskôr uvedený do prevádzky a aby sa mohli zaviesť všetky kľúčové prvky rámca interoperability.

Návrhom týkajúcim sa preverovania⁴⁸ by sa zvýšila bezpečnosť v schengenskom priestore, keďže by sa vytvorili jednotné pravidlá týkajúce sa identifikácie štátnych príslušníkov tretích krajín, ktorí nespĺňajú podmienky pre vstup, ako sú uvedené v Kódexe schengenských hraníc, a tieto osoby by sa podrobili zdravotným a bezpečnostným kontrolám na vonkajších hraniciach. Navrhovaný systém Eurodac by podporil tieto ciele, keďže by sa v ňom v prípade, že to vyplynie z preverenia, uvádzalo, že osoba by mohla predstavovať ohrozenie vnútornej bezpečnosti. To by zasa uľahčilo vykonávanie navrhovaného nariadenia o riadení azylu a migrácie. Komisia vyzýva spoluzákonodarcov, aby urýchlene uzavreli rokovania o týchto dokumentoch pred skončením súčasného legislatívneho obdobia.

Boj proti korupcii

Korupcia značne poškodzuje naše demokracie, hospodárstvo a našu bezpečnosť, pretože pôsobí ako faktor, ktorý napomáha páchaniu organizovanej trestnej činnosti a nepriateľskému zahraničnému zasahovaniu. Úspešné predchádzanie korupcii a boj proti nej sú nevyhnutné na ochranu hodnôt EÚ a účinnosti politik EÚ, ako aj na presadzovanie právneho štátu a dôveru v tých, ktorí vládnu, a vo verejné inštitúcie. Ako predsedníčka von der Leyenová oznámila v prejave o stave Únie v roku 2022, Komisia 3. mája 2023 prijala balík protikorupčných opatrení⁴⁹. Návrh Komisie na smernicu o boji proti korupcii zahŕňa posilnené pravidlá kriminalizácie trestných činov korupcie a harmonizáciu sankcií v rámci EÚ. Okrem toho umožňuje účinné vyšetrovanie a trestné stíhanie a kladie silný dôraz na prevenciu a vytváranie kultúry integrity, v ktorej sa korupcia netoleruje. V Európskom parlamente a Rade sa začali diskusie o tomto návrhu. Členské štáty sa okrem toho vyzývajú, aby vykonali odporúčania vyplývajúce z protikorupčného piliera správy o právnom štáte 2023, ktorá bola prijatá 5. júla 2023. V návrhu vysokého predstaviteľa podporenom Komisiou sa navrhuje aj to, aby sa v rámci

⁴⁷ COM(2021) 891.

⁴⁸ COM(2020) 612.

⁴⁹ COM(2023) 234.

spoločnej zahraničnej a bezpečnostnej politiky (SZBP) zriadil osobitný sankčný režim cielený na závažné akty korupcie na celom svete.

Posilnenie práv obetí

Komisia 12. júla 2023 navrhla zmenu smernice o právach obetí s cieľom posilniť prístup obetí k informáciám, ich podporu a ochranu, účasť na trestnom konaní a prístup k náhrade škody. Jedným z celkových cieľov revízie je prispieť k vysokej úrovni bezpečnosti tým, že sa vytvorí bezpečnejšie prostredie pre obeť, aby ich motivovali oznamovať trestné činy, čo zníži strach z represálií.

Komisia vyzýva Európsky parlament a Radu, aby čo najskôr ukončili medziinštitucionálne rokovania o týchto otvorených dokumentoch, a to v každom prípade pred skončením mandátu súčasného Európskeho parlamentu:

- návrh nariadenia o prümskom rámci II,
- návrhy týkajúce sa vopred poskytovaných informácií o cestujúcich (API),
- návrhy týkajúce sa boja proti korupcii a predovšetkým zriadenia osobitného sankčného režimu v rámci spoločnej zahraničnej a bezpečnostnej politiky (SZBP),
- návrh na zmenu nariadenia o Kódexe schengenských hraníc,
- návrh smernice o právach obetí,
- návrh týkajúci sa preverovania.

Komisia vyzýva členské štáty, aby:

- čo najskôr zabezpečili uvedenie systému vstup/výstup do prevádzky, aby bolo možné dokončiť zavádzanie architektúry EÚ v oblasti výmeny informácií.

VI. Vykonávanie

Zaistenie bezpečnosti Európy ako celku je spoločnou zodpovednosťou, kde musí plniť svoju úlohu každý aktér, od Komisie a spoluzákonodarcov prijímajúcich nové, pevné, komplexné a praktické pravidlá až po včasnú transpozíciu, vykonávanie a uplatňovanie takýchto pravidiel členskými štátmi a operačnú činnosť, ktorú na mieste vykonávajú rôzne orgány, organizácie a zainteresované strany. Kľúčovú úlohu zohrávajú aj agentúry EÚ v oblasti spravodlivosti, vnútorných vecí a kybernetickej bezpečnosti. Ich úloha sa vďaka nedávnomu rozšíreniu ich povinností zvýšila.

Lepšie preverovanie prijímateľov finančných prostriedkov EÚ

Pokiaľ ide o plnenie rozpočtu EÚ, Komisia je zodpovedná za zabezpečenie toho, aby prijímatelia finančných prostriedkov EÚ rešpektovali hodnoty EÚ. Už existujú spoľahlivé mechanizmy a systémy kontroly určujúce, kto má nárok získať finančné prostriedky EÚ, a prebiehajúce rokovania o prepracovanom znení nariadenia o rozpočtových pravidlách majú takisto za cieľ poskytnúť Komisii silnejšie právne prostriedky, aby mohla v prípade potreby konať. Komisia okrem toho v súčasnosti pracuje na spôsoboch, ako ďalej skvalitniť preverovanie súčasných a potenciálnych budúcich prijímateľov finančných prostriedkov EÚ, zlepšovaním usmernení k povinnostiam týkajúcim sa rešpektovania hodnôt EÚ a dôsledkom, ktoré by mali vyplývať z porušenia hodnôt EÚ. Vďaka týmto usmerneniam sa objasnia povinnosti prijímateľov, ako aj subjektov vykonávajúcich kontroly na úrovni EÚ, pričom môžu slúžiť ako zdroj inšpirácie na vnútroštátnej úrovni. Ak dôjde k porušeniu podmienok financovania, Komisia sa nezdráha ani nebude zdráhať zastaviť spoluprácu s prijímateľmi príslušného projektu a v prípade potreby finančné prostriedky vymáhať. Je dôležité, aby členské štáty iniciatívne poskytovali Komisii informácie, ak sa dozvedia o možných rizikách v súvislosti s organizáciami žiadajúcimi o finančné prostriedky EÚ.

Postupy v prípade nesplnenia povinnosti

Pokiaľ ide o bezpečnosť, Komisia uskutočnila mnoho postupov v prípade nesplnenia povinnosti. Napríklad v roku 2023 sa začalo množstvo konaní o nesplnení povinnosti z dôvodu nesplnenia povinností podľa nariadenia z roku 2021 o riešení šírenia teroristického online obsahu (16 členských štátov)⁵⁰ a v priebehu rokov 2022 a 2023 boli 20 členským štátom doručené dodatočné formálne výzvy z dôvodu nesprávneho vykonávania smernice z roku 2011 o boji proti sexuálnemu zneužívaniu detí⁵¹. Značný počet konaní o nesplnení povinnosti stále prebieha z dôvodu nesúladu vnútroštátnych právnych predpisov so smernicou z roku 2017 o boji proti terorizmu⁵² a netransponovania pravidiel, ktoré uľahčujú využívanie finančných a iných informácií na predchádzanie určitým trestným činom, ich odhaľovanie, vyšetrovanie alebo stíhanie⁵³. Ďalšími oblastami, v ktorých stále prebiehajú konania o nesplnení povinnosti, sú právne predpisy v oblasti strelných zbraní, pravidiel týkajúce sa psychoaktívnych látok používaných v drogách, boj proti podvodom a falšovaniu bezhotovostných platobných prostriedkov, boj proti praniu špinavých peňazí, výmena informácií z registrov trestov medzi členskými štátmi EÚ a smernica o právach obetí. Členským štátom, ktoré vykonávajú dohodnuté iniciatívy a opatrenia, bola sprístupnená (technická a finančná) podpora a Komisia môže naďalej spolupracovať s členskými štátmi na optimalizácii vykonávania.

Monitorovanie prostredníctvom schengenských hodnotení a jeho nový systém správy

Schengenský hodnotiaci a monitorovací mechanizmus naďalej prispieva k účinnému vykonávaniu schengenských pravidiel zameraných na posilnenie bezpečnosti v priestore bez vnútorných kontrol. V roku 2023 boli vykonané prvé hodnotenia v rámci posilneného schengenského hodnotiaceho a monitorovacieho mechanizmu, ktoré umožnili včasnú identifikáciu a nápravu strategických slabých miest, ktoré majú cezhraničný vplyv na bezpečnosť a ochranu v rámci EÚ. Okrem toho Komisia v roku 2023 začala tematické schengenské hodnotenie s cieľom posúdiť postupy členských štátov, ktoré čelia podobným výzvam v boji proti obchodovaniu s drogami a ich dovozu do EÚ, s osobitným dôrazom na boj proti obchodovaniu s drogami vo veľkom objeme. Týmito hodnoteniami sa zaviedlo posilnené a komplexnejšie zameranie na bezpečnostné prvky Schengenu. Na základe výsledkov pravidelných, tematických a neohlásených schengenských hodnotení Rada v júni 2023 stanovila priority schengenského cyklu na roky 2023 – 2024. Stanovujú sa v ňom oblasti záujmu, ktoré si vyžadujú ďalší impulz pre bezpečnejší a silnejší schengenský priestor. Účinné a rýchle vykonávanie týchto priorít spoločne s intenzívnejšou politickou koordináciou schengenskej rady ešte viac posilní boj proti organizovanej trestnej činnosti a maximalizuje cezhraničnú operačnú spoluprácu.

Úloha agentúr a orgánov EÚ

Partnerstvo je kľúčovým prvkom vykonávania iniciatív týkajúcich sa bezpečnostnej únie, keďže na dosiahnutie konkrétnych výsledkov je potrebná práca rôznych vnútroštátnych a európskych úradov a orgánov. Napríklad EMPACT (Európska multidisciplinárna platforma proti hrozbám trestnej činnosti) umožňuje štruktúrovanú multidisciplinárnu spoluprácu členských štátov s podporou všetkých inštitúcií, orgánov a agentúr EÚ (ako je Europol, Frontex, Eurojust, CEPOL, OLAF, eu-LISA). V rámci operácií platformy EMPACT, ktoré sa uskutočňujú aj prostredníctvom osobitných operačných jednotiek (OTF), sa koordinuje úsilie členských štátov a operačných partnerov v boji proti zločineckým sieťam a závažnej trestnej činnosti. Len v roku 2022 operácie platformy

⁵⁰ Nariadenie (EÚ) 2021/784 o riešení šírenia teroristického obsahu online.

⁵¹ Smernica (EÚ) 2011/93 o boji proti sexuálnemu zneužívaniu detí.

⁵² Smernica Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV.

⁵³ Smernica Európskeho parlamentu a Rady (EÚ) 2019/1153 z 20. júna 2019, ktorou sa stanovujú pravidlá uľahčovania využívania finančných a iných informácií na predchádzanie určitým trestným činom, ich odhaľovanie, vyšetrovanie alebo stíhanie a ktorou sa zrušuje rozhodnutie Rady 2000/642/SVV.

EMPACT celkovo viedli k zatknutiu 9 922 osôb, zaisteniu aktív a peňazí vo výške viac ako 180 miliónov EUR, začatiu 9 263 vyšetrovaní, identifikácii 4 019 obetí, zaisteniu viac ako 62 ton drog, identifikácii 51 cieľov s vysokou hodnotou a k zatknutiu 12 z nich, operáciám v súvislosti s útočnou vojnou proti Ukrajine, najmä s cieľom bojovať proti obchodovaniu s ľuďmi a hrozbám súvisiacim so strelnými zbraňami⁵⁴.

Agentúra Frontex, Európska námorná bezpečnostná agentúra (EMSA) a Európska agentúra pre kontrolu rybníctva (EFCA) ďalej zintenzívňujú svoju spoluprácu v oblasti funkcií pobrežnej stráže s cieľom podporiť vnútroštátne orgány pri zvyšovaní bezpečnosti a ochrany na mori. Tieto agentúry budú výrazne prispievať k vykonávaniu stratégie námornej bezpečnosti EÚ.

Niekoľko iniciatív týkajúcich sa bezpečnostnej únie prináša nové povinnosti a úlohy príslušných agentúr, čo má v niektorých prípadoch vplyv na ľudské zdroje.

Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA)

Pokiaľ ide o pripravenosť a reakcie na incidenty s cieľom posilniť kybernetickú bezpečnosť, Komisia zaviedla krátkodobé opatrenie na podporu členských štátov, v rámci ktorého sa finančné prostriedky z programu Digitálna Európa previedli **Agentúre Európskej únie pre kybernetickú bezpečnosť (ENISA)**, aby sa posilnila pripravenosť a kapacity na reakciu na závažné kybernetické incidenty. Z tohto opatrenia vychádza návrh aktu o kybernetickej solidarite, ktorý bol prijatý v apríli 2023, a po jeho prijatí spoluzákondarcami môže byť agentúra ENISA poverená dodatočnými úlohami, ako je prevádzka a správa budúcej rezervy Únie na účely kybernetickej bezpečnosti alebo príprava správy o preskúmaní incidentu v nadväznosti na rozsiahle kybernetické incidenty. Na základe navrhovaného aktu o kybernetickej odolnosti by bola agentúra ENISA poverená prijímaním oznámení od výrobcov o zraniteľnostiach produktov s digitálnymi prvkami a o incidentoch, ktoré ovplyvňujú bezpečnosť týchto produktov, pričom agentúra ENISA by ich mala postúpiť príslušným jednotkám CSIRT alebo príslušným jednotným kontaktným miestam členských štátov. Od agentúry ENISA sa ďalej očakáva, že každé dva roky vypracuje technickú správu o vznikajúcich trendoch týkajúcich sa kybernetickobebezpečnostných rizík v prípade produktov s digitálnymi prvkami a predloží ju skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti.

Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti

Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“) je spoločne so sieťou národných koordinačných centier novým orgánom Únie, ktorý podporuje inovácie a priemyselnú politiku v oblasti kybernetickej bezpečnosti. Tento ekosystém posilní kapacity komunity v oblasti kybernetickobebezpečnostných technológií, zachová výskumnú excelentnosť a posilní konkurencieschopnosť priemyslu Únie v tejto oblasti. Kompetenčné centrum a sieť národných koordinačných centier budú prijímať strategické investičné rozhodnutia a združovať zdroje z Únie, jej členských štátov a nepriamo aj priemyslu, aby zlepšili a posilnili technologické a priemyselné kybernetickobebezpečnostné kapacity. Kompetenčné centrum preto zohráva kľúčovú úlohu pri plnení ambiciózných cieľov v oblasti kybernetickej bezpečnosti uvedených v programoch Digitálna Európa a Horizont Európa.

⁵⁴ Prehľadový výsledkový platforma EMPACT za rok 2022: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf

Kompetenčné centrum prijalo viac ako polovicu svojich zamestnancov a čoskoro prijme výkonného riaditeľa. Práca, ktorá už prebieha, zahŕňa kybernetickobezpečnostnú zložku programu Digitálna Európa a nový strategický program⁵⁵ pre vývoj a zavádzanie technológií, v ktorom sa stanovujú prioritné opatrenia na podporu MSP pri vývoji a využívaní strategických technológií, služieb a procesov kybernetickej bezpečnosti, na podporu a rozvoj profesionálnej pracovnej sily, ako aj na posilnenie odborných znalostí v oblasti výskumu, vývoja a inovácií v širšom európskom ekosystéme kybernetickej bezpečnosti.

Europol

Europol bude vďaka úplne novému mandátu lepšie pripravený na podporu členských štátov v boji proti organizovanej trestnej činnosti. Boj proti obchodovaniu s drogami je kľúčovou prioritou vzhľadom na jeho rastúci význam a čoraz väčší negatívny vplyv na bezpečnosť občanov EÚ. Po tom, čo Rada Európskej únie vydala 15. mája 2023 povolenie, Komisia aktívne pracuje na uzavretí medzinárodných dohôd s Bolíviou, Brazíliou, Ekvádorom, Mexikom a Peru o výmene osobných údajov s Europolom s cieľom predchádzať závažnej trestnej činnosti a terorizmu a bojovať proti nim.

Eurojust

Eurojust si s viac ako 20-ročnými skúsenosťami s poskytovaním právnej pomoci vnútroštátnym orgánom, pokiaľ ide o boj proti širokej škále závažných a zložitých cezhraničných trestných činov, upevnil svoje miesto v priestore slobody, bezpečnosti a spravodlivosti EÚ. V snahe posilniť celkovú spoluprácu Komisia rokuje o medzinárodných dohodách s cieľom uľahčiť spoluprácu medzi Eurojustom a 13 tretími krajinami pri výmene osobných údajov na účely boja proti organizovanej trestnej činnosti a terorizmu⁵⁶. Rokovania s Arménskom a Libanonom sa uzavreli, rokovania s Alžírskom a Kolumbiou prebiehajú a rokovania s Bosnou a Hercegovinou sa začali. Komisia vyzýva Európsky parlament a Radu, aby uzatvorili dohody s týmito krajinami pred koncom volebného obdobia, vďaka čomu sa posilní nadnárodná justičná spolupráca a rozšíri sa boj proti cezhraničným trestným činom.

Európska prokuratúra

Európska prokuratúra sa od začatia operačných činností v júni 2021 osvedčila ako účinný nástroj v súbore nástrojov Únie zameranom na vyšetrovanie a stíhanie trestných činov poškodzujúcich rozpočet Únie vrátane trestných činov súvisiacich s účasťou na zločinnom spolčení, keď sa dôraz kladie na trestné činy poškodzujúce rozpočet Únie. Komisia vyzýva členské štáty, ktoré sa ešte nezúčastňujú na posilnenej spolupráci Európskej prokuratúry, aby sa zapojili čo najskôr. Umožnilo by to dosiahnuť plný potenciál Európskej prokuratúry pri ochrane peňazí daňovníkov EÚ.

Agentúra EÚ pre drogy

Vďaka novému mandátu, ktorý prijali spoluzákonodarcovia v júni 2023, sa existujúce Európske monitorovacie centrum pre drogy a drogovú závislosť (EMCDDA) zmení na plnohodnotnú agentúru – **Agentúru Európskej únie pre drogy (EUDA)**, ktorá bude mať posilnenú úlohu. Agentúra bude môcť komplexnejšie posudzovať nové zdravotné a bezpečnostné výzvy, ktoré predstavujú nelegálne drogy, a účinnejšie prispievať k práci na úrovni členských štátov a na medzinárodnej úrovni. Hlavnou úlohou agentúry bude aj naďalej zhromažďovanie, analýza a šírenie údajov, ale posilnený mandát takisto agentúre umožní rozvíjať všeobecné kapacity

⁵⁵ https://cybersecurity-centre.europa.eu/strategic-agenda_en.

⁵⁶ Alžírsko, Argentína, Arménsko, Bosna a Hercegovina, Brazília, Egypt, Izrael, Jordánsko, Kolumbia, Libanon, Maroko, Tunisko a Turecko.

posudzovania zdravotných a bezpečnostných hrozieb s cieľom identifikovať vznikajúce hrozby vrátane súbežného užívania viacerých látok, posilniť spoluprácu prostredníctvom národných kontaktných miest a vytvoriť sieť laboratórií, ktoré budú agentúre poskytovať forenzné a toxikologické informácie. To agentúre umožní vydávať upozornenia, ak sa na trhu objavia obzvlášť nebezpečné látky, a zvyšovať informovanosť.

Komisia vyzýva Európsky parlament a Radu, aby čo najskôr ukončili medziinštitucionálne rokovania o týchto otvorených dokumentoch, a to v každom prípade pred skončením mandátu súčasného Európskeho parlamentu:

- návrh na prepracovanie nariadenia o rozpočtových pravidlách.

Komisia vyzýva členské štáty, aby:

- iniciatívne poskytovali Komisii informácie, ak sa dozvedia o možných rizikách v súvislosti s organizáciami žiadajúcimi o finančné prostriedky EÚ,
- urýchlene plnili priority schengenského cyklu na roky 2023 – 2024 v záujme bezpečnejšieho a silnejšieho schengenského priestoru,
- sa venovali postupom v prípade nespĺnenia povinnosti, ktoré proti nim prebiehajú, s cieľom zabezpečiť riadnu transpozíciu príslušných právnych predpisov.

VII. Záver

Počas posledných troch rokov sa neustále vyvíjalo rozhodné úsilie oživiť ambíciu vytvorenia bezpečnostnej únie pre EÚ. Dosiahol sa výrazný pokrok v celom spektre bezpečnostnej politiky. Neustále sa vyvíjajúce hrozby si aktuálne vyžadujú nepretržité úsilie, ako aj čerstvú dávku motivácie. Prácu na legislatívnom rámci je potrebné ukončiť v dostatočnom predstihu pred koncom volebného obdobia na jar 2024. Členské štáty sú neustále povinné transponovať, vykonávať a uplatňovať nové právne predpisy. Vykonávanie si vyžaduje spoločné úsilie, a to aj s podporou agentúr EÚ, a veľmi často si vyžaduje čoraz intenzívnejšiu spoluprácu s našimi medzinárodnými partnermi.

Len kolektívnym a rozhodným úsilím všetkých zainteresovaných strán dosiahneme úroveň bezpečnosti a ochrany v EÚ, ktorú občania očakávajú. V súčasnej situácii by malo byť pre každého aktéra prioritou, aby plnil svoju úlohu pri posilňovaní bezpečnosti EÚ.