EVROPSKÁ
KOMISE

V Bruselu dne 18.10.2023
COM(2023) 665 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

o šesté zprávě o pokroku při provádění strategie bezpečnostní unie EU

I. Úvod

Před třemi lety přijala Komise strategii bezpečnostní unie na období let 2020–2025[1], která definuje hlavní priority Unie v oblasti bezpečnosti. Od té doby jsme dosáhli výrazného pokroku v rámci všech čtyř pilířů strategie a přijali jsme zásadní právní předpisy v oblasti ochrany kritických subjektů i zvýšení kybernetické odolnosti. Mezitím se však bezpečnostní hrozby v Evropě a našem sousedství stále vyvíjejí. Teroristické útoky v jedné z našich škol ve Francii a v ulicích Bruselu, k nimž došlo v minulých dnech, jsou jasnou připomínkou toho, jak naléhavě je třeba pokračovat v přizpůsobování a posilování naší bezpečnostní architektury. Nebezpečí, které představují kybernetické útoky, stále roste, k čemuž přispívá i to, že se do probíhajících konfliktů zapojují subjekty s nekalými úmysly. Hybridní hrozby, včetně dezinformací, se stále množí. Europol označil ruskou útočnou válku proti Ukrajině za příčinu výrazného nárůstu kybernetických útoků proti cílům v EU, přičemž hlavní útoky byly politicky motivované a koordinované proruskými hackerskými skupinami[2]. Konkrétně se jednalo o blokování přístupu k internetu a přerušení klíčových služeb, jako jsou energetické sítě[3].

Strategie bezpečnostní unie byla navržena tak, aby EU dokázala lépe čelit vyvíjejícímu se prostředí hrozeb. V době, kdy jsme čelili krizím způsobeným pandemií a válkou, se ukázalo, jak důležitý je přístup, který jsme ve strategii zaujali, tedy naše odhodlání propojit všechny složky bezpečnostního ekosystému EU a odstranit rozdíly mezi kybernetickým a fyzickým rozměrem bezpečnosti, včetně boje proti organizované trestné činnosti a terorismu, jakož i boje proti radikalizaci.

Ostražitost však vyžaduje, abychom neustále zkoumali, co v našem úsilí o zajištění bezpečnosti našich občanů opomíjíme. Strategie stanovila prioritní oblasti, v nichž může Unie dodat přidanou hodnotu a podpořit tak členské státy při posilování bezpečnosti všech lidí žijících v Evropě. Od jejího přijetí byla všechna stanovená opatření splněna a byla začleněna nová, která reagují na přetrvávající bezpečnostní hrozby.

Komise v rámci strategie bezpečnostní unie předložila celkem 36 legislativních iniciativ. U více než poloviny těchto návrhů již byla ukončena interinstitucionální jednání, která vedla k přijetí nových silných právních předpisů, jak je popsáno v tabulce v příloze. O několika klíčových iniciativách navržených Komisí však Evropský parlament a Rada stále jednají. Vzhledem k tomu, že současné volební období končí volbami do Evropského parlamentu v červnu 2024, je potřeba tyto dosud nedořešené spisy urychleně projednat, aby občané mohli plně využívat výhod bezpečnostní unie. Tato šestá zpráva o pokroku bezpečnostní unie se proto zaměřuje na nastínění těch zásadních legislativních a nelegislativních dokumentů bezpečnostní unie, které Komise přijala a pro jejichž dokončení a účinné provádění je třeba vyvinout větší úsilí.

Pokud jde o již schválené právní předpisy EU, jejich přínos se projeví až po jejich uvedení do praxe. Je třeba se zaměřit na jejich správné a úplné provádění, uplatňování a používání členskými státy. V roce 2023 Komise nadále zajišťovala plnění strategie bezpečnostní unie EU tím, že využívala svých institucionálních pravomocí k zahájení řízení o porušení právních předpisů, kdykoli členské státy neprovedly nebo nesprávně provedly právní předpisy EU.

---

[1] COM(2020) 605.

[2] Útoky distribuovaným odmítnutím služby (DDoS): viz zpráva Europolu „Cyber-attacks: the apex of crime-as-a-service“ ze dne 13. září 2023.

[3] Během konfliktu na Ukrajině byly hojně využívány malwarové stírací programy ke zničení dat a systémů, které například narušily přístup k internetu tisícům předplatitelů v EU a také jedné velké německé energetické společnosti, která tak ztratila přístup k dálkovému monitorování více než 5 800 větrných turbín. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict, studie Evropského parlamentu, září 2023 – PE 702.594.

Tato zpráva rovněž shrnuje, v jakých případech je pro plnění strategie zásadní činnost členských států a/nebo agentur EU. Agentury EU hrají zásadní roli při podpoře provádění iniciativ bezpečnostní unie, přičemž jejich odpovědnost se během posledních let rozvinula. Zpráva uvádí některé z hlavních nových úkolů, které jim byly přiděleny s cílem poskytnout členským státům větší podporu při provádění klíčových iniciativ v rámci bezpečnostní unie.

Geopolitická situace navíc zdůraznila význam vnější bezpečnosti pro naši vnitřní bezpečnost. Silnější vnitřní rámec EU v oblasti bezpečnosti je neodmyslitelně spjat s posílením partnerství a spolupráce se třetími zeměmi. EU musí i nadále aktivně usilovat o to, aby angažovanost ve světě pomohla zajistit bezpečnost občanů doma.

II. Bezpečnostní prostředí, které obstojí i v budoucnosti

Kybernetická bezpečnost a odolnost kritické infrastruktury

Prostřednictvím bezpečnostní unie je Unie odhodlána zajistit ochranu všech evropských občanů a podniků online i offline a dále podporovat rozvoj otevřeného, bezpečného a stabilního kyberprostoru. Rostoucí počet kybernetických bezpečnostních incidentů, jejich četnost a dopad představují závažnou hrozbu jak pro fungování sítí a informačních systémů, tak pro vnitřní trh. Ruská útočná válka proti Ukrajině tuto hrozbu ještě více prohloubila a současné geopolitické napětí je umocněno zásahy mnoha se státem spojených, kriminálních a aktivistických hackerských subjektů. Sabotáž plynovodu Nord Stream, k níž došlo loni na podzim, poukázala na to, jak zásadní význam má odolná kritická infrastruktura pro základní odvětví, jako je energetika, digitální infrastruktura, doprava a vesmír. Nedávný incident, který se týkal podmořského plynovodu a telekomunikačního kabelu v Estonsku a Finsku, svědčí o tom, že čelit podobným situacím lze jen s vysokou mírou připravenosti. Přestože příčina škod zůstává nejasná a vyšetřování stále probíhá, sdílení informací na různých úrovních mezi členskými státy a Komisí je podnětné. Narušení nemělo žádný bezprostřední dopad na internetové připojení ani na bezpečnost dodávek plynu na evropské či místní úrovni. To je známkou dosaženého pokroku a zvýšeného úsilí o připravenost v posledních měsících.

Pro zajištění ochrany a odolnosti těchto kritických infrastruktur je proto nezbytný jasný a pevný právní rámec. V této souvislosti bylo dosaženo zásadního průlomu souběžným přijetím revidované směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS2)[4] a směrnice o odolnosti kritických subjektů (CER)[5], které obě vstoupily v platnost dne 16. ledna 2023. Členské státy se nyní naléhavě vyzývají, aby tyto zásadní právní předpisy urychleně a v plném rozsahu provedly do vnitrostátního práva, a to nejpozději do 17. října 2024, a zavedly tak pevný rámec Unie pro ochranu kritické infrastruktury Unie před fyzickými a kybernetickými hrozbami.

V červenci 2023 stanovila Komise v nařízení v přenesené pravomoci základní služby v 11 odvětvích, na něž se vztahuje směrnice CER[6]. Dalším krokem je, aby členské státy provedly

[4] Směrnice (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a směrnice (EU) 2018/1972 (směrnice NIS 2).

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

[6] C(2023) 4878.

posouzení rizik těchto služeb. V návaznosti na doporučení Rady[7] ze dne 8. prosince 2022 se zintenzivnily práce na zátěžových testech kritické infrastruktury, počínaje odvětvím energetiky, a na posílení spolupráce s NATO a klíčovými partnerskými zeměmi. Výsledkem této práce byla zpráva pracovní skupiny EU-NATO o odolnosti kritické infrastruktury z června 2023, která mapuje současné bezpečnostní výzvy pro kritickou infrastrukturu ve čtyřech klíčových odvětvích (energetika, doprava, digitální infrastruktura a vesmír) a předkládá doporučení ke zvýšení odolnosti. Doporučení, včetně doporučení týkajících se zvýšené koordinace, sdílení informací a cvičení, provádějí pracovníci EU a NATO v rámci strukturovaného dialogu o odolnosti.

Současně Komise dne 6. září 2023 přijala návrh[8] doporučení Rady o plánu pro posílení koordinace na úrovni EU v reakci na pokusy o narušení kritické infrastruktury se značným přeshraničním významem. Dne 4. října 2023 bylo uspořádáno cvičení v podobě diskuse o plánu založené na předem připravených scénářích s cílem ověřit, jak by se tento plán uplatňoval v praxi, a získat informace pro probíhající jednání o návrhu v Radě.

Komise, vysoký představitel a skupina pro spolupráci v oblasti bezpečnosti sítí a informací provádějí na základě výzev Rady[9] hodnocení rizik a sestavují rizikové scénáře z hlediska kybernetické bezpečnosti. Tato činnost se prvotně zaměřuje na odvětví telekomunikací a elektřiny. Zapojením všech příslušných agentur a sítí, civilních i vojenských, vzniká poprvé komplexní a inkluzivní hodnocení na úrovni celé Unie. Dále doplní koordinované hodnocení bezpečnostních rizik kritických dodavatelských řetězců, které probíhá v rámci NIS2, a hodnocení rizik a zátěžové testy kritické infrastruktury v odvětví energetiky, digitální infrastruktury, komunikací, dopravy a vesmíru. V zájmu koordinace a soudržnosti by tyto činnosti měly na sebe navazovat, aby pomohly zavést standardní přístup, a měly by být vodítkem pro vývoj budoucích cvičení. Úspěch těchto opatření bude nyní záviset na aktivním zapojení členských států.

Fungování ekonomik a společností je stále závislejší na službách a datech souvisejících s vesmírem, zejména v oblasti bezpečnosti a obrany. Vesmír je stále spornější strategickou oblastí a jeho význam pro bezpečnost vzrostl zejména po ruské invazi na Ukrajinu. V březnu 2023 byla přijata Kosmická strategie EU pro bezpečnost a obranu, která má posílit naše strategické postavení a autonomii ve vesmíru. Jako klíčové opatření vyplývající z této strategie navrhne Evropská komise v roce 2024 právní předpis EU pro oblast vesmíru, který bude upravovat bezpečnost, udržitelnost a odolnost/zabezpečení vesmírných činností v EU.

Pokud jde o vnější rozměr, základem odolnosti globální ekonomiky a dodavatelských řetězců je bezpečná infrastruktura[10], a proto strategie EU Global Gateway zahrnuje silný bezpečnostní rozměr. Stejně tak je vzhledem k propojení infrastruktury EU a partnerských zemí nezbytná další mezinárodní spolupráce, která posílí globální kybernetickou odolnost a podpoří svobodný, otevřený, bezpečný a chráněný kyberprostor.

Akt o kybernetické odolnosti

Pro evropskou kybernetickou bezpečnost je velmi důležité zajistit, aby se spotřebitelé a podniky mohli spolehnout na bezpečné digitální produkty. Komise se na tuto potřebu zaměřila ve svém

---

[7] Doporučení Rady ze dne 8. prosince 2022 o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury.

[8] COM(2023) 526.

[9] Závěry Rady ze dne 23. května 2022 o rozvoji kybernetické pozice Evropské unie a výzva z Nevers ze dne 9. března 2022 k posílení kapacit EU v oblasti kybernetické bezpečnosti.

[10] JOIN(2021) 30.

návrhu aktu o kybernetické odolnosti[11], který přijala dne 15. září 2022. Ten by zavedl povinné horizontální požadavky na kybernetickou bezpečnost produktů s digitálními prvky po dobu pěti let nebo po celou dobu jejich životního cyklu (podle toho, co je kratší). Vytvořil by podmínky pro navrhování a vývoj bezpečných produktů s digitálními prvky tím, že by zajistil, aby byly na trh uváděny hardwarové a softwarové produkty s co nejmenším počtem zranitelných míst. Jednalo by se o klíčový milník při zvyšování evropských standardů kybernetické bezpečnosti ve všech oblastech, který se pravděpodobně stane mezinárodním referenčním bodem a poskytne průmyslu kybernetické bezpečnosti Unie jasné výhody na světových trzích. Evropský parlament a Rada přijaly své postoje v červenci 2023 a jednání by měla rychle pokročit.

Klíčovou roli při zvyšování důvěry v produkty a služby IKT hraje také certifikace kybernetické bezpečnosti, která umožňuje spotřebitelům, podnikům a úřadům činit informovaná rozhodnutí s odpovídající úrovní kybernetické bezpečnosti. Činnosti v oblasti certifikace kybernetické bezpečnosti pokračují, přičemž v rámci postupu projednávání ve výborech se posuzuje systém certifikace kybernetické bezpečnosti založený na společných kritériích EU. Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) v současné době připravuje evropský systém certifikace kybernetické bezpečnosti pro cloudové služby (EUCS), který je projednáván v Evropské skupině pro certifikaci kybernetické bezpečnosti. Intenzivní práce s odborníky z různých odvětví, spotřebiteli a poskytovateli by měla vést k vytvoření spolehlivého právního a technického přístupu, který poskytne nezbytné bezpečnostní záruky v souladu s právem Unie, mezinárodními závazky a závazky WTO. Kromě toho agentura ENISA připravuje návrh systému EU5G a evropskou peněženku digitální identity (EUIDW). Pro zvýšení celkové bezpečnosti produktů, služeb a procesů IKT je nezbytné společné úsilí všech členských států.

Nařízení o bezpečnosti informací a kybernetické bezpečnosti pro orgány, instituce a jiné subjekty EU

Nařízení, která mají upravovat kybernetickou bezpečnost a bezpečnost informací vlastních institucí Unie, byla společně navržena v březnu 2022 a jejich vývoj probíhá různým tempem. V červnu loňského roku bylo dosaženo politické dohody o nařízení o kybernetické bezpečnosti, která umožňuje posílit kybernetickou bezpečnost všech orgánů, institucí a agentur EU a odráží význam, který EU přikládá rychlému provedení tohoto návrhu. V této situaci je obzvláště znepokojující, že souběžný návrh o bezpečnosti informací, který je nezbytný pro dokončení pevného legislativního rámce pro orgány, instituce a jiné subjekty EU, postupuje nečekaně pomalu. Oba návrhy by měly být přijaty před volbami do Evropského parlamentu, aby se evropská správa v současném geopolitickém kontextu dala označit za důvěryhodnou a odolnou. Vytvoření minimálního souboru pravidel a norem pro zabezpečení informací pro všechny orgány, instituce a jiné subjekty EU má přinést jistotu všem zúčastněným stranám a zajistit důslednou ochranu před vyvíjejícími se hrozbami pro jejich informace, ať už se jedná o utajované informace EU, nebo neutajované informace. Celkově mají tato nová pravidla poskytnout stabilní základ pro bezpečnou výměnu informací mezi orgány, institucemi a jinými subjekty EU a členskými státy a standardizované postupy a opatření na ochranu informačních toků. Reagují tak na četné výzvy Rady ke zvýšení odolnosti orgánů, institucí a jiných subjektů EU a k lepší ochraně rozhodovacího procesu Unie před nepřátelským narušováním.

Akt o kybernetické solidaritě

V návaznosti na stávající silný strategický, politický a legislativní rámec by navrhovaný akt o kybernetické solidaritě[12], který Komise přijala dne 18. dubna 2023, přispěl k lepšímu

[11] COM(2022) 454.
[12] COM(2023) 209.

odhalování kybernetických hrozeb a ke zvýšení odolnosti a připravenosti na všech úrovních unijního ekosystému kybernetické bezpečnosti. Tyto cíle mají být realizovány prostřednictvím tří hlavních opatření:

(1) zavedení ***evropského kybernetického štítu*** s cílem vytvořit a posílit společné schopnosti v oblasti detekce a situačního povědomí. Evropský kybernetický štít se skládá z národních bezpečnostních operačních středisek a přeshraničních bezpečnostních operačních středisek,
(2) vytvoření ***mechanismu pro mimořádné události v kybernetické oblasti***, který by podporoval členské státy při přípravě na významné a rozsáhlé kybernetické bezpečnostní incidenty, při reakci na ně a při okamžité obnově po takových incidentech. Podpora reakce na incidenty zahrnuje rezervu EU pro kybernetickou bezpečnost, která by byla k dispozici také orgánům, institucím a jiným subjektům Unie a třetím zemím přidruženým k programu Digitální Evropa za předpokladu, že to stanoví jejich dohoda o přidružení k programu Digitální Evropa,
(3) zřízení ***evropského mechanismu pro kybernetické bezpečnostní incidenty***, který bude přezkoumávat a posuzovat konkrétní významné nebo rozsáhlé incidenty. Zprávu o přezkumu po incidentu by koordinovala a připravovala agentura ENISA.

V Radě a Evropském parlamentu byla zahájena diskuse. Uzavření jednání před koncem stávajícího mandátu Evropského parlamentu by výrazně podpořilo úsilí o ochranu občanů a podniků v celé Unii.

Akademie dovedností v oblasti kybernetické bezpečnosti

Kybernetických hrozeb přibývá a EU naléhavě potřebuje odborníky s dovednostmi a kompetencemi, kteří by jí umožnili předcházet kybernetickým útokům, odhalovat je, odrazovat od nich a bránit ji před nimi. Potřeba pracovních sil v oblasti kybernetické bezpečnosti se v současnosti odhaduje na 883 000 odborníků, přičemž počet neobsazených pracovních míst se v roce 2022 pohyboval mezi 260 000 a 500 000. K zaplnění této mezery by měly být vybízeny všechny skupiny obyvatelstva, ale zejména ženy v roce 2022 tvořily pouze 20 % absolventů v oboru kybernetické bezpečnosti a 19 % odborníků v oblasti informačních a komunikačních technologií. V rámci Evropského roku dovedností 2023 přijala Komise dne 18. dubna 2023[13] iniciativu, která se setkala s kladným ohlasem členských států[14] a jejímž cílem je zřídit Akademii dovedností v oblasti kybernetické bezpečnosti, která by řešila nedostatek talentů v oblasti kybernetické bezpečnosti. Akademie dovedností v oblasti kybernetické bezpečnosti by spojila stávající iniciativy v oblasti kybernetických bezpečnostních dovedností a zlepšila jejich vzájemnou koordinaci. Komise vyzývá členské státy, regionální a místní orgány i evropské veřejné subjekty, aby přijaly specializované strategie nebo iniciativy týkající se kybernetických dovedností nebo aby kybernetické dovednosti začlenily do příslušných strategií nebo iniciativ s širší působností (např. kybernetická bezpečnost, digitální dovednosti, zaměstnanost atd.). Pro snížení nedostatku kybernetických dovedností a souvisejícího nedostatku pracovních sil v Evropě bude rovněž zásadní zapojení soukromých subjektů.

Bezpilotní letouny (drony)

Další rostoucí hrozbou pro veřejná prostranství a kritické infrastruktury je zneužívání dronů. Incidenty související s drony jsou v Unii i mimo ni stále častější a pro donucovací orgány a další veřejné orgány v Unii, jakož i pro soukromé provozovatele kritické infrastruktury jsou

[13] COM(2023) 207.
[14] Závěry Rady ze dne 22. května 2023 o politice kybernetické obrany EU.

klíčovým nástrojem protidronová řešení. Legitimní využívání dronů je přitom významným přínosem pro souběžnou zelenou a digitální transformaci[15]. Jak bylo oznámeno ve strategii pro drony 2.0 přijaté v listopadu 2022, Komise dnes přijímá sdělení o tom, jak čelit potenciálním hrozbám, které drony představují, doplněné dvěma příručkami s praktickými pokyny ke klíčovým technickým aspektům[16]. Cílem této iniciativy je nabídnout komplexní a harmonizovaný politický rámec se společným chápáním pravidel pro boj proti možným hrozbám ze strany dronů a pro případné přizpůsobení se rychlému vývoji technologií. Členské státy a příslušné soukromé subjekty se vyzývají, aby v úzké spolupráci s Komisí zajistili její plné provedení.

Námořní a letecká bezpečnost

Nezákonné činnosti, jako je pirátství, ozbrojené loupeže na moři, převaděčství migrantů a obchodování s lidmi, zbraněmi a narkotiky, jakož i terorismus, jsou pro námořní bezpečnost i nadále výzvou, k níž se přidávají i vyvíjející se hrozby včetně hybridních a kybernetických útoků. Komise společně s vysokým představitelem přijala dne 10. března 2023 společné sdělení, kterým se aktualizuje strategie EU v oblasti námořní bezpečnosti[17], jež by nyní měla být prováděna v souladu s aktualizovaným akčním plánem.

V oblasti ochrany letectví před protiprávními činy přijala Komise dne 2. února 2023 pracovní dokument útvarů Komise „Working towards an enhanced and more resilient aviation security policy“ (Snaha posílit politiku ochrany letectví před protiprávními činy a zvýšit její odolnost)[18], který obsahuje ambiciózní program, jehož cílem je 1) modernizovat regulační strukturu ochrany letectví před protiprávními činy, 2) podpořit vývoj a zavádění inovativnějších řešení a 3) aktualizovat základní úroveň ochrany letectví před protiprávními činy, aby letiště v Unii mohla plně využívat nové a špičkové technologie k řešení nejnaléhavějších hrozeb. Do dvou let je třeba provést čtrnáct stěžejních opatření.

Komise vyzývá Evropský parlament a Radu, aby urychleně, nejpozději však před koncem funkčního období současného Evropského parlamentu, dokončily jednání o těchto spisech:

- návrh aktu o kybernetické odolnosti,
- návrh aktu o kybernetické solidaritě,
- návrh nařízení o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie.

Komise členské státy vyzývá, aby:

- přednostně pokračovaly v provedení směrnice o odolnosti kritických subjektů ve vnitrostátním právu, jakož i v zátěžovém testování kritické infrastruktury v odvětví energetiky,
- přijaly doporučení Rady o plánu pro koordinaci reakce na narušení kritické infrastruktury se značným přeshraničním významem,
- plně a urychleně provedly směrnici NIS2 ve svém vnitrostátním právu s cílem zvýšit kybernetickou bezpečnost základních a významných subjektů,
- aktivně přistoupily k provádění posouzení rizik kybernetické bezpečnosti a vytváření rizikových scénářů kritické infrastruktury a dodavatelských řetězců,

[15] COM(2022) 652.
[16] COM (2023) 659.
[17] JOIN(2023) 8.
[18] SWD(2023) 37.

- navázaly na Akademii dovedností v oblasti kybernetické bezpečnosti silným zapojením na evropské úrovni a specializovanými vnitrostátními strategiemi nebo iniciativami v oblasti kybernetických bezpečnostních dovedností za účasti klíčových zúčastněných stran včetně regionálních a místních orgánů,
- spolupracovaly s příslušnými soukromými subjekty a Komisí s cílem zajistit provádění všech opatření uvedených ve sdělení o boji proti potenciálním hrozbám způsobeným drony,
- prováděly akční plán strategie EU pro námořní bezpečnost a pravidelně podávaly zprávy o dosažených výsledcích,
- prováděly čtrnáct stěžejních opatření určených ke zvýšení bezpečnosti letectví.

III. Potírání vyvíjejících se hrozeb

Nové geopolitické napětí je jasným důkazem toho, že bezpečnostní výzvy pro EU nejen rostou, ale jsou stále více nestabilní a umocněné hybridní povahou mnoha hrozeb. Bezpečnost musí rovněž reagovat na změny ve společnosti a technologiích. V souvislosti s pandemií COVID-19 se posílily příležitosti pro pachatele kybernetických trestných činů a zejména se zvýšilo riziko šíření materiálů zobrazujících pohlavní zneužívání dětí na internetu. Zločinci a subjekty s nekalými úmysly jsou vždy připraveni technologického vývoje využít ve svůj prospěch. Tváří v tvář těmto často komplexním a vícerozměrným hrozbám je zapotřebí důrazných a důsledných opatření na úrovni EU.

Nařízení o boji proti pohlavnímu zneužívání dětí na internetu

Z posouzení hrozeb organizované trestné činnosti na internetu, které provedl Europol, vyplynulo, že v roce 2022 došlo k dalšímu nárůstu četnosti a závažnosti pohlavního zneužívání a vykořisťování dětí, přičemž pachatelé nadále využívají technických možností k maskování svého jednání a identity[19]. Ukázalo se, že současný systém založený na dobrovolném odhalování a oznamování ze strany společností je pro ochranu dětí nedostatečný. Prozatímní nařízení umožňuje dobrovolné odhalování a oznamování ze strany společností, pokud je to v souladu se zákonem podle obecného nařízení o ochraně osobních údajů (GDPR). Platnost tohoto nařízení skončí v srpnu 2024. V květnu 2022 Komise navrhla nařízení[20], které se zabývá zneužíváním online služeb k pohlavnímu zneužívání dětí. Navrhovaný rámec klade velký důraz na prevenci. Společnostem by byla uložena povinnost posoudit riziko pohlavního zneužívání dětí prostřednictvím jejich systémů a přijmout preventivní opatření. Jako krajní opatření, a to pouze v případě významného rizika, by mohly vnitrostátní soudy nebo nezávislé správní orgány vydávat poskytovatelům služeb příkazy k cílenému odhalování. Úsilí poskytovatelů služeb by mělo usnadnit nové nezávislé středisko EU, které by fungovalo jako centrum odborných znalostí, poskytovalo spolehlivé informace o zjištěném materiálu, přijímalo a analyzovalo online oznámení o pohlavním zneužívání dětí od poskytovatelů služeb s cílem identifikovat chybná oznámení a rovněž poskytovalo podporu obětem. Je nezbytné, aby nová pravidla byla přijata a zavedena co nejdříve, aby se děti ochránily před dalším zneužíváním, zabránilo se opětovnému šíření materiálů na internetu a pachatelé byli postaveni před soud. V Radě a

[19] Europol (2023), Posouzení hrozeb organizované trestné činnosti na internetu (IOCTA) 2023.
[20] COM(2022) 209.

Parlamentu probíhají jednání s cílem dosáhnout dohody o tomto spisu před koncem mandátu Parlamentu.

Směrnice o potírání násilí vůči ženám a domácího násilí

Kybernetické násilí vůči ženám, a to i v souvislosti s domácím násilím, se stalo novou formou tohoto násilí, která prostřednictvím internetu a nástrojů IT překračuje hranice jednotlivých členských států. Komise v březnu 2022 navrhla směrnici, která se zabývá násilím na ženách a domácím násilím, včetně zvláštních pravidel pro kybernetické násilí a opatření k odstranění nedostatků v oblasti ochrany, přístupu ke spravedlnosti a prevence. Její včasné přijetí a provedení by členským státům poskytlo další nástroje pro potírání této formy trestné činnosti. Spolunormotvůrci zahájili interinstitucionální jednání v červenci 2023 a jejich cílem je dokončit jednání před koncem stávajícího mandátu Evropského parlamentu.

Kybernetická bezpečnost sítí 5G

Bezpečnost sítí 5G je pro Komisi hlavní prioritou a zásadní součástí její strategie bezpečnostní unie. Sítě 5G jsou ústřední infrastrukturou, která poskytuje základ pro širokou škálu služeb nezbytných pro fungování vnitřního trhu a pro životně důležité společenské a hospodářské funkce. Orgány členských států EU zastoupené ve skupině pro spolupráci v oblasti bezpečnosti sítí a informací za podpory Komise a agentury ENISA zveřejnily dne 15. června 2023 druhou zprávu o pokroku při provádění souboru opatření EU pro kybernetickou bezpečnost sítí 5G. Podle zprávy 24 členských států přijalo nebo připravuje legislativní opatření, která dávají vnitrostátním orgánům pravomoc provádět hodnocení dodavatelů a vydávat omezení, přičemž 10 členských států již taková omezení zavedlo. Je však třeba přijmout další opatření, aby se předešlo zranitelnosti Unie jako celku, což by mohlo mít závažné negativní dopady na bezpečnost jednotlivých uživatelů a společností v celé Unii a na kritickou infrastrukturu Unie. Všechny členské státy musí tento soubor opatření neprodleně zavést. Téhož dne přijala Komise sdělení o provádění souboru opatření členskými státy a o vlastních podnikových komunikacích a činnostech Unie v oblasti financování. Zdůraznila tak silné obavy z rizik, která pro bezpečnost EU představují dodavatelé komunikačních zařízení pro mobilní sítě Huawei a ZTE. V této souvislosti Komise přijímá opatření, aby zabránila vystavení své podnikové komunikace mobilním sítím, které využívají jako dodavatele společnosti Huawei a ZTE. Ze zadávání veřejných zakázek budou vyloučeny nové služby konektivity, které jsou závislé na zařízeních těchto dodavatelů, a Komise bude spolupracovat s členskými státy a telekomunikačními operátory, aby zajistila, že tito dodavatelé budou postupně vyřazováni ze stávajících služeb konektivity v prostorách Komise. Komise rovněž zkoumá, jak toto rozhodnutí zohlednit v příslušných programech a nástrojích financování Unie, a to v plném souladu s právem Unie.

Přístup k údajům pro účely účinného prosazování práva

Součástí téměř každého trestného činu je v dnešní digitální době digitální prvek. K trestným činům jsou využívány i různé technologie a nástroje, včetně těch, které jsou nezbytné pro zajištění potřeby kybernetické bezpečnosti, ochrany dat a soukromí naší společnosti. Proto je stále náročnější udržet účinné prosazování práva v celé EU, aby byla zajištěna veřejná bezpečnost a aby bylo možné předcházet trestné činnosti, odhalovat ji, vyšetřovat a stíhat. Ačkoli bylo na úrovni Unie i na vnitrostátní úrovni vynaloženo značné úsilí, mimo jiné prostřednictvím právních předpisů i iniciativ v oblasti budování kapacit a inovací, právní a technické problémy přetrvávají. Komise ve spolupráci s předsednictvím Rady zřídila skupinu na vysoké úrovni pro přístup k údajům pro účely účinného prosazování práva, aby poskytla platformu pro spolupráci široké škále zúčastněných stran a odborníků, kteří se budou zabývat výzvami, s nimiž se pracovníci v oblasti prosazování trestního práva potýkají (např. šifrování, uchovávání údajů, 5G a standardizace). Komise od skupiny na vysoké úrovni očekává, že do

června 2024 vypracuje vyvážená, solidní a dosažitelná doporučení, která budou zohledňovat složitost těchto otázek, a to i z hlediska kybernetické bezpečnosti a ochrany údajů. Členské státy a zúčastnění odborníci se proto vyzývají, aby se do tohoto procesu aktivně zapojili a usilovali o účinná, zákonná a obecně přijatelná řešení.

Hybridní hrozby

V geopolitickém kontextu, kdy hybridní hrozby nabývají na složitosti a sofistikovanosti, poskytl Strategický kompas pro bezpečnost a obranu EU[21] (dále jen „Strategický kompas“) společné posouzení hrozeb a výzev, kterým Unie čelí, a zároveň poskytl strategický akční plán. Nárůst nepřátelského jednání v kyberprostoru ze strany státních i nestátních subjektů, mimo jiné v souvislosti s válkou proti Ukrajině, dále poukázal na to, že kyberprostor je předmětem zahraniční i bezpečnostní politiky. Potenciální rizika nepřátelských jednání a dezinformací vyžadují v období voleb, včetně období před volbami do Evropského parlamentu v roce 2024, mimořádnou ostražitost.

Vzhledem k vysokému riziku účinků přelévání EU nadále rozvíjí činnosti v oblasti budování kybernetických kapacit a podporuje partnerství se třetími zeměmi, a to i prostřednictvím specializovaných kybernetických dialogů, aby aktivně přispěla ke své celkové odolnosti. S cílem zvýšit schopnost Unie účinně čelit hybridním hrozbám byla vyvinuta, revidována a posílena řada nástrojů, jak je popsáno v sedmé zprávě o pokroku v oblasti hybridních hrozeb zveřejněné dne 14. září 2023[22]. Mezi tyto nástroje patří:

- soubor hybridních nástrojů EU, který má zajistit rámec pro koordinovanou a dobře informovanou reakci na hybridní hrozby a kampaně,
- probíhající práce na zřízení týmů rychlé reakce EU na hybridní hrozby pro krátkodobou podporu přizpůsobenou požadavkům členských států, partnerských zemí a misí a operací společné bezpečnostní a obranné politiky (SBOP),
- revidovaný Protokol EU pro boj proti hybridním hrozbám („EU Playbook“)[23], který popisuje postupy a struktury Unie při řešení hybridních hrozeb a kampaní,
- revidované prováděcí pokyny rámce pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru[24] („soubor nástrojů pro diplomacii v oblasti kybernetiky“), které umožňují vypracovat trvalé, přizpůsobené, soudržné a koordinované strategie proti aktérům přetrvávajících kybernetických hrozeb,
- soubor nástrojů EU pro boj proti zahraniční manipulaci s informacemi a vměšování, který má posílit stávající nástroje Unie pro prevenci, odrazování a reakci na zahraniční manipulaci s informacemi a vměšování,
- politika kybernetické obrany EU[25], jejímž cílem je posílit schopnosti kybernetické obrany EU, zlepšit situační povědomí a koordinovat celou škálu dostupných obranných možností s cílem posílit odolnost, reagovat na kybernetické útoky a zajistit solidaritu a vzájemnou pomoc.

Členské státy se proto vyzývají, aby v této oblasti pokračovaly ve spolupráci a posilovaly ji, a to zajištěním účinného provádění výše uvedených souborů nástrojů, mimo jiné prostřednictvím pravidelných cvičení, a dosažením dohody o koncepci týmů rychlé reakce na hybridní hrozby, která poskytne vodítko pro další kroky směřující ke zřízení těchto týmů.

[21] Dokument Rady č. 7371/22.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23 ze dne 8. června 2023.
[25] JOIN(2022) 49.

UI v kontextu prosazování práva

Umělá inteligence se rychle stala běžnou součástí každodenního života. Dopady využívání umělé inteligence na kyberkriminalitu a kybernetickou bezpečnost zatím nejsou zcela známy, ale je zřejmé, že s sebou přinesou nové výzvy. Ačkoli při bezpečném a kontrolovaném používání může UI přinášet výhody, v rukou nepřátelských subjektů může představovat nebezpečí, mimo jiné tím, že pomáhá zločincům skrývat svou identitu při trestných činech, jako je terorismus a pohlavní zneužívání dětí. Je proto zásadní, aby orgány sledovaly aktuální vývoj, aby bylo možné předcházet zneužívání a reagovat na případy nesprávného využívání[26]. Jednání o navrhovaném aktu o umělé inteligenci se snaží tyto otázky řešit a vstoupila do klíčové fáze, kdy spolunormotvůrci diskutují o technických a politických otázkách, které budou v nadcházejících letech určovat interakce s touto technologií. Bude nezbytné nalézt vyvážená řešení, zejména pokud jde o vysoce rizikové aplikace, a to i v oblasti prosazování práva.

Komise vyzývá Evropský parlament a Radu, aby urychleně, nejpozději však před koncem funkčního období současného Evropského parlamentu, dokončily interinstitucionální jednání o následujících neprojednaných spisech:

- návrh nařízení o boji proti pohlavnímu zneužívání dětí na internetu,
- návrh směrnice o potírání násilí vůči ženám a domácího násilí,
- návrh nařízení, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci).

Komise členské státy vyzývá, aby:

- bezodkladně dosáhly úplného provedení souboru nástrojů EU pro kybernetickou bezpečnost sítí 5G,
- podpořily činnost skupiny na vysoké úrovni týkající se přístupu k údajům pro účely účinného prosazování práva s cílem formulovat jasná, pevná a dosažitelná doporučení k přiměřenému řešení současných a očekávaných problémů,
- ve spolupráci s vysokým představitelem podnikly kroky k zajištění účinného provádění souboru hybridních nástrojů EU, revidovaného souboru nástrojů pro diplomacii v oblasti kybernetiky a souboru nástrojů EU pro boj proti zahraniční manipulaci s informacemi a vměšování, a to i prostřednictvím pravidelných cvičení a s ohledem na dynamiku světového vývoje,
- dosáhly dohody o koncepci týmů rychlé reakce na hybridní hrozby.

IV. Ochrana Evropanů před terorismem a organizovanou trestnou činností

Riziko, že celosvětové nebo místní události zapříčiní nové projevy terorismu, je stále aktuální. Mezi nejvážnější hrozby pro bezpečnost EU zároveň patří organizovaná trestná činnost a obchod s drogami. S cílem zintenzivnit společné úsilí Unie v boji proti těmto hrozbám probíhá společná práce na provádění strategie EU pro boj proti organizované trestné činnosti[27], strategie EU pro boj proti obchodování s lidmi[28], Protidrogové agendy a Akčního plánu EU pro oblast

[26] Viz například zpráva Europolu zveřejněná dne 17. dubna 2023: ChatGPT – the impact of Large Language Models on Law Enforcement.
[27] COM(2021) 170.
[28] COM(2021) 171.

drog[29] a Protiteroristické agendy EU[30]. Je však třeba, aby členské státy a EU v reakci na znepokojivě se zhoršující situaci v oblasti organizované trestné činnosti a obchodování s drogami dále zintenzivnily svou práci s cílem posílit naši společnou reakci na zločinecké sítě a lépe chránit oběti trestné činnosti. Současně s touto zprávou je zveřejněn plán EU pro boj proti obchodu s drogami a organizované trestné činnosti[31].

V oblasti boje proti terorismu posiluje EU také svůj soubor externích nástrojů[32], a to plným využitím dialogů na vysoké úrovni o boji proti terorismu a sítě odborníků na boj proti terorismu / bezpečnost při delegacích EU, jakož i zapojením do mnohostranných fór, včetně spolupředsednictví Globálního fóra pro boj proti terorismu.

Obchod s drogami

Díky novému mandátu Agentury EU pro drogy, který bude platit od července 2024, bude EU lépe vybavena k řešení složitého bezpečnostního a zdravotního problému, který se týká milionů lidí v EU i na celém světě. Komise rovněž provádí revizi[33] nařízení o prekursorech drog[34], aby se vypořádala s hlavními výzvami zjištěnými v hodnocení tohoto nařízení z roku 2020[35], v němž byla zdůrazněna potřeba řešit problémy, které představují tzv. designer prekurzory[36], s cílem snížit nabídku nelegálních drog.

Vzhledem k bezprecedentnímu nárůstu množství nelegálních drog dostupných v Evropě je však třeba ve spolupráci s mezinárodními partnery zintenzivnit boj proti obchodu s drogami. K rozbití zločineckých sítí a lepší ochraně obětí trestné činnosti je zapotřebí dalších opatření ze strany členských států a EU. Komise dnes představuje plán EU pro boj proti obchodu s drogami a organizované trestné činnosti. Tento plán stanoví sedmnáct opatření ve čtyřech prioritních oblastech: posílení odolnosti logistických uzlů za pomoci evropské aliance přístavů, rozbití zločineckých sítí, zvýšení preventivního úsilí a posílení spolupráce s mezinárodními partnery. Tato opatření mají být provedena v letech 2024 a 2025.

Palné zbraně

Obchodování s palnými zbraněmi podporuje organizovanou trestnou činnost jak v EU, tak i v sousedních zemích. Odhaduje se, že až 35 milionů nedovolených palných zbraní se nachází v rukou civilistů v EU a přibližně 630 000 palných zbraní je v Schengenském informačním systému vedeno jako odcizené nebo ztracené. S rozvojem rychlého doručování balíků a nových technologií, jako je 3D tisk, nabývá nedovolené obchodování s palnými zbraněmi nových forem, které umožňují uniknout kontrolám. Riziko šíření palných zbraní zvýšila také ruská agresivní válka proti Ukrajině. Komise přijala v říjnu 2022 návrh na aktualizaci stávajících právních předpisů o dovozu, vývozu a tranzitu civilních palných zbraní s cílem odstranit mezery ve stávajících pravidlech, které mohou zvýšit počet zbraní, které se pašují a odklánějí do EU[37]. Ve střednědobém horizontu tato nová pravidla pomohou snížit riziko obcházení embarga v případě vývozu palných zbraní pro civilní použití a zvýšit kontroly dovozu tohoto druhu

[29] COM(2020) 606.
[30] COM(2020) 795.
[31] COM (2023) 641.
[32] Podle požadavku Strategického kompasu a závěrů Rady o „Řešení vnějšího rozměru neustále se vyvíjející teroristické a násilné extremistické hrozby se zaměřením na vnější rozměr“ přijatých v červnu 2022.
[33] Revize právních předpisů EU o prekursorech drog (europa.eu)
[34] Nařízení (ES) č. 273/2004 o prekursorech drog a nařízení Rady (ES) č. 111/2005, kterým se stanoví pravidla pro sledování obchodu s prekursory drog mezi Společenstvím a třetími zeměmi.
[35] COM(2020) 768.
[36] Opatření č. 23 protidrogového akčního plánu, COM(2020) 606.
[37] COM(2022) 480.

palných zbraní ze zemí mimo EU. Oba spolunormotvůrci musí k tomuto spisu ještě zaujmout svá stanoviska s cílem dosáhnout dohody o tomto spisu před koncem funkčního období Parlamentu.

Obchodování s lidmi

Obchodování s lidmi je obzvláště závažnou formou organizované trestné činnosti a hrubým porušením základních práv. Oběti jsou v rámci EU obchodovány zejména za účelem sexuálního a pracovního vykořisťování, ale také za účelem nuceného žebrání a páchání trestné činnosti a dalších forem vykořisťování. Komise v prosinci 2022 navrhla změnu směrnice o boji proti obchodování s lidmi[38] s aktualizovanými pravidly, která by řešila nedostatky stávajícího právního rámce. Po přijetí revidované směrnice by se do její působnosti zařadily zejména nucené sňatky a nezákonné adopce a uvedl by se v ní výslovný odkaz na problematiku obchodování s lidmi, které se odehrává online. Rovněž by zahrnovala povinný režim sankcí pro pachatele a formalizovala by zřízení národních referenčních mechanismů s cílem zlepšit včasnou identifikaci a přeshraniční poskytování pomoci a podpory obětem. Vědomé využívání služeb poskytovaných oběťmi obchodování s lidmi by se stalo trestným činem a vznikla by také povinnost každoročního sběru údajů o obchodování s lidmi, které by zveřejňoval Eurostat. Rada přijala obecný přístup v červnu 2023, zatímco Evropský parlament musí svůj postoj teprve přijmout. K dosažení dohody před koncem funkčního období tohoto Parlamentu bude zapotřebí jednat co nejrychleji.

Trestná činnost proti životnímu prostředí

Trestná činnost proti životnímu prostředí se stala celosvětovou hrozbou, která roste odhadem o 5 až 7 % ročně. Značné zisky, kterých lze dosáhnout, právní mezery mezi členskými státy a nízké riziko odhalení jsou pro organizovanou trestnou činnost velkým lákadlem. Podle Europolu existují náznaky, že výnosy z těchto činností jsou využívány k financování terorismu. Komise přijala v prosinci 2021 návrh na nahrazení směrnice o trestněprávní ochraně životního prostředí z roku 2008. Návrh se zaměřuje na zpřesnění a aktualizaci definic kategorií trestné činnosti proti životnímu prostředí a na vymezení účinných, odrazujících a přiměřených druhů a úrovní sankcí pro fyzické a právnické osoby. Nově se mezi trestné činy řadí trestné činy spojené s nezákonným odlesňováním, porušováním právních předpisů EU v oblasti chemických látek, nezákonným čerpáním povrchových nebo podzemních vod a nedovolenou recyklací lodí. Cílem návrhu je výrazně posílit řetězec prosazování práva a přeshraniční spolupráci mezi orgány členských států a agenturami a subjekty EU. Evropský parlament a Rada přijaly k návrhu své postoje a nyní probíhají jednání, která by měla být uzavřena do konce roku. Revidovaný akční plán EU[39] pro boj proti nezákonnému obchodu s volně žijícími a planě rostoucími druhy vyžaduje provedení s cílem dále posílit prevenci a prosazování práva.

Vymáhání a konfiskace majetku

Klíčem k potlačení organizované trestné činnosti je připravit zločince o jejich nezákonné zisky. Proto Komise kromě návrhu, který poskytuje donucovacím orgánům přístup k informacím o bankovních účtech v celé EU[40] (pro nějž byla dosažena politická dohoda v červnu 2023), předložila v květnu 2022 návrh směrnice o vymáhání a konfiskaci majetku[41] s cílem posílit možnosti vysledování, identifikace, zajišťování, konfiskace a správy majetku. Klíčová ustanovení návrhu se týkají požadavků na finanční šetření a dalších pravomocí a nástrojů úřadů

[38] COM(2022) 732.
[39] COM(2022) 581.
[40] COM(2021) 429.
[41] COM(2022) 245.

pro vyhledávání majetku z trestné činnosti, jakož i účinnějších opatření na zajišťování a konfiskaci majetku v případě rozšířeného okruhu trestných činů. Jedním z nových trestných činů, na které by se tato opatření vztahovala, je porušení omezujících opatření Unie. Komise v prosinci 2022 přijala samostatný návrh na harmonizaci trestněprávních definic a sankcí za porušení omezujících opatření Unie. Účinné provádění a prosazování omezujících opatření Unie zůstává pro Komisi hlavní prioritou, kterou posiluje práce pracovní skupiny „Freeze and Seize“, kterou Komise zřídila v reakci na ruskou útočnou válku proti Ukrajině. K oběma návrhům přijaly Evropský parlament a Rada své postoje s cílem dosáhnout dohody do konce tohoto roku.

Balíček opatření proti praní peněz

Téměř veškerá trestná činnost v EU, z níž plynou výnosy, je spjata s praním peněz[42], které tak představuje klíčový faktor v oblasti boje proti trestné činnosti v EU. Komise v červenci 2021 předložila ambiciózní návrhy na posílení opatření EU proti praní peněz a financování terorismu[43], které zahrnují čtyři legislativní návrhy na posílení prevence a odhalování pokusů pachatelů trestné činnosti o praní nezákonných výnosů nebo financování teroristické činnosti prostřednictvím finančního systému. Jednu ze čtyř iniciativ balíčku, která má zajistit sledovatelnost převodů kryptoaktiv, přijali spolunormotvůrci v květnu 2023[44]. Toto nařízení bude použitelné ode dne 30. prosince 2024. K tomuto datu budou muset všichni poskytovatelé služeb v oblasti kryptoaktiv shromažďovat a uchovávat informace o původci a příjemci převodů kryptoaktiv. Zbývající tři návrhy mají za cíl i) zřídit nový orgán EU pro boj proti praní peněz, který zajistí konzistentní a vysoce kvalitní dohled na celém vnitřním trhu, včetně nejrizikovějších přeshraničních subjektů, a podpoří a zkoordinuje práci finančních zpravodajských jednotek, ii) stanovit harmonizovaná pravidla pro soukromý sektor, včetně zavedení celoevropského limitu 10 000 EUR pro velké hotovostní platby výměnou za služby a zboží, a iii) posílit pravomoci a nástroje spolupráce příslušných orgánů. Očekává se, že tento balíček výrazně posílí schopnost EU bojovat proti praní peněz a chránit občany EU před terorismem a organizovanou trestnou činností. O třech zbývajících návrzích v současné době jednají spolunormotvůrci s cílem dosáhnout dohody o tomto spisu před koncem funkčního období Parlamentu.

Komise vyzývá Evropský parlament a Radu, aby urychleně, nejpozději však před koncem funkčního období současného Evropského parlamentu, dokončily interinstitucionální jednání o následujících neprojednaných spisech:

- návrh směrnice o vymáhání a konfiskaci majetku,
- návrh směrnice o harmonizaci trestněprávních definic a sankcí za porušení omezujících opatření Unie,
- návrh směrnice o boji proti obchodování s lidmi,
- návrh směrnice o zlepšení trestněprávní ochrany životního prostředí,
- návrh balíčku opatření proti praní peněz,
- návrh na aktualizaci stávajících právních předpisů o dovozu, vývozu a tranzitu civilních palných zbraní.

[42] Europol, Enterprising criminals – Europe’s fight against the global networks of financial and economic crime (Podnikaví zločinci – Evropa v boji proti globálním sítím finanční a hospodářské trestné činnosti), 2020.

[43] COM (2021) 420.

[44] Nařízení (EU) 2023/1113 ze dne 31. května 2023 o informacích doprovázejících převody peněžních prostředků a některých kryptoaktiv a o změně směrnice (EU) 2015/849.

Komise vyzývá členské státy, agentury a subjekty EU, aby:

- spolupracovaly na provádění 17 opatření plánu EU pro boj proti obchodu s drogami a organizované trestné činnosti v letech 2023 a 2024.

V. Silný evropský bezpečnostní ekosystém

Bezpečnostní hrozby mají v posledních letech čím dál více přeshraniční charakter, což vyžaduje další součinnost a užší spolupráci na všech úrovních. Od přijetí strategie bezpečnostní unie byly přijaty důležité iniciativy k maximalizaci přeshraniční spolupráce, zefektivnění a modernizaci dostupných nástrojů a postupů jak na vnějších hranicích, tak v rámci schengenského prostoru, jakož i k posílení výměny informací mezi donucovacími a justičními orgány s cílem lépe bojovat proti organizované trestné činnosti. V této souvislosti je účinné provádění rámce interoperability pro výměnu údajů důležitým pilířem pro zvýšení bezpečnosti a účinnou evropskou reakcí na přeshraniční hrozby při současném zajištění volného vnitřního pohybu.

Posílená výměna informací v rámci schengenského prostoru: předběžné informace o cestujících (API), jmenná evidence cestujících (PNR) a Prüm II

Dva návrhy týkající se API, které Komise přijala v prosinci 2022[45] , by posílily vnitřní bezpečnost Unie tím, že by donucovacím orgánům členských států poskytly další nástroje pro boj proti závažné trestné činnosti a terorismu. Zejména předběžné informace o cestujících na letech uvnitř EU, používané společně se jmennou evidencí cestujících v letecké dopravě, by umožnily donucovacím orgánům členských států výrazně zvýšit účinnost jejich vyšetřování pomocí cílenějších zásahů. Je důležité, aby byla navrhovaná pravidla přijata co nejdříve: podpořilo by to nejen boj proti organizované trestné činnosti a terorismu, ale také by se výrazně snížila potřeba systematických kontrol všech cestujících v případě dočasného znovuzavedení ochrany vnitřních hranic, což by usnadnilo cestování letadlem a volný pohyb. Evropská komise dne 6. září 2023 doporučila, aby Rada schválila jednání se Švýcarskem, Islandem a Norskem o dohodách o předávání údajů PNR. Přijetí těchto tří doporučení by podpořilo konzistentní a účinnou vnější politiku EU týkající se PNR.

Výměnu informací na základě rámce Prüm denně využívá policie v boji proti organizované trestné činnosti, drogám, terorismu, sexuálnímu vykořisťování a obchodování s lidmi. Návrh nařízení o automatizované výměně údajů pro policejní spolupráci („Prüm II“)[46] reviduje stávající rámec Prüm s cílem odstranit informační mezery a posílit prevenci, odhalování a vyšetřování trestných činů v EU. Revidovaná pravidla pro automatizovanou výměnu údajů v rámci policejní spolupráce doplňují návrhy týkající se policejní spolupráce v tomto mandátu společně s již přijatým doporučením Rady o posílení operativní přeshraniční spolupráce a směrnicí o výměně informací mezi donucovacími orgány. Urychlené přijetí a provedení těchto souvisejících nástrojů by zlepšilo, usnadnilo a urychlilo výměnu údajů mezi donucovacími orgány a pomohlo by identifikovat pachatele trestné činnosti.

Plně interoperabilní systém správy hranic pro zajištění bezpečného, silného, digitálního a jednotného schengenského prostoru

[45] COM(2022) 729, COM(2022) 73.
[46] COM(2021) 784.

Dobře fungující schengenský prostor bez vnitřních hranic je založen na vzájemné důvěře mezi členskými státy. Ta se zase opírá o účinnou ochranu, ať už na vnějších hranicích Unie, nebo jako alternativní opatření na území členských států. Pozměňovací návrh Komise k Schengenskému hraničnímu kodexu[47] stanoví, jak mohou členské státy lépe využívat alternativy k ochraně vnitřních hranic, které mohou nabídnout vysokou úroveň bezpečnosti. Je důležité, aby byla změna Schengenského hraničního kodexu přijata a provedena v plném rozsahu, což zajistí vysokou a přiměřenou úroveň bezpečnosti v schengenském prostoru. Pokračuje také vývoj nové architektury informačních systémů EU, která má lépe podporovat činnost vnitrostátních orgánů při zajišťování bezpečnosti a správy hranic. Tvoří ji obnovený Schengenský informační systém, Evropský systém pro cestovní informace a povolení, Systém vstupu/výstupu, aktualizace Vízového informačního systému a rámec interoperability pro propojení systémů při zajištění plné bezpečnosti. Po úplném dokončení by tato nová architektura poskytovala vnitrostátním orgánům komplexnější a spolehlivější bezpečnostní informace. Všechny složky rámce interoperability jsou zásadní, a proto zpoždění v jednom aspektu nebo v jednom členském státě způsobí zpoždění v zavádění u všech. Zpoždění v technickém vývoji systému vstupu/výstupu by měla být omezena na minimum, aby systém vstupu/výstupu mohl začít fungovat co nejdříve a aby mohly být zavedeny všechny klíčové prvky rámce interoperability.

Návrh nařízení o prověřování[48] by posílil bezpečnost v schengenském prostoru vytvořením jednotných pravidel týkajících se zjištění totožnosti státních příslušníků třetích zemí, kteří nesplňují podmínky vstupu podle Schengenského hraničního kodexu, a jejich podrobení zdravotním a bezpečnostním kontrolám na vnějších hranicích. Tyto cíle by podpořil i navrhovaný systém Eurodac, který by na základě prověření uváděl, které osoby by mohly představovat hrozbu pro vnitřní bezpečnost. To by následně usnadnilo provádění navrhovaného nařízení o řízení azylu a migrace. Komise vyzývá spolunormotvůrce, aby jednání o těchto spisech urychleně uzavřeli ještě před koncem stávajícího legislativního období.

Boj proti korupci

Korupce velmi škodí našim demokraciím, hospodářství a bezpečnosti, neboť napomáhá organizované trestné činnosti a nepřátelskému zahraničnímu vměšování. Úspěšná prevence a boj proti korupci jsou nezbytné jak pro ochranu hodnot EU a účinnost politik EU, tak pro zachování zásad právního státu a důvěry v ty, kdo vládnou, a veřejné instituce. Jak oznámila předsedkyně von der Leyenová v projevu o stavu Unie v roce 2022, Komise přijala dne 3. května 2023 balíček protikorupčních opatření[49]**.** Návrh směrnice o boji proti korupci, který Komise předložila, zahrnuje zpřísněná pravidla pro trestnost činů spojených s korupcí a harmonizaci trestů v celé EU. Umožňuje také účinné vyšetřování a stíhání a klade velký důraz na prevenci a vytváření kultury integrity, v níž se korupce netoleruje. Projednávání tohoto návrhu v Evropském parlamentu a Radě již bylo zahájeno. Kromě toho se členské státy vyzývají, aby provedly doporučení vyplývající z protikorupčního pilíře zprávy o právním státu 2023, která byla přijata dne 5. července 2023. Návrh vysokého představitele, který podpořila Komise, rovněž navrhuje zavést zvláštní režim sankcí v rámci společné zahraniční a bezpečnostní politiky (SZBP), který by se zaměřil na závažné korupční jednání na celém světě.

Posilování práv obětí

[47] COM(2021) 891.
[48] COM(2020) 612.
[49] COM(2023) 234.

Komise dne 12. července 2023 navrhla změny směrnice o právech obětí s cílem posílit přístup obětí k informacím, podpoře a ochraně, jejich účast v trestním řízení a přístup k odškodnění. Jedním z obecných cílů revize je přispět k vysoké úrovni bezpečnosti vytvořením bezpečnějšího prostředí pro oběti, které by podpořilo oznamování trestných činů a snížilo obavy z odvetných opatření.

Komise vyzývá Evropský parlament a Radu, aby urychleně, nejpozději však před koncem funkčního období současného Evropského parlamentu, dokončily interinstitucionální jednání o následujících neprojednaných spisech:

- návrh nařízení Prüm II,
- návrhy týkající se předběžných informací o cestujících (API),
- návrhy týkající se boje proti korupci a zejména zavedení zvláštního režimu sankcí v rámci společné zahraniční a bezpečnostní politiky (SZBP),
- návrh na změnu nařízení o Schengenském hraničním kodexu,
- návrh směrnice o právech obětí,
- návrh nařízení o prověřování.

Komise členské státy vyzývá, aby:

- zajistily co nejrychlejší vstup systému vstupu/výstupu v platnost s cílem dokončit provádění architektury EU pro výměnu informací.

VI. Provádění

Zajištění bezpečnosti Evropy jako celku je společnou odpovědností, na níž se musí podílet každý aktér, od Komise a spolunormotvůrců, jež přijímají nová, pevná, komplexní a praktická pravidla, přes členské státy, jež tato pravidla včasně provádějí, uplatňují a používají, až po různé orgány, organizace a zúčastněné strany, které provádějí operativní činnost v terénu. Klíčovou roli hrají také agentury EU v oblasti spravedlnosti, vnitřních věcí a kybernetické bezpečnosti, jejichž pravomoci se v poslední době rozšířily.

Posílené prověřování příjemců finančních prostředků EU

Při plnění rozpočtu EU má Komise povinnost zajistit, aby příjemci finančních prostředků EU dodržovali hodnoty EU. Mechanismy a kontrolní systémy, které určují, kdo může využívat finanční prostředky EU, jsou již nyní robustní a probíhající jednání o přepracovaném znění finančního nařízení se rovněž snaží poskytnout Komisi silnější právní prostředky, aby mohla v případě potřeby jednat. Kromě toho Komise v současné době pracuje na způsobech, jak dále posílit prověřování současných a potenciálních budoucích příjemců finančních prostředků EU, a to lepším vymezením povinností týkajících se dodržování hodnot EU a důsledků, které by měly následovat v případě jejich porušení. Tento krok vyjasní povinnosti příjemců i osob provádějících kontroly na úrovni EU a může sloužit jako zdroj inspirace pro vnitrostátní úroveň. V případě porušení podmínek financování Komise bez váhání zastaví spolupráci s příjemci dotčeného projektu a v případě potřeby bude finanční prostředky vymáhat zpět. Pokud si členské státy povšimnou možných rizik týkajících se organizací, které žádají o finanční prostředky EU, je důležité, aby aktivně sdílely informace s Komisí.

Porušení předpisů

Komise provedla v oblasti bezpečnosti řadu řízení o porušení právních předpisů. Například v roce 2023 bylo zahájeno velké množství řízení o porušení právních předpisů z důvodu neplnění

povinností podle nařízení z roku 2021 o šíření teroristického obsahu online (16 členských států)[50] a v průběhu let 2022 a 2023 obdrželo 20 členských států další výzvy k odstranění nedostatků z důvodu nesprávného provádění směrnice z roku 2011 o boji proti pohlavnímu zneužívání dětí[51]. Stále je otevřen značný počet případů porušení právních předpisů z důvodu nesouladu vnitrostátních právních předpisů se směrnicí z roku 2017 o boji proti terorismu[52] a z důvodu neprovedení pravidel, která usnadňují využívání finančních a jiných informací pro prevenci, odhalování, vyšetřování nebo stíhání některých trestných činů[53]. Mezi další oblasti, v nichž probíhají řízení pro porušení právních předpisů, patří právní předpisy o střelných zbraních, pravidla týkající se psychoaktivních látek používaných v drogách, boj proti podvodům a padělání bezhotovostních platebních prostředků, boj proti praní peněz, výměna informací z rejstříku trestů mezi členskými státy EU a směrnice o právech obětí. Členským státům, které provádějí dohodnuté iniciativy a opatření, byla poskytnuta podpora (technická a finanční) a Komise je i nadále připravena spolupracovat s členskými státy na optimalizaci provádění.

Monitorování v rámci schengenského hodnocení a jeho nový systém řízení

Schengenský hodnotící a monitorovací mechanismus nadále přispíval k účinnému provádění schengenských pravidel zaměřených na posílení bezpečnosti v prostoru bez vnitřních kontrol. V roce 2023 byla provedena první hodnocení v rámci posíleného schengenského hodnotícího a monitorovacího mechanismu, která umožnila včasnou identifikaci a nápravu strategických slabin, jež mají přeshraniční dopad na bezpečnost a ochranu v rámci EU. Kromě toho Komise v roce 2023 zahájila tematické schengenské hodnocení s cílem posoudit postupy členských států, které v boji proti pašování drog do EU čelí podobným výzvám, zejména se zaměřením na pašování drog ve velkých objemech. Toto hodnocení vtisklo bezpečnostním prvkům Schengenu posílený a komplexnější ráz. Na základě výsledků pravidelných, tematických a neohlášených schengenských hodnocení stanovila Rada v červnu 2023 priority schengenského cyklu pro období 2023–2024. Stanovuje oblasti, na které je třeba se zaměřit a které vyžadují další impuls k dosažení bezpečnějšího a silnějšího schengenského prostoru. Účinné a rychlé provádění těchto priorit spolu se zvýšenou koordinací politik schengenské rady dále posílí boj proti organizované trestné činnosti a maximalizuje přeshraniční operativní spolupráci.

Úloha agentur a subjektů EU

Klíčovým faktorem pro provádění iniciativ bezpečnostní unie je partnerství, neboť k dosažení konkrétních výsledků je zapotřebí spolupráce různých vnitrostátních a evropských orgánů a subjektů. Například platforma EMPACT (evropská multidisciplinární platforma pro boj proti hrozbám vyplývajícím z trestné činnosti) umožňuje členským státům uskutečňovat strukturovanou multidisciplinární spolupráci, kterou podporují všechny orgány, instituce a agentury EU (např. Europol, Frontex, Eurojust, CEPOL, OLAF, EU-LISA). Operace prováděné v rámci platformy EMPACT, včetně operací prováděných prostřednictvím specializovaných operativních pracovních skupin, koordinují úsilí členských států a operativních partnerů v boji proti zločineckým sítím a závažné trestné činnosti. Jen v roce 2022 bylo zásluhou platformy EMPACT zatčeno celkem 9922 osob, zabaven majetek a peníze v hodnotě více než 180 milionů EUR, zahájeno 9263 vyšetřování, identifikováno 4019 obětí, zabaveno více než 62 tun drog,

[50] Nařízení (EU) 2021/784 o šíření teroristického obsahu online.

[51] Směrnice (EU) 2011/93 o boji proti pohlavnímu zneužívání dětí.

[52] Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV.

[53] Směrnice Evropského parlamentu a Rady (EU) 2019/1153 ze dne 20. června 2019 o stanovení pravidel usnadňujících používání finančních a dalších informací k prevenci, odhalování, vyšetřování či stíhání určitých trestných činů a o zrušení rozhodnutí Rady 2000/642/SVV.

identifikováno 51 cílů vysoké důležitosti (High Value Targets – HVT) a zatčeno 12 osob, operace v souvislosti s útočnou válkou proti Ukrajině, zejména v rámci boje proti obchodování s lidmi a hrozbám souvisejícím se střelnými zbraněmi.

Agentura Frontex, Evropská agentura pro námořní bezpečnost (EMSA) a Evropská agentura pro kontrolu rybolovu (EFCA) nadále posilují spolupráci v oblasti pobřežní stráže s cílem podpořit vnitrostátní orgány při zvyšování bezpečnosti a ochrany na moři. Tyto agentury se budou významně podílet na provádění strategie EU pro námořní bezpečnost.

Několik iniciativ bezpečnostní unie přineslo příslušným agenturám nové povinnosti a úkoly, které měly v některých případech dopad na lidské zdroje.

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA)

Pokud jde o připravenost a reakci na kybernetické incidenty, Komise zřídila krátkodobé opatření na podporu členských států a převedla finanční prostředky z programu Digitální Evropa **Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA)** s cílem posílit připravenost a schopnost reakce na závažné kybernetické incidenty. Návrh aktu o kybernetické solidaritě přijatý v dubnu 2023 na toto opatření navazuje a po přijetí spolunormotvůrci může být agentura ENISA pověřena dalšími úkoly, jako je provoz a správa budoucí rezervy Unie pro kybernetickou bezpečnost nebo příprava zprávy o přezkumu incidentů po rozsáhlých kybernetických bezpečnostních incidentech. Navrhovaný zákon o kybernetické odolnosti by agentuře ENISA uložil povinnost přijímat od výrobců oznámení o zranitelnostech produktů s digitálními prvky a o incidentech, které mají dopad na bezpečnost těchto výrobků, a agentura ENISA by je měla předávat příslušným skupinám pro reakci na počítačové bezpečnostní incidenty (CSIRT) nebo příslušným jednotným kontaktním místům členských států. Agentura ENISA má také každé dva roky vypracovat technickou zprávu o nových trendech týkajících se kybernetických bezpečnostních rizik u výrobků s digitálními prvky a předložit ji skupině pro spolupráci v oblasti bezpečnosti sítí a informací.

Evropské centrum kompetencí pro kybernetickou bezpečnost

Evropské centrum kompetencí pro kybernetickou bezpečnost (ECCC) je spolu se sítí národních koordinačních center novým orgánem Unie na podporu inovací a průmyslové politiky v oblasti kybernetické bezpečnosti. Tento ekosystém posílí kapacity technologické komunity v oblasti kybernetické bezpečnosti, udrží excelenci výzkumu a posílí konkurenceschopnost průmyslu Unie v této oblasti. Centrum ECCC a síť národních koordinačních center budou přijímat strategická investiční rozhodnutí a sdružovat zdroje Unie, jejích členských států a nepřímo i průmyslu s cílem zlepšit a posílit technologické a průmyslové kapacity v oblasti kybernetické bezpečnosti. Centrum ECCC má proto hrát klíčovou úlohu při plnění ambiciózních cílů v oblasti kybernetické bezpečnosti stanovených v programech Digitální Evropa a Horizont Evropa.

Centrum ECCC již přijalo do pracovního poměru více než polovinu svých zaměstnanců a brzy obsadí i pozici výkonného ředitele. Práce, které již probíhají, zahrnují část programu Digitální Evropa týkající se kybernetické bezpečnosti a nový strategický program[54] pro vývoj a zavádění technologií, který stanoví prioritní opatření na podporu malých a středních podniků při vývoji a využívání strategických technologií, služeb a procesů v oblasti kybernetické bezpečnosti, na podporu a rozvoj odborné pracovní síly a na posílení odborných znalostí v oblasti výzkumu, vývoje a inovací v širším evropském ekosystému kybernetické bezpečnosti.

Europol

Díky zcela novému mandátu bude **Europol** lépe vybaven k podpoře členských států v boji proti organizované trestné činnosti. Vzhledem k rostoucímu významu obchodu s drogami a jeho rostoucímu negativnímu dopadu na bezpečnost občanů EU je boj proti němu jednou z hlavních priorit. Na základě pověření Rady Evropské unie ze dne 15. května 2023 Komise aktivně pracuje na uzavření mezinárodních dohod s Bolívií, Brazílií, Ekvádorem, Mexikem a Peru o výměně osobních údajů s Europolem s cílem předcházet závažné trestné činnosti a terorismu a bojovat proti nim.

Eurojust

Díky více než dvacetiletým zkušenostem s poskytováním justiční podpory vnitrostátním orgánům v boji proti široké škále závažných a složitých přeshraničních trestných činů si **Eurojust** upevnil své postavení v prostoru svobody, bezpečnosti a práva EU. V zájmu posílení všeobecné spolupráce Komise sjednává mezinárodní dohody, které usnadní spolupráci mezi Eurojustem a třinácti třetími zeměmi při výměně osobních údajů v boji proti organizované trestné činnosti a terorismu[55]. Jednání již byla dokončena s Arménií a Libanonem, nyní probíhají s Alžírskem a Kolumbií a byla zahájena s Bosnou a Hercegovinou. Komise vybízí Evropský parlament a Radu, aby dokončily uzavírání dohod s těmito zeměmi do konce volebního období, a posílily tak přeshraniční justiční spolupráci a rozšířily boj proti přeshraniční trestné činnosti.

EPPO

Od zahájení své operativní činnosti v červnu 2021 se **Úřad evropského veřejného žalobce (EPPO)** osvědčil jako mocný nástroj v unijním souboru nástrojů pro vyšetřování a stíhání trestných činů poškozujících rozpočet Unie, včetně trestných činů souvisejících s účastí na zločinném spolčení, jedná-li se o trestné činy poškozující rozpočet Unie. Komise vyzývá členské státy, které se dosud neúčastní posílené spolupráce v rámci EPPO, aby tak učinily co nejdříve, a využily tak plného potenciálu EPPO při ochraně peněz daňových poplatníků EU.

EUDA

Díky novému mandátu, který spolunormotvůrci přijali v červnu 2023, se stávající Evropské monitorovací centrum pro drogy a drogovou závislost (EMCDDA) promění v plnohodnotnou agenturu, a to v **Agenturu Evropské unie pro drogy**, která bude mít posílenou úlohu. Agentura bude moci komplexněji posuzovat nové zdravotní a bezpečnostní výzvy, které představují nelegální drogy, a účinněji přispívat k práci na úrovni jednotlivých členských států i na mezinárodní úrovni. Hlavním úkolem agentury bude i nadále shromažďování, analýza a šíření údajů, ale posílený mandát jí také umožní rozvíjet obecné schopnosti posouzení hrozeb v oblasti zdraví a bezpečnosti s cílem identifikovat nově vznikající hrozby, včetně polyvalentního

[54] https://cybersecurity-centre.europa.eu/strategic-agenda_en

[55] Alžírsko, Argentina, Arménie, Bosna a Hercegovina, Brazílie, Egypt, Izrael, Jordánsko, Kolumbie, Libanon, Maroko, Tunisko a Turecko.

užívání, posílit spolupráci prostřednictvím vnitrostátních kontaktních míst a vytvořit síť laboratoří, které budou agentuře poskytovat forenzní a toxikologické údaje. To agentuře pomůže vydávat výstrahy, když se na trhu objeví obzvláště nebezpečné látky, a zvyšovat povědomí o nich.

Komise vyzývá Evropský parlament a Radu, aby urychleně, nejpozději však před koncem funkčního období současného Evropského parlamentu, dokončily interinstitucionální jednání o následujících neprojednaných spisech:

- Návrh na přepracování finančního nařízení.

Komise členské státy vyzývá, aby:

- aktivně sdílely informace s Komisí, pokud si jsou vědomy možných rizik týkajících se organizací, které žádají o finanční prostředky EU,
- urychleně provedly priority schengenského cyklu pro období 2023–2024 k dosažení bezpečnějšího a silnějšího schengenského prostoru,
- se zabývaly řízeními o porušení právních předpisů, která jsou proti nim vedena, s cílem zajistit řádné provedení příslušných právních předpisů.

VII. Závěr

Poslední tři roky se nesly ve znamení soustavného a odhodlaného úsilí o oživení ambice vytvořit bezpečnostní unii pro EU. V celém spektru bezpečnostní politiky bylo dosaženo obrovského pokroku. Realita neustále se vyvíjejících hrozeb nyní vyžaduje nepřetržité úsilí s novou motivací. Práce na legislativním rámci musí být ukončeny včas, tedy ještě před koncem volebního období Evropského parlamentu na jaře 2024. Členské státy nesou soustavnou odpovědnost za provádění, uplatňování a používání nových právních předpisů. Provádění vyžaduje společné úsilí, včetně podpory agentur EU, a velmi často také stále silnější spolupráci s našimi mezinárodními partnery.

Pouze společným a odhodlaným úsilím všech zúčastněných stran dosáhneme úrovně bezpečnosti v EU, kterou občané očekávají – a v dnešní situaci by mělo být prioritou každého aktéra, aby se na posílení bezpečnosti EU podílel.