Rada
Evropské unie

Brusel 30. července 2020
(OR. en)

10010/20

JAI 624	**DROIPEN 61**
COSI 121	**COPEN 215**
ENFOPOL 190	**FREMP 51**
ENFOCUSTOM 95	**JAIEX 72**
IXIM 79	**CFSP/PESC 644**
CT 61	**COPS 256**
CRIMORG 66	**HYBRID 20**
FRONT 207	**DISINFO 16**
ASIM 55	**TELECOM 121**
VISA 84	**DIGIT 63**
CYBER 140	**COMPET 347**
DATAPROTECT 71	**RECH 286**
CATS 56	

PRŮVODNÍ POZNÁMKA

Odesílatel:	Jordi AYET PUIGARNAU, ředitel, za generální tajemnici Evropské komise
Datum přijetí:	27. července 2020
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	COM(2020) 605 final
Předmět:	SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, EVROPSKÉ RADĚ, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ o strategii bezpečnostní unie EU

Delegace naleznou v příloze dokument COM(2020) 605 final.

Příloha: COM(2020) 605 final

EVROPSKÁ
KOMISE

V Bruselu dne 24.7.2020
COM(2020) 605 final

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

o strategii bezpečnostní unie EU

I. Úvod

V politických směrech Komise bylo jasně řečeno, že k ochraně našich občanů musíme použít všech možných prostředků. Celková bezpečnost je nejen základem pro bezpečnost osobní, ale přispívá také k ochraně základních práv a je zdrojem důvěry a dynamiky v našem hospodářství, společnosti a demokracii. Evropané se dnes potýkají s nestabilní bezpečnostní situací, kterou ovlivňují vyvíjející se hrozby i další faktory, jako je změna klimatu, demografické trendy a politická nestabilita za našimi hranicemi. Globalizace, volný pohyb a digitální transformace nadále přinášejí prosperitu, zjednodušují každodenní život a podněcují inovace a růst, jejich přínos je však nutně vyvážen riziky a náklady. Mohou být zneužity k terorismu, organizovanému zločinu či obchodu s drogami a s lidmi, které přímo ohrožují občany a evropský způsob života. Kybernetické útoky a kyberkriminalita obecně nadále rostou. Bezpečnostní hrozby se rovněž stávají komplexnějšími: těží z možnosti působit přes hranice, pomáhá jim vzájemné propojení a stírání hranic mezi fyzickým a digitálním světem, a využívají také zranitelných skupin a sociálních a hospodářských rozdílů. K útokům může docházet znenadání, stopa, kterou zanechají, může být malá či vůbec žádná, státní i nestátní aktéři mohou použít různé hybridní hrozby[1] a situace mimo EU může zásadně ovlivnit bezpečnost uvnitř EU.

Krize vyvolaná onemocněním COVID-19 rovněž změnila naše chápání bezpečnosti, bezpečnostních hrozeb a příslušných politik. Zdůraznila také potřebu zajistit bezpečnost ve fyzickém i v digitálním prostředí a podtrhla význam otevřené strategické autonomie pro naše dodavatelské řetězce z hlediska kritických produktů, služeb, infrastruktury a technologií. Dále ukázala, že je nutné, aby všichni lidé v každém sektoru společně pracovali v první řadě na zlepšení připravenosti a odolnosti EU a na tom, aby měla k dispozici lepší nástroje pro reakci v případě potřeby.

Občany nemohou chránit pouze členské státy jednající samostatně. Nikdy nebylo zásadnější využít našich silných stránek v zájmu spolupráce a EU nikdy neměla větší potenciál k dosažení změny. Evropská unie může jít příkladem tím, že zlepší svůj celkový systém řízení krizí a uvnitř i vně svých hranic bude pracovat na zlepšení celosvětové stability. Primární odpovědnost za bezpečnost sice nesou členské státy, nicméně v posledních letech je stále jasnější, že bezpečnost jednoho členského státu je vázána na bezpečnost všech. EU může reagovat multidisciplinárním a integrovaným způsobem a pomáhat bezpečnostním aktérům v členských státech s nástroji a informacemi, které potřebují[2].

Aby měla politická opatření ten správný důvěryhodný základ, může EU rovněž zaručit, že bezpečnostní politika zůstane zakotvena ve společných evropských hodnotách, kterými je dodržování a prosazování zásad právního státu, rovnost[3], základní práva, zaručení transparentnosti, odpovědnost a demokratická kontrola. Může vybudovat účinnou a skutečnou bezpečnostní unii, v níž budou práva a svobody jednotlivců řádně chráněny. Bezpečnost a dodržování základních práv nejsou cíle protichůdné, ale naopak konzistentní, které se vzájemně doplňují. Naše hodnoty a základní práva proto musí být základem

[1] Definice hybridních hrozeb se liší, jejich podstatou však je vystihnout soubor různých nátlakových a podvratných činností a konvenčních i nekonvenčních metod (např. diplomatických, vojenských, ekonomických a technologických), které mohou různí státní i nestátní aktéři koordinovaným způsobem využívat k tomu, aby dosáhli konkrétních cílů, aniž by formálně vyhlásili válku. Viz JOIN(2016) 18 final.

[2] Například prostřednictvím služeb poskytovaných v rámci kosmického programu EU, jako je Copernicus, který nabízí data z pozorování Země a aplikace pro ostrahu hranic, námořní bezpečnost, prosazování práva, boj proti pirátství a proti pašování drog, jakož i pro řešení mimořádných událostí.

[3] Unie rovnosti: Strategie pro rovnost žen a mužů na období 2020–2025, COM(2020) 152.

bezpečnostních politik, přičemž je nutné dodržovat zásadu nezbytnosti, proporcionality a zákonnosti a mít vhodné záruky pro odpovědnost a soudní nápravu. Zároveň je potřeba umožnit účinnou odezvu v zájmu ochrany jednotlivců, zejména těch nejzranitelnějších.

Významné právní, praktické a podpůrné nástroje již existují, musí však být posíleny i lépe používány. Značného pokroku bylo dosaženo ve zlepšení výměny informací a zpravodajské spolupráce s členskými státy a také v zúžení prostoru, v němž teroristé a pachatelé trestné činnosti operují. Roztříštěnost však trvá.

Je také nutné působit i za hranicemi EU, protože ochrana Unie a jejích občanů již není pouze otázkou zajištění bezpečnosti uvnitř unijních hranic, ale také řešení vnějšího rozměru bezpečnosti. Zásadním prvkem v úsilí EU o zvýšení bezpečnosti uvnitř Unie je proto přístup k vnější bezpečnosti v rámci společné zahraniční a bezpečnostní politiky (SZBP) a společné bezpečnostní a obranné politiky (SBOP). Pro účinnou a komplexní reakci má ústřední význam spolupráce při řešení společných problémů s třetími zeměmi a na globální úrovni, přičemž pro vlastní bezpečnost EU je rozhodující stabilita a bezpečnost v jejím sousedství.

Tato nová strategie, která staví na předchozí činnosti Evropského parlamentu[4], Rady[5] a Komise[6], ukazuje, že skutečná a účinná bezpečnostní unie musí kombinovat silnou základní složku nástrojů a politik pro zajištění bezpečnosti v praxi s vědomím, že bezpečnost má důsledky pro všechny složky společnosti a pro všechny veřejné politiky. EU musí zajistit bezpečné prostředí pro každého bez ohledu na jeho rasový či etnický původ, náboženství, přesvědčení, pohlaví, věk nebo sexuální orientaci.

Tato strategie se týká období 2020–2025 a zaměřuje se na budování schopností a kapacit s cílem vytvořit takové bezpečnostní prostředí, které obstojí i v budoucnu. Vymezuje celospolečenský přístup k bezpečnosti, který dokáže koordinovaným způsobem účinně reagovat na rychle se měnící prostředí hrozeb. Definuje též strategické priority a odpovídající opatření pro integrované řešení digitálních a fyzických rizik v celém ekosystému bezpečnostní unie se zaměřením na oblasti, kde může mít EU přidanou hodnotu. Jejím cílem je skutečný přínos z hlediska bezpečnosti s cílem chránit každého v EU.

II. Rychle se měnící podoba bezpečnostních hrozeb v Evropě

Bezpečnost, prosperita a dobré životní podmínky občanů závisí na tom, zda žijí v bezpečí. Narušení této jistoty závisí na tom, jak moc jsou jejich životy a živobytí zranitelné, přičemž čím větší je zranitelnost, tím větší je riziko, že ji lze zneužít. Zranitelná místa i hrozby se neustále vyvíjejí, čemuž se EU musí přizpůsobit.

V každodenním životě závisíme na nejrůznějších službách, jako je energetika, doprava, finance či zdravotnictví. Tyto služby využívají fyzickou a digitální infrastrukturu, což zvyšuje jejich zranitelnost i potenciál narušení. V průběhu pandemie COVID-19 udržely nové technologie mnoho podniků a veřejných služeb v chodu, ať už zajištěním připojení při práci na dálku nebo zachováním logistiky dodavatelských řetězců. Tato situace však také

[4] Například činnost výboru Evropského parlamentu proti terorismu (TERR), který vydal zprávu v listopadu 2018.

[5] Od závěrů Rady z června 2015 o „obnovené strategii vnitřní bezpečnosti“ až po nedávné výsledky zasedání Rady z prosince 2019.

[6] Sdělení Naplňování Evropského programu pro bezpečnost v zájmu boje proti terorismu a položení základů účinné a skutečné bezpečnostní unie, COM(2016) 230 final ze dne 20. dubna 2016. Viz nejnovější hodnocení provádění právních předpisů v oblasti vnitřní bezpečnosti: Provádění právních předpisů v oblasti vnitřní bezpečnosti v období 2017–2020, SWD(2020) 135.

otevřela cestu mimořádnému nárůstu zlovolných útoků s cílem zneužít problémů vyvolaných pandemií a přechodem na online práci z domova k trestné činnosti[7]. Nedostatek určitého zboží vytvořil nový prostor pro organizovanou trestnou činnost. Následky mohly být fatální, například v podobě narušení základních zdravotních služeb v době nejintenzivnějšího tlaku.

Kybernetická bezpečnost technologií se stala otázku strategického významu i kvůli stále rozmanitějším cestám, jak digitální technologie zjednodušují náš život.[8] Kybernetické útoky páchají velké škody v domácnostech, bankách, finančních službách i v podnicích (zejména malých a středních). Případná škoda je ještě více znásobena vzájemnou závislostí fyzických a digitálních systémů: každý fyzický problém nutně zasáhne digitální systémy, a naopak kybernetické útoky na informační systémy a digitální infrastruktury mohou vést ke kolapsu základních služeb[9]. Vzestup internetu věcí a intenzivnější využívání umělé inteligence tak přinesou vedle nových výhod i nová nejrůznější rizika.

Náš svět stojí na digitální infrastruktuře, technologiích a online systémech, které nám umožňují podnikat, nakupovat výrobky a využívat služeb. Komunikaci a interakci potřebují naprosto všichni a tato závislost na internetu otevřela prostor vlně **kyberkriminality**[10]. Kybernetické trestné činy jako služba na objednávku a stínová ekonomika zaměřená na kybernetickou kriminalitu dávají snadný přístup ke kyberkriminálním produktům a službám na internetu. Zločinci se rychle přizpůsobují a nové technologie využívají k vlastním účelům. Například nepravé a padělané léčivé přípravky pronikly do legálního dodavatelského řetězce farmaceutických přípravků[11]. Exponenciální růst dětské pornografie na internetu[12] dokládá sociální důsledky měnících se forem trestné činnosti. Podle nedávného průzkumu většinu lidí v EU (55 %) znepokojuje, že by kriminální živly a podvodníci mohli mít přístup k jejich údajům[13].

Globální prostředí tyto hrozby rovněž zhoršuje. Asertivní průmyslová politika třetích zemí v kombinaci s nepřetržitými krádežemi duševního vlastnictví, které jsou prováděny kybernetickými prostředky, mění strategické paradigma, pokud jde o ochranu a prosazování evropských zájmů. Tuto změnu ještě umocňuje nárůst aplikací s dvojím užitím, a proto má silné odvětví civilní techniky velký přínos pro obranné a bezpečnostní kapacity. Významný dopad na hospodářství, zaměstnanost a růst v EU má průmyslová špionáž: kybernetické krádeže obchodního tajemství stojí Evropskou unii odhadem 60 miliard EUR[14]. Tato situace

---

7 Europol: *Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU* (Jak bude COVID-19 utvářet podobu závažné a organizované trestné činnosti v EU), duben 2020.

8 Doporučení Komise o kybernetické bezpečnosti sítí 5G, C(2019) 2335, sdělení Bezpečné zavádění sítí 5G v EU – Implementace souboru opatření EU, COM(2020) 50.

9 V březnu 2020 se Fakultní nemocnice Brno stala terčem kybernetického útoku, kvůli němuž byla nucena přesunout pacienty do jiných zařízení a odložit chirurgické výkony (Europol: *Pandemic Profiteering. How criminals exploit the COVID-19 crisis*). Umělá inteligence může být zneužívána pro digitální, politické a fyzické útoky i ke sledování. Sběr dat v rámci internetu věcí může být využíván ke sledování lidí (inteligentní hodinky, virtuální asistenti atd.).

10 Podle některých prognóz dosáhnou do roku 2024 škody v důsledku porušení ochrany údajů 5 bilionů USD ročně, oproti 3 bilionům USD v roce 2015 (Juniper Research, *The Future of Cybercrime & Security*).

11 Jedna studie z roku 2016 (Legiscript) odhadla, že na celém světě působí legálně pouze 4 % internetových lékáren, přičemž spotřebitelé z EU jsou hlavním cílem 30 000 až 35 000 nelegálních internetových lékáren.

12 Strategie EU pro účinnější boj proti pohlavnímu zneužívání dětí, COM(2020) 607.

13 Agentura Evropské unie pro základní práva (2020), *Your rights matter*: *Security concerns and experiences* (Vaše práva jsou důležitá: bezpečnostní obavy a zkušenosti), průzkum základních práv, Lucemburk, Úřad pro publikace.

14 *The scale and impact of industrial espionage and theft of trade secrets through cyber* (Rozsah průmyslové špionáže a krádeže obchodních tajemství v kyberprostoru a jejich dopad), 2018.

vyžaduje důkladně posoudit, jak závislost různého druhu a zvýšená expozice kybernetickým hrozbám ovlivňují schopnost EU chránit fyzické osoby i podniky.

Krize způsobená onemocněním COVID-19 rovněž zdůraznila, jak sociální rozdíly a nejistoty zvyšují bezpečnostní zranitelnost. Zvyšuje se tak potenciál důmyslnějších a **hybridních útoků** ze strany státních i nestátních aktérů a slabiny jsou zneužívány formou různých kybernetických útoků, poškozování kritické infrastruktury[15], dezinformačních kampaní a radikalizace politického diskursu.[16]

Zároveň se nepřetržitě vyvíjejí dlouhodobé hrozby. V roce 2019 došlo k poklesu **teroristických útoků**, hrozba džihádistických útoků na občany EU ze strany Dá'iš, al-Káidy a jejich odnoží je však stále vysoká.[17] Zároveň roste i hrozba násilného pravicového extremismu.[18] Vážné znepokojení musí vzbuzovat útoky motivované rasistickou ideologií: vražedné antisemitské teroristické útoky v Halle připomněly, že je nutno posílit reakci v souladu s prohlášením Rady z roku 2018[19]. Pětina osob v EU se značně obává teroristického útoku v následujících dvanácti měsících.[20] U naprosté většiny teroristických útoků v poslední době se jednalo o technologicky nenáročné útoky spáchané samostatně jednajícími aktéry, kteří útočili na osoby ve veřejném prostoru. Teroristická propaganda na internetu získala novou dimenzi v souvislosti s živým vysíláním útoků ve městě Christchurch[21]. Radikalizované osoby stále představují vysokou hrozbu, kterou mohou ještě zhoršit navracející se zahraniční terorističtí bojovníci a extremisté propuštění z vězení.[22]

Krize rovněž ukázala, jak se mohou stávající hrozby vyvíjet za nových okolností. Skupiny **organizované trestné činnosti** zneužívají nedostatku zboží k vytváření nových nezákonných trhů. Obchod s nedovolenými drogami zůstává největším kriminálním trhem v EU, kde se jeho minimální maloobchodní hodnota odhaduje na 30 miliard EUR ročně[23]. Neustále probíhá obchodování s lidmi: podle odhadů činí celkový roční zisk ze všech forem vykořisťování téměř 30 miliard EUR[24]. Mezinárodní obchod s padělanými léčivými přípravky dosáhl 38,9 miliardy EUR[25]. Nízká míra konfiskování zároveň umožňuje

---

15 Kritické infrastruktury jsou zásadní pro zachování nejdůležitějších společenských funkcí, zdraví, bezpečnosti, zabezpečení a dobrých hospodářských či sociálních podmínek, jejichž narušení nebo zničení má závažný dopad (směrnice Rady 2008/114/ES).

16 Na 97 % občanů EU se setkává s falešnými zprávami, 38 % denně. Viz JOIN(2020) 8 final.

17 Třináct členských států EU nahlásilo celkem 119 dokonaných, neúspěšných a zmařených teroristických útoků, při nichž zahynulo deset osob a 27 bylo zraněno (zpráva Europolu o stavu a vývoji terorismu v Evropské unii, 2020).

18 V roce 2019 bylo ve třech členských státech spácháno šest pravicových teroristických útoků (jeden dokonaný, jeden neúspěšný, čtyři zmařené). Naproti tomu v roce 2018 to byl pouze jeden útok, k dalším úmrtím došlo v případech, které nebyly klasifikovány jako terorismus (Europol, 2020).

19 Viz rovněž prohlášení Rady k boji proti antisemitismu a rozvoji společného bezpečnostního přístupu v zájmu lepší ochrany židovských komunit a institucí v Evropě.

20 Agentura EU pro základní práva: *Your rights matter: Security concerns and experience*s (Vaše práva jsou důležitá: bezpečnostní obavy a zkušenosti), 2020.

21 Od července 2015 do konce roku 2019 zjistil Europol teroristický obsah na 361 platformách (Europol, 2020).

22 Europol: *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism* (Přezkum transatlantických osvědčených postupů pro potírání radikalizace ve věznicích a recidivismu teroristů), 2019.

23 Zpráva Evropského monitorovacího centra pro drogy a drogovou závislost (EMCDDA) a Europolu o trhu s drogami v EU za rok 2019.

24 Zpráva Europolu o finančním obchodním modelu obchodování s lidmi, 2015.

25 Zpráva Úřadu EU pro duševní vlastnictví a OECD o obchodu s padělanými farmaceutickými výrobky.

pachatelům nadále rozšiřovat spektrum trestné činnosti a infiltrovat legální ekonomiku[26]. Zločinci včetně teroristů mají snadnější přístup k palným zbraním, a to na online trzích nebo prostřednictvím nových technologií, jako je 3D tisk[27]. Riziko, že pachatelé trestných činů využijí přínosů inovací k nekalým účelům, bude ještě zvýšeno využíváním umělé inteligence, nových technologií a robotiky[28].

Tyto hrozby se vymykají klasifikaci do kategorií a různými způsoby zasahují různé části společnosti. Všechny představují velké ohrožení osob i podniků a vyžadují komplexní a ucelenou reakci na úrovni EU. Pokud bezpečnostní slabiny vykazují i malé vzájemně propojené domácí spotřebiče, například lednička nebo kávovar připojené na internet, nelze se při zajišťování bezpečnosti již spoléhat pouze na tradiční státní aktéry. Hospodářské subjekty musí nést větší odpovědnost za kybernetickou bezpečnost výrobků a služeb, které uvádějí na trh, a také lidé musí mít alespoň základní povědomí o kybernetické bezpečnosti, aby se mohli chránit sami.

III. Koordinovaná reakce EU pro celou společnost

EU již ukázala, jak může přinést skutečnou přidanou hodnotu. Od roku 2015 byly díky bezpečnostní unii vytvořeny nové vazby ve způsobu, jakým je bezpečnostní politika řešena na úrovni EU. Je však třeba učinit více, aby se zapojila celá společnost, včetně úřadů veřejné správy na všech úrovních, podniků ve všech odvětvích a jednotlivců ve všech členských státech. Rostoucí povědomí o rizicích závislosti[29] a potřeba silné evropské průmyslové strategie[30] ukazují, že Evropská unie musí disponovat kritickým objemem průmyslu, technologickou produkcí a odolným dodavatelským řetězcem. Síla rovněž znamená plně respektovat základní práva a hodnoty EU, jež jsou předpokladem legitimní, účinné a udržitelné bezpečnostní politiky. Tato strategie bezpečnostní unie vymezuje konkrétní oblasti činnosti, v nichž je třeba pokročit. Vychází z následujících společných cílů:

- ***Rozvoj schopností a budování kapacit pro včasné odhalování a prevenci krizí a rychlou reakci na ně:*** Evropa musí být odolnější, aby dokázala předcházet budoucím otřesům, chránit před nimi a zvládat je. Musíme rozvíjet schopnosti a budovat kapacity pro včasné odhalení bezpečnostních krizí a rychlou reakci na ně prostřednictvím integrovaného a koordinovaného přístupu, a to jak v obecném měřítku, tak i prostřednictvím zvláštních iniciativ pro jednotlivé sektory (např. pro finančnictví, energetiku, soudnictví, prosazování práva, zdravotní péči, námořnictví a dopravu), přičemž je třeba vycházet ze stávajících iniciativ[31]. Komise rovněž předloží návrhy na

[26] Zpráva o vyhledávání a konfiskaci majetku: zajištění toho, aby se trestná činnost nevyplácela, COM(2020) 217.

[27] V roce 2017 byly palné zbraně použity v 41 % všech teroristických útoků (Europol, 2018).

[28] V červenci 2020 představila francouzská a nizozemská policie a soudy spolu s Europolem a Eurojustem výsledky společného vyšetřování, díky němuž se podařilo rozbít síť EncroChat, šifrovanou telefonní síť používanou zločineckými sítěmi zapojenými do násilných útoků, korupce, pokusů vraždy a rozsáhlého pašování drog.

[29] Mezi rizika závislosti na zahraničí patří zvýšená expozice vůči potenciálním hrozbám, od využití slabých míst informačních infrastruktur s důsledkem ohrožení kritických infrastruktur (např. energetiky, dopravy, bankovnictví, zdravotnictví) či ovládnutí průmyslových řídicích systémů až po zvýšenou možnost krádeží dat nebo špionáže.

[30] Sdělení Komise Nová průmyslová strategie pro Evropu, COM(2020) 102.

[31] Např. integrovaná opatření pro politickou reakci na krize (IPCR), středisko pro koordinaci odezvy na mimořádné události, doporučení Komise o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (C(2017) 6100), operační protokol EU pro boj proti hybridním hrozbám (EU Playbook), SWD(2016) 227.

zřízení rozsáhlého systému řízení krizí uvnitř EU, který by mohl být využitelný i pro bezpečnostní záležitosti.

- ***Důraz na výsledky***: Strategie zaměřená na výkonnost musí být založena na pečlivé analýze hrozeb a rizik, abychom mohli napřít úsilí s co nejlepším účinkem. Musí definovat správná pravidla a vhodné prostředky a vést k jejich uplatnění v praxi. Je nutné, aby její součástí bylo spolehlivé strategické zpravodajství jako základ pro bezpečnostní politiky EU. Jsou-li vyžadovány právní předpisy EU, je třeba tyto předpisy sledovat, aby byly provedeny v plné míře, zabránilo se roztříštěnosti a nebyly ponechány zneužitelné nedostatky. Účinné provedení této strategie bude rovněž záviset na zajištění odpovídajícího finančního krytí v příštím programovém období 2021–2027, a to i pro relevantní agentury EU.
- ***Propojení všech subjektů veřejného a soukromého sektoru ve společném úsilí:*** Klíčové subjekty z veřejného i soukromého sektoru nejsou ochotny sdílet důležité bezpečnostní informace, například kvůli obavám z ohrožení konkurenceschopnosti či národní bezpečnosti.[32] Nejefektivnější však jsme, dokážeme-li spolupracovat a vzájemně se podporovat. V první řadě to vyžaduje intenzivnější spolupráci členských států se zapojením donucovacích, soudních a jiných orgánů veřejné správy a také orgánů a agentur EU s cílem nastolit porozumění a navázat vztahy potřebné pro nalezení společných řešení. Zásadní význam má i spolupráce se soukromým sektorem, a to tím spíše, že průmysl vlastní významnou část digitální a nedigitální infrastruktury, která je základním prvkem pro účinný boj proti trestné činnosti a terorismu. Mohou přispět i jednotlivci, například prostřednictvím rozvoje dovedností a zvyšování informovanosti v oblasti boje proti kyberkriminalitě nebo šíření dezinformací. V neposlední řadě platí, že toto společné úsilí musí přesáhnout naše hranice a směřovat k vybudování užších vazeb s podobně smýšlejícími partnery.

IV. Ochrana všech v EU: strategické priority bezpečnostní unie

EU má jedinečné předpoklady k tomu, aby na zmíněné nové globální hrozby a výzvy dokázala reagovat. Z výše uvedené analýzy hrozeb vyplývají čtyři vzájemně provázané strategické priority, které by měly být realizovány na úrovni EU při plném respektování základních práv: i) bezpečnostní prostředí, které obstojí i v budoucnosti; ii) potírání vyvíjejících se hrozeb; iii) ochrana Evropanů před terorismem a organizovanou trestnou činností a iv) silný evropský bezpečnostní ekosystém.

1. Bezpečnostní prostředí, které obstojí i v budoucnosti

Ochrana kritické infrastruktury a její odolnost

Lidé využívají klíčových infrastruktur v běžném životě k cestování, k práci, když potřebují základní veřejné služby, jako je zdravotní péče, doprava, dodávky energie, nebo k výkonu svých demokratických práv. Nejsou-li tyto infrastruktury dostatečně chráněny a nemají-li odpovídající odolnost, mohou útoky napáchat ohromné fyzické i digitální škody v jednotlivých členských státech i potenciálně v celé EU.

[32] Společné sdělení Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU, JOIN(2017) 450.

Stávající rámec EU pro ochranu kritických infrastruktur[33] a zvýšení jejich odolnosti již neodpovídá měnícím se rizikům. Rostoucí vzájemná závislost znamená, že narušení jednoho sektoru může bezprostředně zasáhnout i fungování sektorů jiných: útok na elektrárnu může z provozu vyřadit telekomunikace, nemocnice, banky nebo letiště, a naopak útok na digitální infrastrukturu může narušit fungování elektrických či finančních sítí. Naše hospodářství a společnost se stále více přesunují do online prostředí, a proto se pravděpodobnost těchto a podobných událostí neustále zvyšuje. Legislativní rámec potřebuje na tuto zvýšenou provázanost a vzájemnou závislost reagovat prostřednictvím důkladných opatření na ochranu kritické infrastruktury a zvýšení její odolnosti z kybernetického i fyzického hlediska. Základní služby, včetně služeb založených na kosmických infrastrukturách, musí být řádně chráněny před současnými a předpokládanými hrozbami, ale také musí být odolné. Každý systém se tedy musí dokázat připravit na nepříznivé události, počítat s nimi, absorbovat je, zotavit se z nich a úspěšněji se jim přizpůsobit.

Členské státy zároveň využily svého širokého prostoru k uvážení a uplatňují stávající legislativu různým způsobem. Výsledná roztříštěnost může narušit vnitřní trh a ztížit přeshraniční koordinaci, především v příhraničních regionech. Poskytovatelé základních služeb v různých členských státech se musí řídit různými režimy podávání zpráv. Komise zkoumá, zda by do zajištění spolehlivého poskytování základních služeb mohl vnést větší jednotnost a soudržnost **nový rámec pro fyzické i digitální infrastruktury**. Na tento rámec musí navazovat **odvětvové iniciativy** zaměřené na řešení rizik specifických pro kritické infrastrukturní systémy, jako je doprava, kosmické systémy, energetika, finance a zdravotnictví[34]. Prvním krokem bude iniciativa pro zvýšení digitální provozní odolnosti finančních odvětví vzhledem k vysoké závislosti finančního sektoru na informatických službách a jeho vysoké zranitelnosti vůči kybernetickým útokům. Další cílená iniciativa se kvůli obzvláštní citlivosti a významu energetického systému zaměří na zvýšení odolnosti kritické energetické infrastruktury vůči fyzickým, kybernetickým a hybridním hrozbám a na zajištění rovných podmínek pro všechny přeshraniční provozovatele energetických sítí.

Účinky přímých zahraničních investic relevantní pro bezpečnost, které mohou ovlivnit kritické infrastruktury nebo kritické technologie, budou mimo jiné předmětem posouzení prováděných členskými státy EU a Komisí podle nového evropského rámce pro prověřování přímých zahraničních investic[35].

Na podporu odolnosti kritických infrastruktur může EU rovněž vytvořit nové nástroje. Internet na celém světě zatím vykazuje vysokou míru odolnosti, zejména pokud jde o schopnost zvládnout větší objem provozu. Je ale nutné se připravit na možné budoucí krize, které by ohrozily jeho bezpečnost, stabilitu a odolnost. Pro zajištění nepřetržité funkčnosti internetu musíme být dobře připraveni na kybernetické incidenty a nepřátelské činnosti online a snížit závislost na infrastrukturách a službách umístěných mimo Evropu. Aby byla

[33] Směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016); směrnice Rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

[34] Vzhledem k tomu, že během krize způsobené onemocněním COVID-19 bylo tlaku vystaveno zejména odvětví zdravotnictví, Komise rovněž zváží iniciativy na posílení rámce EU pro zdravotní bezpečnost a odpovědných agentur EU, aby zvládly reagovat na vážné přeshraniční zdravotní hrozby.

[35] Od 11. října 2020 se začne v plném rozsahu uplatňovat nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie, jež vybaví EU novým mechanismem spolupráce v otázce přímých investic ze zemí mimo EU, které by mohly ovlivnit bezpečnost nebo veřejný pořádek. Podle tohoto nařízení posoudí členské státy a Komise potenciální rizika spojená s těmito přímými zahraničními investicemi, a je-li to vhodné a relevantní nejméně pro dva členské státy, navrhnou k jejich zmírnění vhodné prostředky.

zaručena vysoká společná úroveň bezpečnosti sítí a informačních systémů v EU, bude to vyžadovat různé právní předpisy ve spojení s přezkumem stávajících pravidel. Také budou nutné vyšší investice do výzkumu a inovací a případně zavedení nebo stabilizace základních internetových infrastruktur a prostředků, zejména systému DNS[36].

Zásadním faktorem pro ochranu klíčových digitálních aktiv EU a jednotlivých států je mít k dispozici bezpečný komunikační kanál pro kritické infrastruktury. Komise spolupracuje s členskými státy na zavedení certifikované, pozemní a kosmické zabezpečené kvantové infrastruktury mezi koncovými body, která bude kombinována se zabezpečeným systémem družicové komunikace v rámci státní správy, jak je stanoven v nařízení o kosmickém programu[37].

Kybernetická bezpečnost

Počet kybernetických útoků neustále roste[38]. Tyto útoky jsou stále důmyslnější, pocházejí od nejrůznějších původců uvnitř i mimo EU a cílí na nejzranitelnější oblasti. Často jsou do nich zapojeny státní či státem podporovaní aktéři, kteří se zaměřují na hlavní digitální infrastruktury, např. na velké poskytovatele cloudových služeb[39]. Kybernetická rizika začínají rovněž významně ohrožovat finanční systém. Mezinárodní měnový fond odhadl v celosvětovém měřítku roční ztrátu v důsledku kybernetických útoků na 9 % čistého příjmu bank, tj. přibližně 100 miliard USD[40]. Přechod na propojená zařízení přinese uživatelům značné výhody, avšak s tím, jak bude méně dat uchováváno a zpracováváno v datových centrech a více jich bude zpracováváno blíže uživatelům na okraji sítě[41], se při zajišťování kybernetické bezpečnosti již nelze soustředit pouze na ochranu ústředních prvků[42].

V roce 2017 předložila EU koncepci kybernetické bezpečnosti zaměřenou na budování odolnosti, rychlou reakci a účinné odrazování.[43] Nyní musí zajistit, aby její kapacity v oblasti kybernetické bezpečnosti odpovídaly reálné situaci a odolnost i lepší reakci skutečně přinesly. Podmínkou toho je zapojit celou společnost, včetně orgánů, institucí a jiných subjektů EU, členských států, průmyslu, akademické obce a jednotlivců, a dát kybernetické bezpečnosti prioritu, kterou potřebuje[44]. Tento horizontální přístup pak musí doplnit zvláštní koncepce kybernetické bezpečnosti pro jednotlivá odvětví, např. energetiku, finanční služby, dopravu nebo zdravotnictví. Další fáze činnosti EU by měly být vymezeny v revidované evropské strategii kybernetické bezpečnosti.

---

[36] Systém názvů domén (DNS) je hierarchicky uspořádaný a decentralizovaný systém názvů pro počítače, služby nebo jiná zařízení připojená k internetu nebo soukromé síti. Tento systém převádí názvy domén na IP adresy potřebné pro lokalizaci a identifikaci počítačových služeb a zařízení.

[37] Návrh nařízení, kterým se zavádí kosmický program Unie a Agentura Evropské unie pro kosmický program, COM(2018) 447 final.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Neustálou hrozbu představuje útok distribuovaným odmítnutím služby (DDoS): velcí poskytovatelé museli odrážet masivní útoky DDoS, např. útok na webové služby společnosti Amazon v únoru 2020.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

[41] „Edge computing“ (hraniční architektura) je distribuovaná, otevřená IT architektura, která se vyznačuje decentralizovanou strukturou zpracování dat a používá se pro technologie mobilních zařízení a internetu věcí. V rámci hraniční architektury jsou data zpracovávána samotným zařízením nebo místním počítačem či serverem namísto toho, aby byla předána do datového centra.

[42] Sdělení Evropská strategie pro data, COM(2020) 66 final.

[43] Společné sdělení Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU, JOIN(2017) 450.

[44] Zpráva Společného výzkumného střediska *Cybersecurity – our digital Anchor* (Kybernetická bezpečnost – naše digitální opora) poskytuje všestranný vhled do nárůstu kybernetické bezpečnosti za posledních 40 let.

Součástí úsilí o posílení kybernetické bezpečnosti, jakož i boje proti terorismu, extremismu, radikalismu a hybridním hrozbám by mělo být zkoumání nových a zdokonalených forem spolupráce mezi zpravodajskými službami, Zpravodajským a informačním centrem EU (EU INTCEN) a dalšími organizacemi zabývajícími se bezpečností.

Vzhledem k postupnému zavádění **infrastruktury sítí 5G** v celé EU a k potenciální závislosti řady kritických služeb na těchto sítích by jakékoliv systematické a rozsáhlé narušení mělo velmi vážné následky. Díky procesu zahájenému Komisí v doporučení o kybernetické bezpečnosti sítí 5G[45] z roku 2019 již některé členské státy podnikly kroky k uskutečnění hlavních opatření stanovených v sadě nástrojů pro sítě 5G[46].

Jednou z nejdůležitějších dlouhodobých potřeb je rozvíjet kulturu **kybernetické bezpečnosti již od návrhu**, aby bylo zabezpečení zabudováno do výrobků a služeb od samého počátku. Významným přínosem v tomto směru bude nový rámec pro certifikaci kybernetické bezpečnosti podle aktu o kybernetické bezpečnosti[47]. Na rámci se již pracuje: připravují se dva systémy certifikace a priority pro další programy mají být stanoveny později v tomto roce. Zásadní význam v této oblasti má spolupráce mezi Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA), úřady pro ochranu údajů a Evropským sborem pro ochranu údajů[48].

Komise již v minulosti konstatovala, že je nezbytné, aby strukturovanou a koordinovanou operativní spolupráci zajišťovala **společná kybernetická jednotka**. Jedním z prvků této spolupráce by mohl být mechanismus vzájemné pomoci v krizové situaci na úrovni EU. V návaznosti na provádění doporučení o plánu koordinované reakce[49] by společná kybernetická jednotka mohla pracovat na budování důvěry mezi různými aktéry v evropském ekosystému kybernetické bezpečnosti a nabízet členským státům zásadní služby. Komise zahájí jednání s příslušnými zainteresovanými stranami (počínaje členskými státy) a do konce roku 2020 stanoví jasný postup, milníky a harmonogram.

Důležitá jsou rovněž společná pravidla o bezpečnosti informací a kybernetické bezpečnosti pro všechny orgány, instituce a jiné subjekty EU. Cílem by mělo být vytvořit závazné a přísné společné normy pro bezpečnou výměnu informací a bezpečnost digitálních infrastruktur a systémů ve všech orgánech, institucích a jiných subjektech EU. Tento nový rámec by měl ve všech z nich podnítit rozsáhlou a efektivní operativní spolupráci v oblasti kybernetické bezpečnosti, v níž by ústřední roli hrála skupina pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (CERT-EU).

Vzhledem ke globální povaze kybernetické bezpečnosti má zásadní význam pro další předcházení kybernetickým útokům, odrazování od nich a odezvu na ně budování a udržování pevných **mezinárodních partnerství**. Rámec pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti

---

[45] Doporučení Komise o kybernetické bezpečnosti sítí 5G, COM(2019) 2335. Přezkum doporučení má být proveden v posledním čtvrtletí roku 2020.

[46] Viz zpráva skupiny pro spolupráci v oblasti bezpečnosti sítí a informací o provádění této sady nástrojů ze dne 24. července 2020.

[47] Nařízení (EU) 2019/881 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti).

[48] Sdělení Ochrana osobních údajů jakožto pilíř posílení postavení občanů a přístup EU k digitální transformaci – dva roky uplatňování obecného nařízení o ochraně údajů, COM(2020) 264.

[49] Doporučení Komise (EU) 2017/1584 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize.

kybernetiky“)[50] stanoví opatření společné zahraniční a bezpečnostní politiky, včetně omezujících opatření (sankcí), která mohou být použita proti činnostem poškozujícím politické, bezpečnostní a hospodářské zájmy Unie. EU by rovněž měla zintenzivnit svou činnost prostřednictvím fondů pro rozvoj a spolupráci s cílem zajistit budování kapacit, které partnerským státům pomohou při posilování digitálních ekosystémů, přijímání národních legislativních reforem a dodržování mezinárodních norem. Zvyšuje to odolnost celého společenství a jeho schopnost čelit kybernetickým hrozbám a účinně na ně reagovat. Patří sem i konkrétní snahy o prosazování unijních norem a příslušných právních předpisů s cílem zvýšit kybernetickou bezpečnost partnerských zemí v sousedství[51].

Ochrana veřejných prostor

Nedávné teroristické útoky se zaměřily na **veřejné prostory**, včetně bohoslužebných prostor a dopravních uzlů, přičemž využily jejich otevřenosti a přístupnosti. Vzedmutí terorismu vyvolaného politickým nebo ideologicky motivovaným extremismem tuto hrozbu ještě umocnilo. Je potřeba zvýšit fyzickou ochranu těchto míst a nasadit vhodné systémy detekce, aniž by však byly ohroženy občanské svobody[52]. Komise posílí spolupráci veřejného a soukromého sektoru při ochraně veřejných prostor prostřednictvím financování, výměny zkušeností a osvědčených postupů a také vydá konkrétní pokyny[53] a doporučení[54]. Součástí toho bude rovněž zvyšování informovanosti, stanovení požadavků na výkonnost, testování detekčních zařízení a zlepšení kontrol bezúhonnosti k řešení vnitřních hrozeb. Jako důležitý aspekt je třeba zohlednit, že neúměrně mohou být postiženy obzvláště menšiny a zranitelní lidé, například osoby, které jsou terčem kvůli svému náboženskému vyznání nebo pohlaví, a vyžadují proto zvláštní pozornost. Při zlepšování bezpečnosti veřejných prostor hrají důležitou úlohu regionální a místní orgány veřejné správy. Komise rovněž pomáhá podporovat související inovace ve městech[55]. V listopadu 2018 bylo v rámci nové městské agendy[56] zahájeno partnerství zaměřené právě na bezpečnost ve veřejném prostoru, což odráží pevné odhodlání členských států, Komise a měst bezpečnostní hrozby v městském prostoru lépe řešit.

Nepřetržitě roste trh s **drony** (bezpilotními vzdušnými prostředky), které mají četné cenné a legitimní využití. Mohou však být také zneužity pachateli trestné činnosti včetně teroristů, přičemž veřejné prostory jsou ohroženy obzvláště. Mezi cíle mohou patřit jednotlivci, shromáždění lidí, kritická infrastruktura, donucovací orgány, hranice nebo veřejné prostory. Znalosti o používání dronů v konfliktech by se mohly dostat do Evropy buď přímo (s navracejícími se zahraničními teroristickými bojovníky) nebo online cestou. Důležitý první krok představují pravidla již vypracovaná Evropskou agenturou pro bezpečnost letectví,

---

50 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

51 Viz pokyny EU pro budování vnějších kapacit přijaté v závěrech Rady ze dne 26. června 2018.

52 Zvláštní pozornost si zaslouží systémy biometrické identifikace na dálku. Prvotní názory Komise jsou nastíněny v bílé knize Komise ze dne 19. února 2020 o umělé inteligenci, COM(2020) 65.

53 Viz například *Guidance on selecting proper security barrier solutions for public space protection* (Pokyny pro výběr vhodných řešení bezpečnostních bariér pro ochranu veřejného prostoru) (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

54 Pokyny k osvědčeným postupům jsou uvedeny v dokumentu SWD(2019) 140, který obsahuje i oddíl o spolupráci veřejného a soukromého sektoru. Na posílení této spolupráce jsou určeny především finanční prostředky z Fondu pro vnitřní bezpečnosti – policie.

55 Tři města (řecký Pireus, finské Tampere a italský Turín) budou testovat nová řešení v rámci Městských inovativních opatření, která jsou spolufinancována z Evropského fondu pro regionální rozvoj (EFRR).

56 Městská agenda EU představuje novou víceúrovňovou pracovní metodu, která podporuje spolupráci mezi členskými státy, městy, Evropskou komisí a dalšími zúčastněnými stranami s cílem stimulovat růst a inovace v evropských městech, zlepšit jejich obyvatelnost a identifikovat a úspěšně řešit sociální výzvy.

která se týkají například registrace provozovatelů dronů či povinné identifikace dronů na dálku. Vzhledem k tomu, že se rozšíření dronů, jejich dostupnost a schopnosti zvyšují, je třeba přijmout další opatření. Ta by mohla například zahrnovat sdílení informací, poradenství a osvědčené postupy otevřené všem, včetně pro účely prosazování práva, ale i rozsáhlejší testování prostředků proti dronům[57]. Vedle toho je třeba podrobněji analyzovat a řešit důsledky používání dronů ve veřejných prostorech na soukromí a ochranu údajů.

Klíčová opatření
• Právní předpisy o ochraně kritické infrastruktury a zvýšení její odolnosti • Revize směrnice o bezpečnosti sítí a informací • Iniciativa pro zvýšení provozní odolnosti finančního sektoru • Ochrana a kybernetická bezpečnost kritické energetické infrastruktury a kodex sítě pro kybernetickou bezpečnost přeshraničních toků elektřiny • Evropská strategie kybernetické bezpečnosti • Další kroky směrem k vytvoření společné kybernetické jednotky • Společná pravidla pro všechny orgány, instituce a jiné subjekty EU týkající se bezpečnosti informací a kybernetické bezpečnosti • Intenzivnější spolupráce při ochraně veřejných prostor, včetně bohoslužebných míst • Sdílení osvědčených postupů, jak přistupovat k zneužívání dronů

2. Potírání vyvíjejících se hrozeb

Kyberkriminalita

Technologie přináší nové příležitosti pro společnost. Nabízí rovněž nové nástroje pro soudnictví a prosazování práva, zároveň ale otevírá dveře pachatelům trestné činnosti. Škodlivý software, krádež osobních či obchodních dat hackery a přerušení digitálních aktivit, které způsobuje finanční újmu či poškození dobré pověsti, to vše je na vzestupu. Nejdůležitější obranou proti tomu je odolné prostředí se silnou kybernetickou bezpečností. Donucovací orgány musí být schopny provádět vyšetřování v digitálním prostředí podle jasných pravidel pro vyšetřování a stíhání trestných činů a zároveň řádně chránit poškozené. Tato práce by měla navázat na činnost společné pracovní skupiny pro boj proti kyberkriminalitě v Europolu a na nouzový protokol pro reakci prostřednictvím prosazování práva, který byl vytvořen za účelem koordinace reakce na rozsáhlé kybernetické útoky. Klíčové jsou též účinné mechanismy umožňující partnerství veřejného a soukromého sektoru a jejich spolupráci.

Boj proti kybernetické kriminalitě by se zároveň měl stát strategickou komunikační prioritou v celé EU, aby všichni Evropané byli informování o rizicích a preventivních opatřeních, která mohou podniknout. To vše by mělo být součástí proaktivního přístupu. Zásadním krokem je rovněž úplné provedení stávajícího právního rámce[58]: Komise bude v případě potřeby připravena použít řízení o porušení Smlouvy a stávající rámec bude nepřetržitě vyhodnocovat, aby zajistila jeho vhodnost. Spolu s Europolem a Agenturou EU pro kybernetickou bezpečnost ENISA též Komise posoudí možnost vytvoření celounijního

[57] Nedávno byl vypracován víceletý testovací program, který má pomoci členským státům při vytvoření společné metodiky a vývoji zkušební platformy.

[58] Směrnice 2013/40/EU o útocích na informační systémy.

systému včasného varování o kyberkriminalitě, který by pomohl zajistit tok informací a rychlou reakci v případě jejího prudkého nárůstu.

Kyberkriminalita je globální problém, který vyžaduje účinnou mezinárodní spolupráci. EU prosazuje budapešťskou Úmluvu Rady Evropy o počítačové kriminalitě, což je účinný, zavedený rámec umožňující všem zemím určit, jaké systémy a komunikační kanály mají v zájmu efektivní spolupráce zavést.

Téměř polovina občanů EU se obává zneužití údajů[59] a zejména **krádeže totožnosti**[60]. Používání falešné identity za účelem finančního zisku je jeden aspekt, ale může se jednat i o významný osobní a psychologický zásah, protože na internetu mohou dlouhá léta zůstat nelegální příspěvky vytvořené osobou, která totožnost zcizila. Komise posoudí možná praktická opatření na ochranu obětí proti všem formám krádeže totožnosti, přičemž zohlední připravovanou evropskou iniciativu zaměřenou na digitální identitu[61].

Abychom dokázali kyberkriminalitu úspěšně potírat, musíme hledět do budoucnosti. Zároveň s tím, jak společnost využívá technologického pokroku k rozvoji hospodářství a společnosti, mohou pachatelé trestné činnosti rovněž hledat možnosti, jak tyto nástroje využít k nekalým účelům. Pachatelé mohou například použít umělou inteligenci k hledání a identifikaci hesel nebo k jednoduššímu naprogramování škodlivého softwaru s cílem získat obrazové a zvukové záznamy, jež lze následně zneužít ke krádeži či podvodnému zneužití totožnosti.

Moderní prosazování práva

Odborníci v oblasti prosazování práva a justice se musí přizpůsobit novým technologiím. Technologický vývoj a nové hrozby si žádají, aby donucovací orgány měly přístup k novým nástrojům, získaly nové dovednosti a vypracovaly alternativní vyšetřovací metody. V zájmu doplnění legislativních opatření, která mají zlepšit přeshraniční přístup k elektronickým důkazům pro účely vyšetřování trestných činů, může EU pomoci donucovacím orgánům vytvořit nezbytnou kapacitu pro identifikaci, zabezpečení a čtení dat potřebných pro vyšetřování trestných činů a pro využití těchto dat jako důkazního materiálu u soudu. Komise posoudí opatření pro **zvýšení kapacity donucovacích orgánů pro vyšetřování v digitálním prostředí**, přičemž definuje, jak k vytvoření nových nástrojů pro prosazování práva co nejlépe využít výzkumu a vývoje. Vymezí také, jaká odborná příprava může nabídnout správný soubor dovedností pro donucovací orgány a soudy. Společné výzkumné středisko Komise v rámci toho vypracuje přísná vědecká hodnocení a zkušební metody.

Společný přístup může rovněž zajistit, aby se **umělá inteligence, kosmické kapacity, data velkého objemu** a **vysoce výkonná výpočetní technika začlenily** do bezpečnostní politiky způsobem účinným jak v boji proti trestné činnosti, tak z hlediska dodržování základních práv. Umělá inteligence by mohla v boji proti trestné činnosti fungovat jako účinný nástroj, neboť může nesmírně zvýšit kapacitu vyšetřování díky analýze velkého objemu informací a identifikaci vzorců a anomálií[62]. Může rovněž nabídnout konkrétní nástroje, které například pomohou identifikovat teroristický obsah na internetu, odhalit podezřelé transakce při

[59] Celkem 46 % (průzkum Eurobarometr o postojích Evropanů ke kybernetické bezpečnosti, leden 2020).

[60] Naprostá většina respondentů v průzkumu Eurobarometr z roku 2018 nazvaného Postoje Evropanů k bezpečnosti na internetu (95 %) považuje krádež totožnosti za závažný trestný čin, a sedm z deseti míní, že se jedná o trestný čin, který je velmi závažný. Průzkum Eurobarometr zveřejněný v lednu 2020 potvrdil, že veřejnost se obává kyberkriminality, internetových podvodů a krádeží identity: dvě třetiny respondentů uvedly, že se bojí bankovního podvodu (67 %) nebo krádeže identity (66 %).

[61] Sdělení ze dne 19. února 2020 o utváření digitální budoucnosti Evropy, COM(2020) 67.

[62] Například u finančních trestných činů.

prodeji nebezpečných výrobků nebo pomoci lidem v krizových situacích. K využití tohoto potenciálu je nutné propojit výzkum a inovace s odpovídající správou a technickou infrastrukturou a aktivně zapojit uživatele umělé inteligence, soukromý sektor a akademickou obec. Znamená to také, že je třeba zaručit nejvyšší standardy dodržování základních práv a zároveň účinně chránit občany. Zejména platí, že rozhodnutí, která ovlivňují život konkrétní osoby, musí být vždy posouzena člověkem a musí vyhovovat příslušným platným právním předpisům EU[63].

Elektronické informace a důkazy jsou potřebné přibližně v 85 % vyšetřování závažných trestných činů, přičemž 65 % všech žádostí směřuje na poskytovatele online služeb, kteří mají sídlo v jiné jurisdikci[64]. Skutečnost, že namísto tradičních fyzických stop je nyní třeba pátrat na internetu, dále rozevírá nůžky mezi schopnostmi donucovacích orgánů a pachatelů. Zásadní význam má vytvoření jasných pravidel pro přeshraniční přístup k elektronickým důkazům pro účely trestního vyšetřování, a proto je velmi důležité, aby Evropský parlament a Rada rychle přijaly návrhy o elektronických důkazech a odborníci z praxe tak získali účinný nástroj. Přeshraniční přístup k elektronickým důkazům prostřednictvím mnohostranných a dvoustranných mezinárodních jednání je rovněž rozhodující pro zavedení vzájemně slučitelných pravidel na mezinárodní úrovni[65].

Přístup k digitálním důkazům závisí rovněž na dostupnosti informací. Jsou-li údaje vymazány příliš rychle, mohou důležité důkazy zmizet, což znemožní identifikovat a lokalizovat podezřelé osoby a zločinecké sítě (i oběti). Na druhé straně vyvolávají režimy uchovávání údajů otázky v souvislosti s ochranou soukromí. Komise posoudí další postup v oblasti uchovávání údajů v závislosti na výsledku řízení u Evropského soudního dvora.

Pro vyšetřování trestných činů, kybernetickou bezpečnost a ochranu spotřebitelů je důležitý přístup k informacím o registraci doménových jmen na internetu (údaje WHOIS)[66]. Přístup k těmto informacím je však stále obtížnější – čeká se, dokud Internetové sdružení pro přidělování jmen a čísel (ICANN) nepřijme pro údaje WHOIS nová pravidla. Komise bude se sdružením ICANN a s mnoha dalšími zainteresovanými stranami nadále spolupracovat na tom, aby subjekty včetně donucovacích orgánů, které potřebují legitimní přístup k údajům, mohly získat účinný přístup k údajům WHOIS v souladu s unijními a mezinárodními právními předpisy o ochraně údajů. Součástí bude posouzení možných řešení, včetně toho, zda by bylo třeba přijmout právní předpisy, které by vyjasnily pravidla pro přístup k těmto informacím.

Donucovací orgány a soudy musí být rovněž vybaveny k získání potřebných údajů a důkazů, jakmile bude v EU plně zavedena **architektura sítí 5G pro mobilní telekomunikace**, a to způsobem, který bude plně respektovat důvěrnost komunikace. Komise bude při vytváření mezinárodních norem, definování osvědčených postupů, procesů a technické interoperability v klíčových technologických oblastech, jako je umělá inteligence, internet věcí nebo technologie blockchain, podporovat posílený a koordinovaný přístup.

---

[63] To znamená v souladu se stávajícími právními předpisy včetně obecného nařízení o ochraně osobních údajů (EU) 2016/679 a směrnice o prosazování práva (EU) 2016/680, která upravuje zpracování osobních údajů za účelem odhalování, prevence, vyšetřování a stíhání trestných činů nebo výkonu trestů.

[64] Dokument útvarů Komise SWD(2018) 118 final.

[65] Zejména druhý dodatkový protokol k budapešťské Úmluvě Rady Evropy o kyberkriminalitě a dohoda mezi EU a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům.

[66] Tyto informace jsou uloženy v databázích vedených 2 500 registrátory a provozovateli registrů po celém světě.

Vyšetřování všech forem trestné činnosti a terorismu dnes z velké části využívá **zašifrovaných informací**. Šifrování má zásadní význam pro digitální prostředí, zabezpečení digitálních systémů a transakcí a také pro ochranu řady základních práv, včetně svobody projevu, soukromí a ochrany údajů. Je-li využito k trestné činnosti, může ale sloužit i k zakrytí totožnosti zločinců a skrytí obsahu jejich komunikace. Komise prozkoumá a podpoří vyvážená technická, operativní a právní řešení této problematiky a bude prosazovat přístup, který zachová účinnost šifrování při ochraně soukromí a bezpečnosti komunikací a zároveň přinese efektivní odezvu na trestnou činnost a terorismus.

Potírání nezákonného obsahu na internetu

Sladit bezpečnost digitálního a fyzického prostředí znamená pokračovat v **potírání nezákonného obsahu na internetu**. Nejdůležitější hrozby pro občany, jako je terorismus, extremismus nebo pohlavní zneužívání dětí, stále více využívají digitální prostředí, což vyžaduje konkrétní opatření a rámec pro zajištění dodržování základních práv. Zásadním prvním krokem je rychle dokončit jednání o navrhovaném právním předpisu o teroristickém obsahu online[67] a zajistit jeho provádění. Klíčový význam pro boj proti zneužívání internetu teroristy, násilnými extremisty a pachateli trestné činnosti má rovněž posílení dobrovolné spolupráce mezi donucovacími orgány a soukromým sektorem v rámci **internetového fóra EU**. Jednotka EU pro oznamování internetového obsahu, která je součástí Europolu, bude i nadále hrát důležitou roli při sledování činnosti teroristických skupin online, opatření přijatých platformami[68] i při dalším rozpracování **krizového protokolu EU**[69]. Komise bude též stále spolupracovat s mezinárodními partnery, mimo jiné se v zájmu řešení těchto výzev na celosvětové úrovni zapojí do **globálního internetového fóra pro boj proti terorismu**. Nadále se bude pracovat na rozvoji alternativní argumentace a protiargumentace prostřednictvím programu na podporu občanské společnosti[70].

S cílem předcházet šíření nezákonných nenávistných projevů online a potírat je zveřejnila Komise v roce 2016 kodex chování proti nezákonným nenávistným projevům online, jehož prostřednictvím se online platformy dobrovolně zavázaly k odstraňování těchto projevů. Z nejnovějšího hodnocení vyplývá, že internetové společnosti vyhodnotí 90 % označeného obsahu do 24 hodin a odstraní 71 % obsahu považovaného za nezákonné nenávistné projevy. Platformy však musí zlepšit transparentnost a zpětnou vazbu pro uživatele a zajistit konzistentní hodnocení označeného obsahu[71].

Internetové fórum EU rovněž usnadní výměnu informací o současných a rozvíjejících se technologiích zaměřenou na problémy spojené s pohlavním zneužíváním dětí na internetu. Boji proti tomuto fenoménu se věnuje nová strategie pro posílení **boje proti pohlavnímu zneužívání dětí**[72], jejímž cílem bude maximalizovat využívání nástrojů, které jsou na úrovni EU proti těmto trestným činům k dispozici. Příslušné společnosti musí být schopny pokračovat v práci na odhalování dětské pornografie a jejím odstraňování z internetu, přičemž škody způsobené tímto materiálem vyžadují právní úpravu vymezující jasné a trvalé povinnosti s cílem tento problém řešit. V uvedené strategii bude rovněž oznámeno, že Komise začne připravovat cílený právní předpis zaměřený na zvýšení účinnosti boje proti tomuto fenoménu při plném respektování základních práv.

---

67 Návrh nařízení o prevenci šíření teroristického obsahu online, COM(2018) 640 ze dne 12. září 2018.
68 Europol, listopad 2019.
69 Evropa, která chrání – krizový protokol EU: reakce na teroristický obsah na internetu online (říjen 2019).
70 Ve spojení s činností v rámci programu pro zvyšování povědomí o radikalizaci, viz oddíl IV bod 3 níže.
71 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf
72 Strategie EU pro účinnější boj proti pohlavnímu zneužívání dětí, COM(2020) 607.

Připravovaný akt o digitálních službách v obecnější rovině také vyjasní a aktualizuje pravidla odpovědnosti a bezpečnosti v oblasti digitálních služeb a odstraní překážky, které potírání nezákonného obsahu, zboží nebo služeb brání.

Vedle toho bude Komise nadále spolupracovat s mezinárodními partnery a s **globálním internetovým fórem pro boj proti terorismu**, a to i prostřednictvím nezávislého poradního výboru, a jednat o tom, jak tuto problematiku řešit na celosvětové úrovni při současném zachování hodnot EU a základních práv. Je třeba se zabývat také novými tématy, jako jsou algoritmy nebo hraní online her[73].

Hybridní hrozby

Rozsah a rozmanitost dnešních hybridních hrozeb nemá obdoby. V souvislosti s krizí COVID-19 se tento fakt ještě potvrdil, neboť několik státních a nestátních aktérů se snažilo pandemie zneužít, zejména manipulací s informačním prostředím a napadením základních infrastruktur. Tato situace by mohla oslabit sociální soudržnost a podkopat důvěru v orgány EU a vlády členských států.

Přístup EU k hybridním hrozbám je stanoven ve společném rámci z roku 2016[74] a ve společném sdělení z roku 2018 o zvýšení odolnosti vůči hybridním hrozbám[75]. Opatření na úrovni EU se opírají o rozsáhlý soubor nástrojů zahrnující propojení vnitřních a vnějších vztahů, který vychází z celospolečenského přístupu a z úzké spolupráce se strategickými partnery, zejména s NATO a G7. Zpráva o provádění přístupu EU k hybridním hrozbám se zveřejňuje společně s touto strategií[76]. Na základě mapování[77] předloženého souběžně s touto strategií vytvoří útvary Komise a Evropská služba pro vnější činnost **vyhrazenou internetovou platformu**, na níž budou členské státy moci konzultovat nástroje a opatření, které jsou pro boj proti hybridním hrozbám k dispozici na úrovni EU.

Ačkoli odpovědnost za boj proti hybridním hrozbám nesou v první řadě členské státy, protože je přirozeně provázán s vnitrostátní bezpečnostní a obrannou politikou, mají některá slabá místa všechny členské státy společné a určité hrozby překračují hranice, například útoky na přeshraniční sítě nebo infrastrukturu. Komise a vysoký představitel Unie pro bezpečnostní politiku vypracují přístup EU k hybridním hrozbám, který hladce propojí vnitřní a vnější rozměr i vnitrostátní a celounijní aspekty. Tento přístup musí obsáhnout plné spektrum opatření, od včasného odhalování, analýzy, zvyšování informovanosti, budování odolnosti a prevence až po reakci na krizi a zvládání jejích následků.

Vzhledem k nepřetržitému vývoji hybridních hrozeb bude zvláštní pozornost kromě posíleného provádění věnována **začleňování problematiky hybridních hrozeb do tvorby politik** s cílem udržet krok s proměnlivou situací a zajistit, aby žádná potenciálně relevantní iniciativa nebyla přehlédnuta. Z pohledu problematiky hybridních hrozeb budou posuzovány i účinky iniciativ v oblastech, na něž se boj proti hybridním hrozbám dosud nezaměřoval, jako je vzdělávání, technologie a výzkum. Tento přístup by těžil z práce již vykonané na konceptualizaci hybridních hrozeb, která poskytla komplexní přehled různých prostředků,

[73] Ke komunikaci teroristé stále více využívají chatovací systémy na herních platformách a mladí teroristé si navíc přehrávají násilné útoky ve videohrách.

[74] Společný rámec pro boj proti hybridním hrozbám – Reakce Evropské unie, JOIN (2016) 18.

[75] Zvýšení odolnosti a posílení schopností reagovat na hybridní hrozby, JOIN(2018) 16.

[76] Zpráva o provádění společného rámce pro boj proti hybridním hrozbám z roku 2016, SWD(2020) 153, a společné sdělení o zvýšení odolnosti a posílení kapacit pro řešení hybridních hrozeb z roku 2018.

[77] Mapování opatření týkajících se zvyšování odolnosti a boje proti hybridním hrozbám, SWD(2020) 152.

které by mohli nepřátelé využívat[78]. Cílem by mělo být zajistit, aby se rozhodovací proces opíral o pravidelné a komplexní zpravodajské informace o vývoji hybridních hrozeb. Do značné míry to bude záviset na zpravodajských službách členských států a na prohloubení zpravodajské spolupráce s příslušnými útvary členských států prostřednictvím Zpravodajského a informačního centra EU.

S cílem zlepšit **informovanost o situaci** prozkoumají útvary Komise a Evropská služba pro vnější činnost možnosti, jak zefektivnit informační toky z různých zdrojů, včetně členských států nebo agentur EU jako ENISA, Europol a Frontex. Kontaktním místem EU pro posuzování hybridních hrozeb zůstane středisko EU pro hybridní hrozby. Pro předcházení hybridním hrozbám a ochranu před nimi je zásadní **budování odolnosti**. Je proto nezbytné systematicky sledovat a objektivně měřit pokrok v této oblasti. Prvním krokem bude určit ukazatele hybridní odolnosti v jednotlivých odvětvích jak pro členské státy, tak pro orgány a instituce EU. Ke zvýšení **připravenosti na reakci na hybridní krize** by také měl být přehodnocen stávající protokol pro hybridní hrozby, vymezený v EU Playbook z roku 2016[79], a to s ohledem na zvažovaný obecnější přezkum systému EU pro reakci na krize a jeho posílení[80]. Cílem je maximalizovat účinek opatření EU rychlým propojením reakce jednotlivých odvětví a zajištěním hladké spolupráce s partnery, především s NATO.

Klíčová opatření
• Zajištění, aby právní předpisy týkající se kyberkriminality byly prováděny a plnily svůj účel • Strategie EU pro účinnější boj proti pohlavnímu zneužívání dětí • Návrhy týkající se odhalování a odstraňování dětské pornografie • Přístup EU k boji proti hybridním hrozbám • Přezkum operačního protokolu EU pro boj proti hybridním hrozbám (EU Playbook) • Posouzení, jak zvýšit kapacitu donucovacích orgánů při vyšetřování v digitálním prostředí

3. Ochrana Evropanů před terorismem a organizovanou trestnou činností

Terorismus a radikalizace

Hrozba terorismu v EU je i nadále vysoká. Celkový počet útoků sice klesá, ale přesto mohou mít devastující účinky. Radikalizace může rovněž obecněji polarizovat společnost a destabilizovat sociální soudržnost. Hlavní odpovědnost za boj proti terorismu a radikalizaci stále nesou členské státy, narůstající přeshraniční/meziodvětvový rozměr hrozeb však vyžaduje další kroky v oblasti spolupráce a koordinace EU. Prioritou je účinné provádění právních předpisů EU v oblasti boje proti terorismu[81], včetně omezujících opatření. Cílem

[78] *Landscape of Hybrid Threats*: *A conceptual Model* (Přehled hybridních hrozeb: konceptuální model), JRC117280, vypracovaný Společným výzkumným střediskem ve spolupráci s Evropským střediskem pro boj proti hybridním hrozbám.

[79] Operační protokol EU pro boj proti hybridním hrozbám (EU Playbook), SWD(2016) 227.

[80] Po videokonferenci z 26. března 2020 přijali členové Evropské rady prohlášení o opatřeních EU v reakci na šíření nákazy COVID-19, v němž vyzvali Komisi, aby předložila návrhy na ambicióznější a rozsáhlejší systému řízení krizí uvnitř EU.

[81] S cílem bojovat proti terorismu přijala Rada omezující opatření týkající se ISIL (Dá'iš) a al-Káidy a také zvláštní omezující opatření namířená proti některým osobám a subjektům. Přehled všech omezujících opatření je uveden v mapě sankcí EU (https://www.sanctionsmap.eu/#/main).

zůstává rozšířit mandát Úřadu evropského veřejného žalobce na přeshraniční teroristické trestné činy.

Boj proti terorismu začíná řešením základních příčin tohoto jevu. Polarizace společnosti, skutečná nebo vnímaná diskriminace a další psychologické a sociologické faktory, to vše může zvýšit vnímavost vůči radikálnímu diskursu. Boj proti **radikalizaci** je proto úzce provázán s podporou sociální soudržnosti na místní, celostátní i evropské úrovni. V posledním desetiletí bylo vytvořeno několik iniciativ a politik s vysokým dopadem, zejména prostřednictvím sítě pro zvyšování povědomí o radikalizaci a iniciativy Města EU proti radikalizaci[82]. Nyní je načase zvážit opatření k zefektivnění politik, iniciativ a finančních prostředků EU zaměřených na řešení tohoto fenoménu. Tato opatření mohou podpořit rozvoj schopností a dovedností, prohloubit spolupráci, posílit důkazní základnu a pomoci vyhodnotit dosažený pokrok se zapojením všech příslušných zúčastněných stran, včetně odborníků z praxe v první linii, tvůrců politik a akademické obce[83]. K prevenci radikalizace by mohly přispět tzv. měkké politiky, např. pro vzdělávání, kulturu, mládež a sport, které dávají příležitost ohrožené mládeži a posilují soudržnost uvnitř EU[84]. Prioritně je třeba pracovat na včasném odhalování radikalizovaných jedinců, řízení rizik, budování odolnosti a odklonu od teroristické činnosti, jakož i na rehabilitaci a opětovném začlenění do společnosti.

Teroristé se snaží získat **chemické, biologické, radiologické a jaderné** (CBRN)[85] materiály a rozvíjet své znalosti a schopnost tyto materiály využít jako zbraně[86]. V teroristické propagandě je potenciál chemického, biologického, radiologického nebo jaderného útoku zmiňován velmi často. Vzhledem k vysokým potenciálním škodám je třeba věnovat této problematice zvláštní pozornost. V návaznosti na koncepci použitou při regulaci přístupu k prekurzorům výbušnin se Komise zaměří na omezení přístupu k některým nebezpečným chemickým látkám, které by mohly být použity k útokům. Klíčový bude také vývoj kapacit EU v oblasti reakce civilní ochrany (rescEU) na CBRN rizika. Pro posílení společné kultury bezpečnosti a zabezpečení v oblasti CBRN je také důležitá spolupráce s třetími zeměmi, při níž budou v plném rozsahu využita střediska excelence EU pro zmírňování globálních chemických, biologických, radiologických a jaderných rizik. Tato spolupráce bude zahrnovat posouzení nedostatků a rizik v jednotlivých zemích, podporu národních a regionálních akčních plánů v oblasti CBRN, výměnu osvědčených postupů a činnosti v oblasti budování kapacit pro zmírnění těchto rizik.

EU vypracovala nejvyspělejší právní předpisy na světě pro omezení přístupu k **prekurzorům výbušnin**[87] a odhalování podezřelých transakcí, jejichž cílem je výroba improvizovaných výbušných zařízení. Hrozba podomácku vyrobených výbušnin, které byly použity při mnoha útocích v celé EU, ale zůstává vysoká[88]. Prvním krokem musí být provedení předpisů a zajištění toho, aby internetové prostředí neumožňovalo obcházení kontrol.

---

[82] Pilotní iniciativa „Města EU proti radikalizaci“ má dvojí cíl: podpořit výměnu odborných znalostí mezi městy v EU a získat zpětnou vazbu ohledně toho, jak na úrovni EU co nejlépe podpořit místní komunity.

[83] Například financování v rámci Evropského fondu pro bezpečnost a programu Občanství.

[84] Programy EU jako Erasmus+ Virtuální výměny či e-twinning.

[85] V posledních dvou letech se například objevilo několik případů jak v Evropě (Francie, Německo, Itálie), tak i jinde (Tunisko, Indonésie), kdy byly použity biologické činitele (obvykle toxiny na bázi rostlin).

[86] Rada přijala omezující opatření proti šíření a používání chemických zbraní.

[87] Chemické látky, které by mohly být zneužity k výrobě podomácku vyrobených výbušnin. Jsou upraveny v nařízení (EU) 2019/1148 o uvádění prekurzorů výbušnin na trh a o jejich používání.

[88] Jako příklad těchto zničujících útoků lze uvést útoky v Oslu (2011), Paříži (2015), Bruselu (2016) a Manchesteru (2017). Při útoku s domácí výbušninou v Lyonu (2019) bylo zraněno 13 osob.

Důležitým prvkem politiky boje proti terorismu je rovněž účinné stíhání osob, které spáchaly teroristické trestné činy, včetně **zahraničních teroristických bojovníků**, kteří se nyní nacházejí v Sýrii a Iráku. Ačkoli tyto záležitosti řeší v prvé řadě členské státy, koordinace a podpora ze strany EU jim může pomoci společné problémy vyřešit. Důležitým krokem bude v plném rozsahu provést právní předpisy v oblasti bezpečnosti hranic[89] a plně využít všech důležitých databází EU pro sdílení informací o známých podezřelých osobách. Kromě identifikace vysoce rizikových osob je nutná politika opětovného začlenění a rehabilitace. Přeshraniční spolupráce, včetně s vězeňským a probačním personálem, pomůže soudům lépe pochopit procesy radikalizace vedoucí k násilnému extremismu a zlepšit přístup k ukládání trestů a alternativám k zadržení.

Problém zahraničních teroristických bojovníků je typickým projevem provázanosti vnitřní a **vnější bezpečnosti**. Proto má zásadní význam pro bezpečnost uvnitř EU spolupráce při prevenci terorismu, radikalizace a násilného extremismu a při jejich potírání[90]. Jsou zapotřebí další kroky k rozvoji partnerství a spolupráce při boji proti terorismu se zeměmi v sousedství i mimo něj, přičemž je třeba čerpat z odborných znalostí sítě odborníků EU na boj proti terorismu a bezpečnost. Dobrým příkladem takové cílené spolupráce je společný akční plán boje proti terorismu na západním Balkáně. Zejména je třeba pracovat na podpoře schopnosti partnerských zemí identifikovat a lokalizovat zahraniční teroristické bojovníky. EU bude rovněž nadále prosazovat mnohostrannou spolupráci a spolupracovat s předními světovými aktéry v této oblasti, jako jsou OSN, NATO, Rada Evropy, Interpol a OBSE. Bude rovněž spolupracovat s Globálním fórem pro boj proti terorismu, celosvětovou koalicí proti Dá'iš i s příslušnými zástupci občanské společnosti. Při spolupráci s třetími zeměmi v boji proti terorismu a pirátství hrají důležitou úlohu také nástroje vnější politiky Unie, včetně rozvoje a spolupráce. Mezinárodní spolupráce má zásadní význam též pro odříznutí všech zdrojů **financování terorismu**, například prostřednictvím Finančního akčního výboru.

Organizovaná trestná činnost

Organizovaná trestná činnost má obrovské ekonomické a osobní důsledky. Ekonomické ztráty způsobené organizovanou trestnou činností a korupcí se odhadují na 218 až 282 miliard EUR ročně[91]. V roce 2017 bylo v Evropě vyšetřováno více než 5 000 organizovaných zločineckých skupin, což ve srovnání s rokem 2013 představuje 50% nárůst[92]. Organizovaná trestná činnost stále více funguje přes hranice, a to i z bezprostředního sousedství EU, což vyžaduje intenzivnější operativní spolupráci a výměnu informací s partnery v sousedních zemích.

Objevují se nové problémy a trestné činy se stále více přesouvají na internet: během pandemie COVID-19 byl zaznamenán obrovský nárůst online podvodů cílených na zranitelné skupiny a krádeže a vloupání zaměřené na zdravotnické a hygienické výrobky[93]. EU potřebuje intenzivněji pracovat na boji proti organizované trestné činnosti i na mezinárodní úrovni a mít k dispozici více nástrojů na rozbití operačního modelu organizované kriminality. Boj proti organizované trestné činnosti vyžaduje rovněž úzkou

[89] Včetně nového mandátu Evropské agentury pro pohraniční a pobřežní stráž (Frontex).

[90] Rada ve svých závěrech ze dne 16. června 2020 zdůraznila, že je potřeba chránit občany EU před terorismem a násilným extremismem ve všech jejich formách a bez ohledu na jejich původ a dále posílit vnější činnosti a aktivity EU v oblasti boje proti terorismu v určitých prioritních zeměpisných a tematických oblastech.

[91] Vyjádřeno jako hrubý domácí produkt (HDP); zpráva Europolu: *Does crime still pay? – Criminal asset recovery in the EU* (Stále se zločin vyplácí? Vymáhání majetku z trestné činnosti v EU), 2016.

[92] Europol, posouzení závažných a organizovaných hrozeb (SOCTA), 2013 a 2017.

[93] Europol, 2020.

spolupráci s místními a regionálními správními orgány i s občanskou společností, které jsou klíčovými partnery v prevenci trestné činnosti i při poskytování pomoci a podpory obětem. Pomoc potřebují zejména orgány státní správy v pohraničních oblastech. Tato činnost bude sloučena v rámci **agendy pro potírání organizované trestné činnosti**.

Více než třetina organizovaných zločineckých skupin činných v EU se podílí na výrobě nebo distribuci drog a obchodování s nimi. V roce 2019 způsobila v EU závislost na drogách více než osm tisíc úmrtí v důsledku předávkování. S **drogami se obchoduje** převážně přes hranice, přičemž mnohé zisky jsou legalizovány[94]. Nová protidrogová agenda EU[95] podpoří úsilí EU a členských států, pokud jde o snižování poptávky po drogách a nabídky drog, vymezí společná opatření zaměřená na sdílené problémy a posílí dialog a spolupráci mezi EU a vnějšími partnery na téma drog. Po hodnocení Evropského monitorovacího centra pro drogy a drogovou závislost Komise posoudí, zda jeho mandát vyžaduje aktualizaci s cílem reagovat na nové výzvy.

Organizované zločinecké skupiny a teroristé jsou rovněž klíčovými aktéry v obchodu s **nelegálními palnými zbraněmi**. V letech 2009 až 2018 došlo v Evropě k 23 případům hromadné střelby, při nichž zahynulo více než 340 osob[96]. Palné zbraně jsou často pašovány do EU přes země v jejím bezprostředním sousedství[97]. Poukazuje to na potřebu posílit koordinaci a spolupráci uvnitř EU i s mezinárodními partnery, zejména s Interpolem, s cílem harmonizovat shromažďování informací a nahlašování zabavených palných zbraní. Je rovněž nezbytné zlepšit sledovatelnost zbraní, a to i na internetu, a zajistit výměnu informací mezi orgány, které provádějí registraci, a donucovacími orgány. Komise předkládá nový **akční plán EU proti nedovolenému obchodování s palnými zbraněmi**[98] a rovněž posoudí, zda pravidla pro vývozní povolení a režimy dovozu a vývozu palných zbraní nadále vyhovují svému účelu[99].

Zločinecké organizace zacházejí s migranty a s osobami, které potřebují mezinárodní ochranu, jako se zbožím. Příchod 90 % nelegálních migrantů do EU zprostředkovávají zločinecké sítě.[100] Převaděčství migrantů je také často spojeno s jinými formami organizované trestné činnosti, zejména s obchodováním s lidmi[101]. Europol odhaduje, že vedle ohromných ztrát na životech v důsledku obchodování s lidmi dosahuje celosvětově vytvořený roční zisk ze všech forem vykořisťování v rámci obchodování s lidmi 29,4 miliardy EUR. Jedná se o přeshraniční trestnou činnost s dopadem na všechny členské státy EU, která tyje z nezákonné poptávky v EU i mimo ni. Špatné výsledky v odhalování, stíhání a odsouzení těchto trestných činů vyžadují nový přístup, který povede k intenzivnější činnosti. Nový, **komplexní přístup k obchodování s lidmi** propojí různé směry činnosti. Kromě toho Komise předloží **nový akční plán EU proti pašování migrantů** na období 2021–2025. Obě složky se zaměří na boj proti zločineckým sítím, posílení spolupráce a na podporu činnosti v oblasti prosazování práva.

---

94 Zpráva EMCDDA a Europolu o trzích s drogami v EU za rok 2019 (listopad 2019).

95 Protidrogová agenda a akční plán EU na období 2021–2025, COM(2020) 606.

96 Flemish Peace Institute, *Armed to kill* (Mám zbraň a budu zabíjet) (říjen 2019).

97 EU financuje boj proti šíření ručních palných a lehkých zbraní a obchodování s nimi v regionu od roku 2002, například financuje síť odborníků ze zemí jihovýchodní Evropy na palné zbraně (SEEFEN). Partneři ze západního Balkánu jsou od roku 2019 plně zapojeni do prioritní činnosti evropské multidisciplinární platformy pro boj proti hrozbám vyplývajícím z trestné činnosti (EMPACT) týkající se palných zbraní.

98 COM(2020) 608.

99 Nařízení (EU) č. 258/2012, kterým se provádí článek protokolu 10 Organizace spojených národů proti nedovolené výrobě střelných zbraní a obchodování s nimi.

100 Zdroj: Europol.

101 Europol, Evropské středisko pro boj proti převaděčství, 4. výroční zpráva.

Organizované zločinecké skupiny a stejně tak teroristé hledají také příležitosti v jiných oblastech, zejména pak těch, které vykazují vysokou ziskovost s nízkým rizikem odhalení, jako je například **trestná činnost proti životnímu prostředí**. Nezákonný lov a sběr volně žijících a planě rostoucích druhů a obchod s nimi, nelegální těžba surovin a nezákonná těžba dřeva, nelegální likvidace a přeprava odpadů se staly čtvrtou největší nezákonnou činností na světě[102]. Ke kriminálním účelům byl rovněž zneužit systém obchodování s emisemi a systém energetických osvědčení, ale i finanční prostředky vyčleněné na environmentální odolnost a udržitelný rozvoj. Kromě podpory činnosti EU, členských států a mezinárodního společenství s cílem intenzivněji potírat trestnou činnost proti životnímu prostředí[103] Komise nyní vyhodnocuje, zda nadále plní svůj účel směrnice o trestněprávní ochraně životního prostředí[104]. Na vzestupu je **obchod s kulturními statky**, který se rovněž stal jednou z nejlukrativnějších kriminálních činností a slouží k financování teroristů i organizované trestné činnosti. Měly by se prozkoumat kroky, jak zlepšit sledovatelnost kulturních statků na vnitřním trhu na internetu i mimo něj, jak zkvalitnit spolupráci s třetími zeměmi, v nichž k rabování kulturních statků dochází, a jak poskytovat aktivní podporu donucovacím orgánům a akademickým obcím.

Hospodářská a finanční trestná činnost je velmi složitá, avšak každoročně zasáhne miliony občanů a tisíce podniků v EU. Boj proti podvodům je zásadní a vyžaduje opatření na úrovni EU. Europol a spolu s ním Eurojust, Úřad evropského veřejného žalobce a Evropský úřad pro boj proti podvodům pomáhají členským státům a EU při ochraně hospodářských a finančních trhů a peněz daňových poplatníků v EU. Úřad evropského veřejného žalobce zahájí plný provoz koncem roku 2020 a bude vyšetřovat, stíhat a stavět před soud trestné činy poškozující rozpočet EU, jako jsou podvody, korupce a praní peněz. Zabývat se bude i přeshraničními daňovými podvody v oblasti DPH, které daňové poplatníky každý rok stojí nejméně 50 miliard EUR.

Komise rovněž podpoří rozvoj odborných znalostí a legislativního rámce pro nové rizikové oblasti, jaké představují například kryptoaktiva a nové platební systémy. Zaměří se zejména na to, jak reagovat na objevující se kryptoaktiva, jako je bitcoin, a na účinek těchto nových technologií na způsob vydávání finančních aktiv, jejich výměnu, sdílení a přístup k nim.

V Evropské unii by měla existovat nulová tolerance vůči nezákonným penězům. Během třiceti let vypracovala EU solidní regulační rámec pro předcházení **praní peněz** a financování terorismu a boj proti nim, který plně respektuje nutnost ochrany osobních údajů. Panuje však stále větší shoda na tom, že provádění stávajícího rámce je třeba výrazně zlepšit. Je třeba odstranit významné rozdíly ve způsobu jeho uplatňování a závažné nedostatky při prosazování pravidel. Jak je podrobně uvedeno v akčním plánu z května 2020[105], pracuje se na posouzení možností, jak rámec EU pro boj proti praní peněz a financování terorismu posílit. Je potřeba vyhodnotit například propojení vnitrostátních centralizovaných registrů bankovních účtů, které by mohlo výrazně urychlit přístup finančních zpravodajských jednotek a příslušných orgánů k finančním informacím.

Zisky organizovaných zločineckých skupin v EU se odhadují na 110 miliard EUR ročně. Nyní podnikané kroky zahrnují harmonizaci právních předpisů pro vyhledávání a konfiskaci

[102] UNEP-INTERPOL *Rapid Response Assessment*: *The Rise of Environmental Crime* (Posouzení rychlé reakce EUEP-INTERPOL: Nárůst environmentální trestné činnosti), červen 2016.
[103] Viz Zelená dohoda pro Evropu, COM(2019) 640 final.
[104] Směrnice 2008/99/ES o trestněprávní ochraně životního prostředí.
[105] Akční plán pro předcházení praní peněz a financování terorismu, COM(2020) 2800.

majetku[106], zlepšení zmrazování a konfiskace majetku pocházejícího z trestné činnosti v EU a podporování vzájemné důvěry a účinné přeshraniční spolupráce mezi členskými státy. Zabaveno je však přibližně pouze 1 % těchto zisků[107], což organizovaným zločineckým skupinám umožňuje investovat do rozšiřování trestné činnosti a pronikat do legální ekonomiky. Hlavním terčem praní peněz jsou zejména malé a střední podniky, které mají obtížný přístup k úvěrům. Komise provede analýzu provádění právních předpisů[108] a případné potřeby dalších společných pravidel, včetně pro konfiskaci bez odsouzení pachatele. Aby se zvýšila míra konfiskací, úřady pro vyhledávání majetku z trestné činnosti[109], které jsou hlavním prvkem procesu vymáhání majetku, by navíc mohly být vybaveny lepšími nástroji k rychlejšímu zjišťování a vysledování majetku v EU.

Existuje silná vazba mezi organizovanou trestnou činností a **korupcí**. Hrubé odhady hovoří o tom, že jen samotná korupce stojí hospodářství EU 120 miliard EUR ročně[110]. Prevence a boj proti korupci budou i nadále pravidelně monitorovány v rámci mechanismu právního státu i v procesu evropského semestru. V evropském semestru jsou posuzovány problémy v boji proti korupci, které se týkají například zadávání veřejných zakázek, veřejné správy, podnikatelského prostředí nebo zdravotní péče. Boji proti korupci se bude věnovat i nová výroční zpráva Komise o stavu právního státu, která umožní preventivní konzultace s vnitrostátními orgány a zainteresovanými stranami na úrovni EU a na vnitrostátní úrovni. Organizace občanské společnosti mohou rovněž hrát zásadní úlohu, pokud jde o stimulaci činnosti orgánů veřejné správy při předcházení organizované trestné činnosti a korupci a boji proti nim, a proto by mohlo být užitečné, kdyby se spojily na společném fóru. Vzhledem k jejich přeshraničnímu charakteru je dalším rozhodujícím prvkem spolupráce s regiony, které sousedí s EU, a pomoc těmto regionům.

Klíčová opatření
• Protiteroristická agenda pro EU, včetně obnovených opatření proti radikalizaci v EU • Nová spolupráce s klíčovými třetími zeměmi a mezinárodními organizacemi v boji proti terorismu • Agenda pro potírání organizované trestné činnosti, včetně obchodování s lidmi • Protidrogová agenda a akční plán EU na období 2021–2025 • Posouzení Evropského monitorovacího centra pro drogy a drogovou závislost • Akční plán EU proti nedovolenému obchodování s palnými zbraněmi na období 2020–2025 • Přezkum právních předpisů týkajících se zajišťování a konfiskace a úřadů pro vyhledávání majetku z trestné činnosti • Posouzení směrnice o trestněprávní ochraně životního prostředí • Akční plán EU proti pašování migrantů na období 2021–2025

[106] Podle práva EU musí být úřady pro vyhledávání majetku z trestné činnosti zřízeny ve všech členských státech.

[107] Zpráva o vyhledávání a konfiskaci majetku: zajištění toho, aby se trestná činnost nevyplácela, COM(2020) 217.

[108] Směrnice 2014/42/EU o zajišťování a konfiskaci nástrojů a výnosů z trestné činnosti v Evropské unii.

[109] Rozhodnutí Rady 2007/845/SVV o spolupráci mezi úřady pro vyhledávání majetku z trestné činnosti v jednotlivých členských státech v oblasti vysledování a identifikace výnosů z trestné činnosti nebo jiného majetku v souvislosti s trestnou činností.

[110] Odhadnout celkové ekonomické náklady korupce je obtížné, nicméně podle organizací, jako je Mezinárodní obchodní komora, Transparency International, OSN v rámci globálního paktu a Světové ekonomické fórum, dosahuje hodnota korupce 5 % světového HDP.

4. Silný evropský bezpečnostní ekosystém

Skutečná a účinná bezpečnostní unie musí být společným dílem všech složek společnosti. Veřejná správa, donucovací orgány, soukromý sektor, vzdělávací instituce a samotní občané musí být angažováni, vybaveni a řádně propojeni s cílem rozvíjet připravenost a odolnost všech, zejména těch nejzranitelnějších, obětí a svědků.

Všechny politiky potřebují bezpečnostní rozměr a EU může přispět na všech úrovních. Domácí násilí je jedním z nejzávažnějších bezpečnostních rizik v domácnosti. V EU zažilo 22 % žen násilí ze strany svého partnera[111]. Přistoupení EU k Istanbulské úmluvě o prevenci a potírání násilí vůči ženám a domácího násilí zůstává klíčovou prioritou. Pokud by jednání zůstala zablokována, přijme Komise jiná opatření k dosažení stejných cílů, jaké má úmluva, například navrhne doplnit násilí páchané na ženách do seznamu unijních trestných činů definovaných ve Smlouvě.

Spolupráce a výměna informací

Jedním z nejdůležitějších příspěvků EU k ochraně občanů může být, že přispěje k řádné spolupráci subjektů odpovědných za bezpečnost. Spolupráce a sdílení informací jsou nejsilnějšími nástroji pro boj proti trestné činnosti a terorismu a pro výkon spravedlnosti. Aby byly účinné, musí být cílené a včasné. Aby byly důvěryhodné, musí být doplněny o společné záruky a kontroly.

V zájmu dalšího rozvoje **operativní spolupráce v oblasti prosazování práva** byla vytvořena řada unijních nástrojů a strategií pro jednotlivá odvětví[112]. Jedním z hlavních nástrojů EU na podporu spolupráce mezi členskými státy v oblasti prosazování práva je Schengenský informační systém, který se používá k výměně údajů o hledaných a pohřešovaných osobách a věcech v reálném čase. Jeho přínos se projevil v zatýkání pachatelů trestné činnosti, zabavování drog a záchraně potenciálních obětí[113]. Úroveň spolupráce by se však mohla ještě zlepšit zefektivněním a modernizací dostupných nástrojů. Většina právního rámce EU, o nějž se operativní spolupráce v oblasti prosazování práva opírá, byla vytvořena před 30 lety. Složité předivo dvoustranných dohod mezi členskými státy, mnoha z nich zastaralých či nedostatečně využívaných, může vést k roztříštěnosti. V menších nebo vnitrozemských státech musí příslušníci donucovacích orgánů, kteří pracují i za hranicemi, provádět operativní činnosti v některých případech až podle sedmi různých souborů pravidel s tím výsledkem, že některé operace, např. přeshraniční pronásledování podezřelých osob přes vnitřní hranice, se jednoduše neuskutečňují. Operativní spolupráce s využitím nových technologií, např. dronů, také není současným rámcem EU upravena.

Operativní účinnost lze zvýšit prostřednictvím konkrétní spolupráce v oblasti prosazování práva, která může rovněž pomoci poskytnout klíčovou podporu pro další politické cíle, jako je nové posuzování přímých zahraničních investic z hlediska bezpečnosti. Komise vyhodnotí, jak by mohl přispět kodex policejní spolupráce. Donucovací orgány členských států využívají rostoucí měrou podporu a odborné znalosti na úrovni EU, přičemž důležitou roli při prosazování výměny strategických informací mezi zpravodajskými a bezpečnostními složkami členských států, které poskytují zpravodajské informace o situaci orgánům EU,

[111] Unie rovnosti: Strategie pro rovnost žen a mužů na období 2020–2025, COM(2020) 152.

[112] Například akční plán Strategie Evropské unie pro námořní bezpečnost, který přinesl značné výsledky díky spolupráci mezi příslušnými agenturami EU při výkonu funkcí pobřežní stráže.

[113] Boj EU proti organizované trestné činnosti v roce 2019 (Rada, 2020).

hraje Zpravodajské a informační centrum EU[114]. **Europol** může také zásadně pomoci tím, že rozšíří spolupráci s třetími zeměmi v boji proti trestné činnosti a terorismu v souladu s jinými vnějšími politikami a nástroji EU. V současnosti se však potýká s celou řadou vážných překážek, zejména pokud jde o přímou výměnu osobních údajů se soukromými subjekty, což této agentuře zabraňuje členským státům v boji proti terorismu a trestné činnosti účinně pomáhat. Nyní se vyhodnocuje, jak zlepšit mandát Europolu, aby dokázal plnit své úkoly v plném rozsahu. V této souvislosti by měly příslušné orgány na úrovni EU (např. úřad OLAF, Europol, Eurojust a Úřad evropského veřejného žalobce) intenzivněji spolupracovat a zlepšit výměnu informací.

Jiným důležitým aspektem je další rozvoj **Eurojustu** s cílem maximalizovat součinnost mezi spoluprací v oblasti prosazování práva a justiční spoluprací. EU by rovněž těžila z větší strategické soudržnosti: **EMPACT**[115], politický cyklus EU pro boj proti organizované a závažné mezinárodní trestné činnosti, dává příslušným orgánům metodiku trestné činnosti založenou na zpravodajství, aby mohly společně řešit nejvýznamnější kriminální hrozby postihující EU. V posledním desetiletí přinesl značné operativní výsledky[116]. Na základě zkušeností odborníků z praxe by se měl stávající mechanismus zefektivnit a zjednodušit tak, aby v novém politickém cyklu 2022–2025 dokázal úspěšněji řešit nejnaléhavější a nové hrozby trestné činnosti.

Pro každodenní stíhání trestné činnosti jsou nezbytné včasné a relevantní **informace**. I přes vytvoření nových celounijních databází pro bezpečnost a správu hranic se mnohé informace stále nacházejí v databázích jednotlivých zemí nebo se vyměňují mimo tyto nástroje. Tato situace způsobuje významnou dodatečnou pracovní zátěž, prodlevy a zvýšené riziko přehlédnutí klíčových informací. Lepší, rychlejší a jednodušší postupy, do nichž by byla zapojena celá bezpečnostní komunita, by přinesly lepší výsledky. Správné nástroje jsou nutné, má-li se plně využít potenciál výměny informací pro účinné stíhání trestné činnosti, přičemž se musí uplatňovat nezbytné záruky s cílem dodržovat při sdílení údajů právní předpisy o ochraně údajů a základní práva. S ohledem na technologický vývoj, forenzní vývoj, vývoj v ochraně údajů a na změněné operativní potřeby by EU mohla zvážit, zda není potřeba modernizovat nástroje, jako jsou **prümská rozhodnutí z roku 2008**, zavést automatizovanou výměnu údajů o DNA, otiscích prstů a registraci vozidel či zda neumožnit automatizovanou výměnu dalších kategorií údajů, které jsou již k dispozici v trestních či jiných databázích členských států pro účely vyšetřování. Komise vedle toho posoudí možnost výměny policejních záznamů, která by pomohla určit, zda v jiných členských státech neexistuje o dané osobě policejní záznam, a možnost zjednodušit přístup k těmto záznamům po jejich nalezení za dodržení všech nezbytných záruk.

Informace o cestujících pomohly zlepšit hraniční kontroly, snížit nelegální migraci a identifikovat osoby, které představují bezpečnostní rizika. Předběžné informace o cestujících jsou biografické údaje, které letečtí dopravci shromažďují o každém cestujícím při odbavení a předem zasílají orgánům hraniční kontroly v cílovém místě. Revize právního rámce[117] by umožnila tyto informace účinněji využívat, zajistila zároveň soulad s právními předpisy o ochraně údajů a zjednodušila tok cestujících. Jmenná evidence cestujících (PNR) jsou údaje poskytované cestujícími při nákupu letenek. Zásadně důležité je provedení směrnice o

[114] Zpravodajské a informační centrum EU (EU INTCEN) slouží jako jediná brána pro zpravodajské a bezpečnostní služby členských států, které Evropské unii poskytují zpravodajské poznatky o situaci.

[115] EMPACT je zkratka pro evropskou multidisciplinární platformu pro boj proti hrozbám vyplývajícím z trestné činnosti.

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf

[117] Směrnice Rady 2004/82/ES o povinnosti dopravců předávat údaje o cestujících.

jmenné evidenci cestujících[118], které bude Komise i nadále podporovat a prosazovat. Kromě toho Komise jakožto opatření v polovině období zahájí přezkum stávajícího přístupu k **předávání údajů PNR třetím zemím**.

Justiční spolupráce je nezbytným doplňkem úsilí policie v boji proti přeshraniční trestné činnosti. V posledních 20 letech prošla poměrně hlubokou proměnou. Subjekty, jako je **Úřad evropského veřejného žalobce** a **Eurojust**, musí mít prostředky k tomu, aby mohly fungovat v plném rozsahu, nebo bude třeba je posílit. Rovněž by mohla být posílena spolupráce mezi pracovníky justice prostřednictvím dalších kroků v oblasti vzájemného uznávání soudních rozhodnutí, justičního vzdělávání a výměny informací. Cílem by mělo být zvýšení vzájemné důvěry mezi soudci a státními zástupci, které je zásadní pro hladký průběh přeshraničních řízení. Účinnost soudních systémů v Evropské unii může také zlepšit využívání **digitálních technologií**. Za podpory Eurojustu se buduje nový systém digitální výměny pro předávání evropských vyšetřovacích příkazů, žádostí o vzájemnou právní pomoc a související komunikaci mezi členskými státy. Komise bude spolupracovat s členskými státy na rychlejším zavedení potřebných systémů IT na vnitrostátní úrovni.

Mezinárodní spolupráce je také klíčová pro efektivní spolupráci v oblasti prosazování práva a justiční spolupráci. Dvoustranné dohody s klíčovými partnery hrají hlavní úlohu při zajišťování informací a důkazů mimo EU. Důležitou úlohu hraje **Interpol**, jedna z největších mezivládních organizací kriminální policie. Komise prozkoumá možné způsoby posílení spolupráce s Interpolem, včetně možného přístupu do jeho databází a posílení operativní a strategické spolupráce. Donucovací orgány v EU se při odhalování a vyšetřování zločinců včetně teroristů rovněž opírají o důležité partnerské země. V zájmu posílení spolupráce v boji proti společným hrozbám, jako je terorismus, organizovaná trestná činnost, kyberkriminalita, pohlavní zneužívání dětí a obchodování s lidmi, by mohla být posílena **bezpečnostní partnerství mezi EU a třetími zeměmi**. Tento postup by byl založen na společných bezpečnostních zájmech a stavěl by na zavedených jednáních o spolupráci a bezpečnosti.

Stejně jako výměna informací může být pro zvyšování připravenosti donucovacích orgánů na **netradiční hrozby** obzvláště cenná výměna odborných znalostí. Komise vedle prosazování výměny osvědčených postupů posoudí vytvoření případného **koordinačního mechanismu na úrovni EU pro policejní síly**, který by se aktivoval v případě událostí vyšší moci, jako jsou pandemie. Nynější pandemie rovněž prokázala, že v boji proti trestné činnosti a terorismu bude mít zásadní význam policejní služba veřejnosti v digitálním prostoru ve spojení s právním rámcem pro usnadnění činnosti policie na internetu. Partnerství mezi policií a komunitami, mimo jiné i online, může předcházet trestné činnosti a snižovat vliv organizované trestné činnosti, radikalizace a terorismu. Klíčovým faktorem úspěchu pro bezpečnostní unii EU jako celek je propojení policejních řešení od místních přes regionální a celostátní až po ta unijní.

Přínos silných vnějších hranic

Moderní a účinná správa vnějších hranic má dvojí přínos: zachování integrity schengenského prostoru a zajištění bezpečnosti občanů. Zapojení všech příslušných aktérů s cílem co nejvíce zvýšit bezpečnost na hranicích může opravdu pomoci při předcházení přeshraniční trestné činnosti a terorismu. K předcházení a odhalování přeshraniční trestné činnosti na **vnějších hranicích** a mimo EU přispívají společné operativní činnosti nedávno

[118] Směrnice 2016/681 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.

posílené Evropské pohraniční a pobřežní stráže[119]. Pro boj proti přeshraniční trestné činnosti a terorismu jsou také zásadní celní činnosti spočívající v odhalování bezpečnostních rizik u veškerého zboží před jeho příjezdem do EU a v kontrole zboží při příjezdu. V připravovaném akčním plánu pro celní unii budou oznámena opatření zaměřená mimo jiné na zlepšení řízení rizik a posílení vnitřní bezpečnosti, zejména bude posouzena proveditelnost propojení příslušných informačních systémů pro analýzu bezpečnostních rizik.

V květnu 2019 byl přijat rámec pro **interoperabilitu mezi informačními systémy EU** v oblasti spravedlnosti a vnitřních věcí. Cílem této nové struktury je zlepšit účinnost a účelnost nových nebo modernizovaných informačních systémů[120]. Příslušníci donucovacích orgánů, pohraniční stráže a migrační úředníci budou díky ní rychleji a systematičtěji informováni. Napomůže správnému určování totožnosti a přispěje k potírání podvodného zneužívání totožnosti. Aby se nová struktura stala skutečností, mělo by být zavedení interoperability prioritou na politické i technické úrovni. Pro dosažení cíle plné interoperability do roku 2023 bude rozhodující úzká spolupráce mezi agenturami EU a všemi členskými státy.

Podvody s cestovními doklady jsou považovány za jeden z nejčastěji páchaných trestných činů. Umožňují nelegální pohyb zločinců včetně teroristů a hrají klíčovou úlohu v obchodování s lidmi a s drogami[121]. Komise prozkoumá, jak rozšířit stávající práci na bezpečnostních normách pro doklady o pobytu a cestovní doklady platné v EU, a to i prostřednictvím digitalizace. Od srpna 2021 začnou členské státy vydávat průkazy totožnosti a povolení k pobytu podle harmonizovaných bezpečnostních norem a tyto doklady budou obsahovat také čip s biometrickými identifikátory, které mohou ověřovat všechny pohraniční orgány v EU. Komise bude sledovat plnění těchto nových pravidel, včetně postupného nahrazování dokladů, které jsou nyní v oběhu.

Posílení výzkumu a inovací v oblasti bezpečnosti

Práce na zajištění kybernetické bezpečnosti a boj proti organizované trestné činnosti, kyberkriminalitě a terorismu do značné míry závisejí na vývoji nových nástrojů. Jejich úkolem bude pomoci vytvořit bezpečnější a lépe zabezpečené nové technologie, řešit výzvy související s technologiemi a podporovat práci v oblasti prosazování práva, přičemž je nutno se opřít o soukromé partnery a průmyslová odvětví.

Inovace by měly být považovány za strategický prostředek pro boj proti současným hrozbám a pro předvídání budoucích rizik a příležitostí. Inovativní technologie mohou přinést nové nástroje, které pomohou donucovacím orgánům a dalším aktérům v oblasti bezpečnosti. Umělá inteligence a analýza dat velkého objemu by mohly využívat vysoce výkonnou výpočetní techniku k lepšímu odhalování hrozeb a k rychlé a komplexní analýze[122]. Klíčovou podmínkou pro vývoj spolehlivých technologií je, aby příslušné orgány měly k dispozici vysoce kvalitní soubory údajů pro přípravu, testování a schvalování

[119] Ta je složena z Evropské agentury pro pohraniční a pobřežní stráž (Frontex), orgánů pohraniční stráže členských států a orgánů pobřežní stráže.

[120] Systém vstupu/výstupu (EES), Evropský systém pro cestovní informace a povolení (ETIAS), rozšířený Evropský informační systém rejstříků trestů (ECRIS-TCN), Schengenský informační systém, Vízový informační systém a budoucí aktualizovaný Eurodac.

[121] Vztah mezi podvody s doklady a obchodováním s lidmi je popsán ve druhé zprávě o pokroku dosaženém v oblasti boje proti obchodování s lidmi, COM(2018) 777, v připojeném SWD(2018) 473 a v situační zprávě Europolu o obchodování s lidmi v EU z roku 2016.

[122] Při tom je třeba stavět na strategii Komise pro umělou inteligenci.

algoritmů[123]. Obecněji řečeno, riziko technologické závislosti je v dnešní době silné – EU je například čistým dovozcem produktů a služeb v oblasti kybernetické bezpečnosti, což má důsledky pro hospodářství a kritické infrastruktury. K ovládnutí technologií a zajištění kontinuity dodávek i v případě nepříznivých událostí a krizí musí být Evropa přítomna v kritických částech příslušných hodnotových řetězců a mít odpovídající kapacitu.

Výzkum, inovace a technologický vývoj v EU nabízejí příležitost zohlednit bezpečnostní rozměr při vývoji technologií a během jejich používání. Významný impuls může dát příští generace návrhů EU na financování[124]. Iniciativy zaměřené na evropské datové prostory a cloudové infrastruktury počítají se zabezpečením již od počáteční fáze. Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center[125] mají za cíl vytvořit účinnou a účelnou strukturu pro sdružování a sdílení výzkumných kapacit a výsledků v oblasti kybernetické bezpečnosti. Kosmický program EU nabízí služby na podporu bezpečnosti EU, jejích členských států i soukromých osob[126].

Výzkum v oblasti bezpečnosti financovaný z prostředků EU je s více než 600 projekty v celkové hodnotě téměř 3 miliardy EUR zahájenými od roku 2007 klíčovým motorem technologií a znalostí, které lze využít pro bezpečnostní řešení. V rámci přezkumu mandátu Europolu posoudí Komise vytvoření **Evropského inovačního centra pro vnitřní bezpečnost**[127], které by pracovalo na společných řešeních pro sdílené bezpečnostní výzvy a na využití příležitostí, kterých by členské státy nedokázaly využít samostatně. Spolupráce má zásadní význam pro zacílení investic nejúčinnějším směrem a pro vývoj inovativních technologií s přínosem pro bezpečnost a hospodářství.

Dovednosti a zvyšování informovanosti

Pro vybudování odolnější společnosti s lépe připravenými podniky, správními orgány a jednotlivci je zásadní informovanost o bezpečnostních otázkách a získání dovedností potřebných k řešení potenciálních hrozeb. Problémy v souvislosti s infrastrukturou IT a elektronickými systémy potvrdily, že musíme zlepšit naši schopnost zajistit kybernetickou bezpečnost a odpovídající reakci. Pandemie rovněž zdůraznila význam digitalizace ve všech oblastech hospodářství a ve všech složkách společnosti v EU.

Byť jen **základní znalost bezpečnostních hrozeb** a jejich potírání může zvýšit odolnost celé společnosti. Povědomí o rizicích kybernetické kriminality a nutnosti se před ní chránit může účinkovat společně s ochranou, kterou před kybernetickými útoky nabízejí poskytovatelé služeb. Informace o nebezpečích a rizicích obchodu s drogami mohou zločincům ztížit úspěch. EU může stimulovat šíření osvědčených postupů, například

[123] Evropská strategie pro data, COM(2020) 66 final.

[124] Komise bude v návrzích týkajících se programu Horizont Evropa, Fondu pro vnitřní bezpečnost, Fondu pro integrovanou správu hranic, fondu EU Invest, Evropského fondu pro regionální rozvoj a programu Digitální Evropa podporovat vývoj a zavádění inovativních bezpečnostních technologií a řešení v celém hodnotovém řetězci v oblasti bezpečnosti.

[125] Návrh nařízení ze dne 12. září 2018, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, COM(2018) 630.

[126] Například program Copernicus poskytuje služby, které umožňují dohled nad vnějšími hranicemi EU a námořní dohled, což pomáhá v boji proti pirátství a pašování/převaděčství a při podpoře kritických infrastruktur. Jakmile bude program plně funkční, bude klíčovým prostředkem pro civilní i vojenské mise a operace.

[127] Centrum by spolupracovalo také s Evropskou pohraniční a pobřežní stráží / Frontexem, agenturami CEPOL a eu-LISA a se Společným výzkumným střediskem.

prostřednictvím sítě center pro bezpečnější internet[128], a zajistit, aby tyto cíle byly zapracovány do jejích vlastních programů.

Připravovaný akční plán digitálního vzdělávání by měl obsahovat opatření zaměřená na rozvoj informatických dovedností celé populace v oblasti bezpečnosti. Nedávno přijatá agenda dovedností[129], která podporuje celoživotní rozvoj dovedností, počítá se zvláštními opatřeními na zvýšení počtu absolventů přírodovědných, technických, inženýrských, uměleckých a matematických oborů potřebných ve špičkových oblastech, jako je právě kybernetická bezpečnost. Další opatření, financovaná z programu Digitální Evropa, umožní odborníkům držet krok s vývojem podoby bezpečnostních hrozeb a zároveň řešit nedostatek pracovních sil v tomto oboru na pracovním trhu v EU. Lidé tak budou moci získat dovednosti, které jim umožní čelit bezpečnostním hrozbám, a podniky naleznou odborníky, které v této oblasti potřebují. Profesní dráhy v oblasti přírodních věd, technologií, inženýrství, umění a matematiky budou propagovány i v rámci budoucího Evropského výzkumného prostoru a Evropského prostoru vzdělávání.

Důležitý je také přístup **obětí** k jejich právům: oběti musí obdržet potřebnou pomoc a cílenou podporu. Je třeba se zaměřit zejména na menšiny a nejzranitelnější oběti, např. děti nebo ženy, které se staly oběťmi obchodování s lidmi za účelem sexuálního vykořisťování nebo jsou vystaveny domácímu násilí[130].

Obzvláštní význam má zvyšování **dovedností v oblasti prosazování práva**. Současné a nové technologické hrozby si žádají více investic do prohlubování dovedností pracovníků donucovacích orgánů v co nejranější fázi a po celou dobu jejich profesní dráhy. Důležitým partnerem, který pomáhá členským státům při plnění tohoto úkolu, je Evropská policejní akademie (CEPOL). Vzdělávání a výcvik v oblasti prosazování práva zaměřené na rasismus a xenofobii a obecněji na práva občana musí být nezbytnou součástí kultury bezpečnosti v EU. Vnitrostátní soudní systémy a justiční odborníci musí být rovněž vybaveni k tomu, aby se přizpůsobili nebývalým výzvám a dokázali na ně reagovat. Vzdělávání a výcvik mají zásadní podíl na tom, aby příslušné orgány využívaly těchto nástrojů v operační situaci. Také je nutné vyvinout veškeré úsilí k intenzivnějšímu začleňování hledisek rovnosti žen a mužů do všech oblastí a posílit účast žen na prosazování práva.

Klíčová opatření
• Posílení mandátu Europolu • Posouzení kodexu EU pro policejní spolupráci a policejní koordinace za krizových situací • Posílení vazby Eurojustu na soudy a donucovací orgány • Revize směrnice o předběžných informacích o cestujících • Sdělení o vnějším rozměru jmenné evidence cestujících • Posílení spolupráce mezi EU a Interpolem • Rámec pro jednání s klíčovými třetími zeměmi o sdílení informací • Lepší bezpečnostní normy pro cestovní doklady

[128] Viz www.betterinternetforkids.eu: ústřední portál a národní centra pro bezpečnější internet jsou nyní financovány ze složky Nástroje pro propojení Evropy pro telekomunikace, další financování bylo navrženo z programu Digitální Evropa.

[129] Evropská agenda dovedností pro udržitelnou konkurenceschopnost, sociální spravedlnost a odolnost, COM(2020) 274 final.

[130] Viz strategie pro rovnost žen a mužů, COM(2020) 152, strategie v oblasti práv obětí, COM(2020) 258, a Evropská strategie pro internet lépe uzpůsobený dětem, COM(2012) 196.

- Posouzení možnosti zřídit evropské inovační centrum pro vnitřní bezpečnost

V. Závěr

V čím dál bouřlivějším světě je Evropská unie stále obecně považována za jedno z nejbezpečnějších míst na světě. Nelze to však považovat za samozřejmost.

Nová strategie bezpečnostní unie vytváří základy pro bezpečnostní ekosystém, který obsahuje evropskou společnost v celé její šíři, a je založena na vědomí, že za bezpečnost nesou odpovědnost všichni, protože se týká každého z nás. Aby naše společnost byla bezpečnější, musí vlastní povinnosti plnit všechny orgány státní správy, podniky, sociální organizace, instituce i občané.

Bezpečnostní otázky je nyní třeba vnímat z mnohem širšího pohledu než v minulosti. Musí přestat nepatřičné rozlišování mezi fyzickým a digitálním prostředím. Strategie bezpečnostní unie EU propojuje celé spektrum potřeb v oblasti bezpečnosti a zaměřuje se na oblasti, které jsou v nadcházejících letech pro bezpečnost EU nejdůležitější. Rovněž se v ní uznává, že bezpečnostní hrozby nerespektují zeměpisné hranice a že vnitřní a vnější bezpečnost jsou stále více provázány[131]. V této souvislosti bude důležité, aby EU spolupracovala s mezinárodními partnery na ochraně všech občanů EU a aby provádění této strategie úzce koordinovala se svou vnější činností.

Naše bezpečnost je vázána na naše základní hodnoty. Všechna navrhovaná opatření a iniciativy v této strategii budou základní práva a evropské hodnoty plně respektovat, protože jsou základem našeho evropského způsobu života a musí zůstat ústředním prvkem veškeré naší práce.

Komise si je nadále plně vědoma, že každá politika či opatření jsou jen tak dobré, jak dobré je jejich provádění a prosazování. Proto je potřeba klást neustálý důraz na řádné provádění a prosazování stávajících i budoucích právních předpisů, které budou sledovány v pravidelných zprávách o bezpečnostní unii. Komise bude vždy plně informovat Evropský parlament, Radu a zúčastněné strany a zapojí je do všech příslušných opatření. Dále je Komise připravena podílet se na společných diskusích s ostatními orgány Evropské unie o strategii bezpečnostní unie a tyto diskuse organizovat, aby mohly společně zhodnotit dosažený pokrok a současně se zaměřit na budoucí výzvy.

Komise vyzývá Evropský parlament a Radu, aby tuto strategii bezpečnostní unie schválily jako základ spolupráci a společnou činnost v oblasti bezpečnosti v následujících pěti letech.

[131] Viz globální strategie EU.