EURÓPSKA
KOMISIA

V Bruseli 24. 7. 2020
COM(2020) 605 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, EURÓPSKEJ RADE, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV

o stratégii EÚ pre bezpečnostnú úniu

I. Úvod

V politických usmerneniach Komisie sa jasne uvádza, že pre ochranu našich občanov musíme urobiť úplne všetko. Bezpečnosť nie je len základom osobnej ochrany, ale takisto ochraňuje základné práva a predstavuje základ pre istotu a dynamiku v našom hospodárske, našej spoločnosti a našej demokracii. Európania dnes čelia meniacej sa bezpečnostnej situácii, ktorú ovplyvňujú vyvíjajúce sa hrozby, ako aj iné faktory, medzi ktoré patrí zmena klímy, demografické trendy a politická nestabilita za našimi hranicami. Globalizácia, voľný pohyb a digitálna transformácia naďalej prinášajú prosperitu, uľahčujú nám život a podnecujú inovácie a rast. S týmito prínosmi sú však neoddeliteľne späté riziká a náklady. Môžu byť zmanipulované terorizmom, organizovanou trestnou činnosťou, obchodom s drogami a obchodovaním s ľuďmi, čo sú všetko priame hrozby pre občanov a náš európsky spôsob života. Zvyšuje sa výskyt kybernetických útokov a počítačovej kriminality. Bezpečnostné hrozby sa takisto stávajú čoraz komplexnejšími: prekvitajú vďaka schopnosti fungovať naprieč hranicami a na základe prepojenosti, využívajú stieranie hraníc medzi fyzickým a digitálnym svetom a využívajú zraniteľné skupiny a sociálne a ekonomické rozdiely. Útoky môžu prísť v momente a môžu za sebou zanechať len nepatrnú alebo žiadnu stopu, štátne aj neštátne subjekty môžu vytvoriť celý rad hybridných hrozieb[1] a to, čo sa stane mimo EÚ, môže mať zásadný vplyv na bezpečnosť v rámci EÚ.

Kríza spôsobená ochorením COVID-19 takisto pretvorila našu predstavu o ochrane a bezpečnostných hrozbách a príslušných politikách. Takisto zdôraznila potrebu zaručenia bezpečnosti fyzického aj digitálneho prostredia. Poukázala na dôležitosť otvorenej strategickej autonómie v našich dodávateľských reťazcoch, pokiaľ ide o kritické výrobky, služby, infraštruktúry a technológie. Posilnila potrebu zapojiť do spoločného úsilia každý sektor a každého jednotlivca s cieľom zabezpečiť, aby bola EÚ predovšetkým lepšie pripravená a odolnejšia a mala v prípade potreby lepšie nástroje na reakciu.

Občanov nemôžu chrániť len samostatne konajúce členské štáty. Nikdy predtým nebolo dôležitejšie využiť naše silné stránky v záujme spolupráce a EÚ nikdy predtým nemala viac potenciálu na dosiahnutie zmeny. Môže ísť príkladom okrem iného posilnením celkového systému krízového riadenia a prácou v rámci svojich hraníc a mimo nich, ktorej cieľom je prispieť ku globálnej stabilite. Hoci primárnu zodpovednosť za bezpečnosť nesú členské štáty, v posledných rokoch čoraz viac prevláda presvedčenie, že bezpečnosť jedného členského štátu je bezpečnosťou všetkých. EÚ môže reagovať multidisciplinárne a integrovane a pomáhať bezpečnostným subjektom v členských štátoch nástrojmi a informáciami, ktoré potrebujú.[2]

EÚ môže takisto zabezpečiť, aby sa bezpečnostná politika naďalej zakladala na našich spoločných európskych hodnotách, ktorými sú dodržiavanie a zachovávanie právneho štátu, rovnosti[3] a základných práv a zaručovanie transparentnosti, zodpovednosti a demokratickej kontroly, čím sa vytvorí ten správny základ dôvery v politiky. Môže vybudovať účinnú a skutočnú bezpečnostnú úniu, v ktorej sú práva a slobody jednotlivcov dobre chránené.

---

[1] Definície hybridných hrozieb sú síce rôzne, ich cieľom je však podchytiť súbor rôznych nátlakových a podvratných činností a konvenčných a nekonvenčných metód (napríklad diplomatických, vojenských, ekonomických a technologických), ktoré môžu rôzne štátne aj neštátne subjekty koordinovaným spôsobom využívať na to, aby dosiahli konkrétne ciele (bez toho, aby formálne vyhlásili vojnu). Pozri JOIN(2016) 18 final.

[2] Napríklad prostredníctvom služieb poskytovaných v rámci vesmírneho programu EÚ, ako je Copernicus, ktorý poskytuje údaje získané pozorovaním Zeme a aplikácie na hraničný dozor, námornú bezpečnosť, presadzovanie práva, boj proti pirátstvu, odrádzanie od pašovania drog a riadenie núdzových situácií.

[3] Únia rovnosti: stratégia pre rodovú rovnosť na roky 2020 – 2025, COM(2020) 152.

Bezpečnosť a dodržiavanie základných práv nie sú protichodnými cieľmi, ale trvalými a navzájom sa dopĺňajúcimi cieľmi. Naše hodnoty a základné práva musia byť základom bezpečnostných politík a zabezpečovať súlad so zásadami nevyhnutnosti, proporcionality a zákonnosti, pričom musia byť zavedené riadne záruky na zaistenie zodpovednosti a súdnej nápravy, ktoré zároveň umožnia účinnú reakciu zameranú na ochranu jednotlivcov, a to najmä tých najzraniteľnejších.

Hoci už existujú významné právne, praktické a podporné nástroje, je potrebné ich posilniť a lepšie vykonávať. Došlo k výraznému pokroku, pokiaľ ide o zlepšenie výmeny informácií a spravodajskej spolupráce s členskými štátmi a elimináciu priestoru, v ktorom pôsobia teroristi a páchatelia trestných činov. Fragmentácia však pretrváva.

Činnosť musí takisto presahovať hranice EÚ. Ochrana Únie a jej občanov nespočíva už len v zaistení bezpečnosti v rámci hraníc EÚ, ale aj v riešení vonkajšieho rozmeru bezpečnosti. Prístup EÚ k vonkajšej bezpečnosti v rámci spoločnej zahraničnej a bezpečnostnej politiky (SZBP) a spoločnej bezpečnostnej a obrannej politiky (SBOP) zostáva hlavnou zložkou úsilia EÚ o posilnenie bezpečnosti v EÚ. Spolupráca s tretími krajinami a na globálnej úrovni zameraná na riešenie spoločných výziev je kľúčová z hľadiska účinnej a komplexnej reakcie, pričom stabilita a bezpečnosť v susedstve EÚ je základným predpokladom pre vlastnú bezpečnosť EÚ.

Táto nová stratégia nadväzuje na predchádzajúcu prácu Európskeho parlamentu[4], Rady[5] a Komisie[6] a je dôkazom toho, že skutočná a účinná bezpečnostná únia musí v sebe spájať silné jadro nástrojov a politík, ktoré zaistia bezpečnosť v praxi, a zároveň zohľadňovať skutočnosť, že bezpečnosť má vplyv na všetky súčasti spoločnosti a na všetky verejné politiky. Európska únia musí zabezpečiť bezpečné prostredie pre všetkých bez ohľadu na rasový alebo etnický pôvod, náboženstvo, vieru, pohlavie, vek alebo sexuálnu orientáciu.

Táto stratégia sa týka obdobia 2020 – 2025 a zameriava sa na budovanie spôsobilostí a kapacít na zabezpečenie nadčasového bezpečnostného prostredia. Stanovuje sa v nej celospoločenský prístup k bezpečnosti , ktorý umožní koordinovaným spôsobom účinne reagovať na rýchlo sa meniacu panorámu hrozieb . Vymedzujú sa v nej strategické priority a súvisiace opatrenia na riešenie digitálnych a fyzických rizík integrovaným spôsobom v celom ekosystéme bezpečnostnej únie, pričom dôraz sa kladie na oblasti, v ktorých môže EÚ priniesť väčšiu hodnotu. Jej cieľom je ponúknuť skutočný prínos z hľadiska bezpečnosti v záujme ochrany každého v EÚ.

II. Rýchlo sa meniaca európska panoráma bezpečnostných hrozieb

Bezpečnosť, prosperita a blaho občanov závisia od pocitu bezpečia. Ohrozenie tohto bezpečia závisí od miery zraniteľnosti ich života a živobytia. Čím väčšia je zraniteľnosť, tým väčšie je riziko, že môže dôjsť k jej zneužitiu. Zraniteľnosť aj hrozby sa neustále vyvíjajú a EÚ sa im musí prispôsobiť.

---

[4] Napríklad práca výboru Európskeho parlamentu pre terorizmus (TERR), ktorý podal správu v roku 2018.

[5] Od záverov Rady z júna 2015 o „obnovenej stratégii vnútornej bezpečnosti“ po novšie výsledky Rady z decembra 2019.

[6] Napĺňanie Európskeho programu v oblasti bezpečnosti s cieľom bojovať proti terorizmu a pripraviť pôdu pre účinnú a skutočnú bezpečnostnú úniu, COM(2016) 230 final z 20. apríla 2016. Pozri nedávne vyhodnotenie vykonávania právnych predpisov v oblasti vnútornej bezpečnosti: Vykonávanie právnych predpisov týkajúcich sa vnútorných vecí v oblasti vnútornej bezpečnosti – 2017 – 2020 [SWD(2020) 135].

Náš každodenný život závisí od širokej škály služieb, ako je energetika, doprava, finančné služby a zdravotníctvo. Tie závisia od fyzickej a digitálnej infraštruktúry, čo zvyšuje zraniteľnosť a potenciál narušenia. Počas pandémie spôsobenej ochorením COVID-19 mnohé podniky a verejné služby naďalej fungovali vďaka novým technológiám, či už tým, že nám umožnili vzájomné prepojenie prostredníctvom práce na diaľku alebo zabezpečovaním logistiky dodávateľských reťazcov. Takisto sa tým však vytvoril priestor na mimoriadny nárast škodlivých útokov, ktoré sa pokúšali využiť narušenie spôsobené pandémiou a prechod na digitálnu prácu z domu na kriminálne účely.[7] Nedostatok tovaru vytvoril priestor pre organizovanú trestnú činnosť. Následky mohli byť katastrofálne a mohli spôsobiť narušenie základných zdravotných služieb v čase najväčšieho tlaku.

Keďže z digitálnych technológií profitujeme v našom živote čoraz rozmanitejším spôsobom, **kybernetická bezpečnosť** technológií sa stala otázkou strategického významu.[8] Kybernetické útoky výrazne zasahujú domácnosti, banky, finančné služby a podniky (najmä malé a stredné podniky). Potenciálna škoda sa ďalej znásobuje v dôsledku prepojenia fyzických a digitálnych systémov; akékoľvek fyzické narušenie automaticky ovplyvní digitálne systémy, zatiaľ čo kybernetické útoky na informačné systémy a digitálne infraštruktúry môžu spôsobiť prerušenie základných služieb[9]. Vzostup internetu vecí a zvýšené využívanie umelej inteligencie so sebou prinesie nové výhody, ako aj nový súbor rizík.

Náš svet závisí od digitálnych infraštruktúr, technológií a online systémov, ktoré nám umožňujú obchodovať, konzumovať výrobky a využívať služby. Všetko sa zakladá na komunikácii a interakcii. Závislosť od online prostredia vytvára priestor na vlnu **počítačovej kriminality**.[10] „Počítačová kriminalita ako služba“ a tieňová ekonomika počítačovej kriminality poskytujú ľahký prístup k produktom a službám počítačovej kriminality online. Páchatelia trestnej činnosti sa rýchlo prispôsobujú novým technológiám a využívajú ich vo svoj prospech. Napríklad do legitímneho dodávateľského reťazca s liekmi prenikli falzifikáty a falšované lieky[11]. Exponenciálny nárast detskej pornografie online[12] je dôkazom sociálnych následkov meniacich sa modelov trestnej činnosti. Z nedávneho prieskumu vyplynulo, že väčšina ľudí v EÚ (55 %) sa obáva toho, že páchatelia trestných činov a podvodníci majú prístup k ich údajom.[13]

---

[7] Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU (*Po pandémii. Ako bude pandémia ochorenia COVID-19 pretvárať závažnú a organizovanú trestnú činnosť v EÚ*) (apríl 2020).

[8] Odporúčanie Komisie o kybernetickej bezpečnosti sietí 5G, C(2019) 2335; oznámenie Komisie o bezpečnom zavádzaní 5G v EÚ – Vykonávanie súboru nástrojov, COM(2020) 50.

[9] V marci 2020 sa Univerzitná nemocnica v Brne v Českej republike stala terčom kybernetického útoku, v dôsledku ktorého musela presunúť svojich pacientov do iných zariadení a odložiť operácie [Europol: Pandemic Profiteering. How criminals exploit the COVID-19 crisis (*Profitovanie z pandémie. Ako páchatelia trestných činov zneužívajú krízu spôsobenú ochorením COVID-19*)]. Umelú inteligenciu možno zneužiť na digitálne, politické a fyzické útoky, ako aj na sledovanie. Zber údajov v rámci internetu vecí možno použiť na sledovanie osôb (smart hodinky, virtuálni asistenti atď.).

[10] Podľa niektorých odhadov dosiahnu náklady v súvislosti s porušením ochrany údajov do roku 2024 výšku 5 biliónov USD ročne v porovnaní s 3 biliónmi USD v roku 2015 [Juniper Research, *The Future of Cybercrime & Security* (Budúcnosť počítačovej kriminality a bezpečnosti)].

[11] V štúdii (Legiscript) z roku 2016 sa odhaduje, že celosvetovo sú len 4 % internetových lekární prevádzkované v súlade so zákonom, pričom spotrebitelia v EÚ sú hlavným terčom 30 000 – 35 000 nezákonných lekární aktívnych online.

[12] Stratégia EÚ na účinnejší boj proti sexuálnemu zneužívaniu detí, COM(2020) 607.

[13] Agentúra Európskej únie pre základné práva (2020), Na vašich právach záleží: Bezpečnostné hrozby a skúsenosti, prieskum základných práv, Luxemburg, Úrad pre publikácie.

Globálne prostredie takisto prehlbuje tieto hrozby. Asertívne priemyselné politiky tretích krajín v spojení s nepretržitými krádežami duševného vlastníctva, ktoré umožňuje kybernetický priestor, menia strategickú paradigmu ochrany a presadzovania európskych záujmov. To ešte umocňuje vzostup aplikácií s dvojakým použitím, v dôsledku čoho sa silný sektor civilných technológií stáva veľkou výhodou v rámci obrannej a bezpečnostnej spôsobilosti. Priemyselná špionáž má významný vplyv na hospodárstvo, pracovné miesta a rast EÚ: kybernetické krádeže obchodného tajomstva stoja Európsku úniu odhadom 60 miliárd EUR[14]. V tejto súvislosti je potrebné dôkladne posúdiť, ako vzájomná závislosť a zvýšená expozícia kybernetickým hrozbám ovplyvňujú schopnosť EÚ chrániť občanov aj podniky.

Kríza spôsobená ochorením COVID-19 takisto zdôraznila to, ako sociálne rozdiely a neistota vedú k bezpečnostnej zraniteľnosti. Zväčšuje to potenciál rafinovanejších a **hybridných útokov** zo strany štátnych a neštátnych subjektov, ktoré využívajú zraniteľnosť pomocou kombinácie kybernetických útokov, poškodzovania kritickej infraštruktúry[15], dezinformačných kampaní a radikalizácie politického jazyka.[16]

Zároveň sa naďalej vyvíjajú dlhodobejšie etablované hrozby. V roku 2019 sa trend **teroristických útokov** v EÚ oslabil. Občanom EÚ však naďalej hrozí veľké riziko džihádistických útokov zo strany Islamského štátu a siete al-Káida a ich pridružených organizácií alebo nimi inšpirovaných útokov.[17] Zároveň narastá aj hrozba násilného pravicového extrémizmu.[18] Rasovo motivované útoky musia byť dôvodom vážnych obáv: smrteľné antisemitské teroristické útoky v Halle nám pripomenuli potrebu zintenzívniť reakciu v súlade s vyhlásením Rady z roku 2018[19]. Jeden z piatich ľudí v EÚ má veľké obavy z teroristického útoku počas nasledujúcich 12 mesiacov.[20] Pri prevažnej väčšine nedávnych teroristických útokov išlo o technicky nenáročné útoky páchané samostatne konajúcimi aktérmi, ktorí sa zamerali na jednotlivcov vo verejných priestoroch, zatiaľ čo teroristická propaganda online nadobudla živým prenosom útokov v meste Christchurch[21] nový význam. Hrozba, ktorú predstavujú radikalizovaní jednotlivci, zostáva vysoká a potenciálne ju prehlbujú vracajúci sa zahraniční teroristickí bojovníci a extrémisti prepustení z väzení.[22]

---

[14] The scale and impact of industrial espionage and theft of trade secrets through cyber (*Rozsah a vplyv priemyselnej špionáže a krádeže obchodného tajomstva prostredníctvom kybernetického priestoru*), 2018.

[15] Kritické infraštruktúry sú nevyhnutné pre základné funkcie spoločnosti, zdravie, ochranu, bezpečnosť a kvalitu života obyvateľov z ekonomického a sociálneho hľadiska, ktorých narušenie alebo zničenie by malo závažné dôsledky (smernica Rady 2008/114/ES).

[16] Až 97 % občanov EÚ sa stretlo s falošnými správami, pričom 38 % sa s nimi stretáva každodenne. Pozri JOIN(2020) 8 final.

[17] Trinásť členských štátov EÚ nahlásilo celkovo 119 dokonaných, neúspešných a zmarených teroristických útokov, pri ktorých zomrelo desať ľudí a 27 bolo zranených (Europol, správa EÚ o situácii a trendoch v oblasti terorizmu, 2020).

[18] V roku 2019 došlo k šiestim pravicovým teroristickým útokom (k jednému dokonanému, jednému neúspešnému a štyrom zmareným v troch členských štátoch) v porovnaní len s jedným v roku 2018, pričom k ďalším úmrtiam došlo v prípadoch, ktoré neboli klasifikované ako terorizmus (Europol, 2020).

[19] Pozri takisto vyhlásenie Rady o boji proti antisemitizmu a vypracovaní spoločného bezpečnostného prístupu k lepšej ochrane židovských komunít a inštitúcií v Európe.

[20] Agentúra EÚ pre základné práva: Your rights matter: Security concerns and experiences (*Na vašich právach záleží: Bezpečnostné hrozby a skúsenosti*), 2020.

[21] V období od júla 2015 do konca roka 2019 odhalil Europol teroristický obsah na 361 platformách (Europol, 2020).

[22] Europol: A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism,(*Prehľad transatlantických najlepších postupov v boji proti radikalizácii vo väzeniach a teroristickej recidivite)*, 2019.

Kríza takisto odhalila, ako sa môžu existujúce hrozby vyvíjať za nových okolností. **Organizované zločinecké skupiny** zneužívajú nedostatok tovaru, ktorým sa vytvára priestor pre nové nezákonné trhy. Trh s nelegálnymi drogami je aj naďalej najväčším zločineckým trhom v EÚ, pričom jeho minimálna hodnota v EÚ sa ročne odhaduje na 30 miliárd EUR (v maloobchodných cenách)[23]. Naďalej pretrváva obchodovanie s ľuďmi: podľa odhadov dosahuje ročný globálny zisk zo všetkých foriem vykorisťovania výšku takmer 30 miliárd EUR.[24] Medzinárodný obchod s falšovanými liekmi dosiahol hodnotu 38,9 miliárd EUR[25]. Nízka miera konfiškácie zároveň umožňuje páchateľom ďalej rozširovať svoju trestnú činnosť a prenikať do legálneho hospodárstva[26]. Páchateľom trestných činov a teroristom umožňuje online trh a nové technológie, ako je 3D tlač, ľahší prístup k palným zbraniam.[27] V dôsledku využívania umelej inteligencie, nových technológií a robotiky sa bude naďalej zvyšovať riziko, že páchatelia trestných činov budú zneužívať výhody inovácií na nekalé účely[28].

Tieto hrozby sa vymykajú z jednotlivých kategórií a rozličné časti spoločnosti postihujú rôznym spôsobom. Všetky predstavujú vážnu hroznu pre jednotlivcov a podniky a vyžadujú si komplexnú a súdržnú reakciu na úrovni EÚ. V dobe, keď bezpečnostné slabiny môžu vykazovať dokonca aj malé vzájomne prepojené domáce spotrebiče, ako napr. chladnička alebo kávovar napojené na internet, sa pri zaisťovaní našej bezpečnosti nemôžeme viac spoliehať len na tradičné štátne subjekty. Hospodárske subjekty musia prevziať väčšiu zodpovednosť za kybernetickú bezpečnosť výrobkov a služieb, ktoré uvádzajú na trh a zároveň musia mať aj občania aspoň základné vedomosti o kybernetickej bezpečnosti, aby sa mohli chrániť.

III. Koordinovaná reakcia EÚ za celú spoločnosť

EÚ už preukázala, že dokáže priniesť skutočnú pridanú hodnotu. Od roku 2015 prispela bezpečnostná únia k vytvoreniu nových väzieb, pokiaľ ide o spôsob, akým je bezpečnostná politika riešená na úrovni EÚ. Je však potrebné zintenzívniť snahy o zapojenie celej spoločnosti vrátane orgánov verejnej správy na všetkých úrovniach, podnikov vo všetkých sektoroch a jednotlivcov vo všetkých členských štátoch. V dôsledku čoraz väčšej informovanosti o rizikách závislosti[29] a potrebe silnej európskej priemyselnej stratégie[30] sa poukazuje na to, že EÚ musí zabezpečiť kritické množstvo priemyslu, technologickej produkcie a odolnosti dodávateľského reťazca. Sila takisto znamená plné rešpektovanie základných práv a hodnôt EÚ, ktoré sú predpokladom legitímnych, účinných a udržateľných

[23] Správa centra EMCDDA a Europolu o trhu s drogami v EÚ z roku 2019.
[24] Správa Europolu o obchodovaní s ľuďmi, finančný obchodný model (2015).
[25] Správa Úradu Európskej únie pre duševné vlastníctvo a OECD o obchode s falšovanými farmaceutickými výrobkami.
[26] Správa o vymáhaní majetku a konfiškácii: zabezpečenie, aby sa trestná činnosť nevyplácala, COM(2020) 217.
[27] V roku 2017 boli palné zbrane použité v 41 % všetkých teroristických útokov (Europol, 2018).
[28] V júli 2020 francúzske a holandské orgány presadzovania práva a justičné orgány spolu s Europolom a Eurojustom predstavili spoločné vyšetrovanie, ktorého cieľom je rozbiť zašifrovanú telefónnu siete EncroChat využívanú zločineckými sieťami zapojenými do násilných útokov, korupcie, pokusov o vraždu a transport drog veľkého rozsahu.
[29] Medzi riziká závislosti od zahraničia patrí zvýšená expozícia potenciálnym hrozbám, ktoré siahajú od zneužívania zraniteľnosti infraštruktúr informačných technológií, čo môže ohroziť kritické infraštruktúry (napr. energetiku, dopravu, bankovníctvo, zdravotníctvo) alebo viesť k získaniu kontroly nad priemyselnými riadiacimi systémami, až po väčšiu schopnosť krádeže údajov alebo špionáže.
[30] Oznámenie Komisie Nová priemyselná stratégia pre Európu, COM(2020) 102.

bezpečnostných politík. V tejto stratégii bezpečnostnej únie sa stanovujú konkrétne pracovné okruhy, v ktorých je potrebné napredovať. Zakladá sa na týchto spoločných cieľoch:

- ***Budovanie spôsobilosti a kapacít na včasné odhaľovanie kríz, ich predchádzanie a rýchlu reakciu na ne:*** Európa musí byť odolnejšia, aby dokázala zabrániť budúcim otrasom, chrániť sa pred nimi a odolávať im. Musíme budovať spôsobilosť a kapacity na včasné odhaľovanie bezpečnostných kríz a rýchlu reakciu na ne pomocou integrovaného a koordinovaného prístupu, a to celosvetovo, ako aj prostredníctvom sektorových iniciatív (napr. pre finančný, energetický a justičný sektor, sektor presadzovania práva, zdravotnícky, námorný a dopravný sektor) a nadväzovania na existujúce nástroje a iniciatívy[31]. Komisia takisto predloží návrhy týkajúce sa rozsiahleho systému krízového riadenia v rámci EÚ, ktorý by mohol byť relevantný aj z hľadiska bezpečnosti.
- ***Zameranie na výsledky***: Stratégia založená na výkonnosti musí vychádzať z dôkladného posúdenia hrozieb a rizika, aby sme svoje úsilie dokázali zamerať čo najúčinnejšie. Musia sa v nej vymedzovať a uplatňovať správne pravidlá a správne nástroje. Vyžaduje si spoľahlivé strategické spravodajské informácie, ktoré sú základom bezpečnostných politík EÚ. Tam, kde sa vyžadujú právne predpisy EÚ, je potrebné tieto predpisy sledovať, aby sa zabezpečilo ich plne vykonávanie a zabránilo sa fragmentácii a medzerám, ktoré možno zneužiť. Účinné vykonávanie tejto stratégie bude takisto závisieť od zabezpečenia náležitých finančných prostriedkov v nasledujúcom programovom období 2021 – 2027, a to vrátane prostriedkov pre súvisiace agentúry EÚ.
- ***Prepojenie všetkých aktérov vo verejnom a v súkromnom sektore v rámci spoločného úsilia:*** Kľúčoví aktéri vo verejnom aj v súkromnom sektore si len neochotne vymieňajú bezpečnostné informácie , či už z obavy z ohrozenia vnútroštátnej bezpečnosti, alebo konkurencieschopnosti.[32] Najväčší účinok však dosiahneme vtedy, keď sa všetci spojíme a budeme sa navzájom podporovať. V prvom rade to znamená intenzívnejšiu spoluprácu medzi členskými štátmi so zapojením orgánov presadzovania práva a justičných a iných verejných orgánov, ako aj s inštitúciami a agentúrami EÚ, s cieľom rozvíjať porozumenie a výmenu potrebnú na hľadanie spoločných riešení. Spolupráca so súkromným sektorom je takisto kľúčová, a to najmä vzhľadom na skutočnosť, že priemysel vlastní dôležitú časť digitálnej a nedigitálnej infraštruktúry, ktorá je ústredným prvkom v účinnom boji proti trestnej činnosti a terorizmu. Prispieť môžu aj jednotlivci, a to napríklad prostredníctvom získavania zručností a vytváraním povedomia o boji proti počítačovej kriminalite alebo dezinformáciám. V neposlednom rade treba zdôrazniť, že toto spoločné úsilie musí presahovať naše hranice, vďaka čomu sa vytvoria užšie väzby s partnermi s rovnakým zmýšľaním.

[31] Napríklad integrovaná politická reakcia na krízu (IPCR), Koordinačné centrum pre reakcie na núdzové situácie, odporúčanie Komisie o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu [C(2017) 6100], Operačný protokol EÚ na boj proti hybridným hrozbám (operačný protokol EÚ) SWD(2016) 227.

[32] Spoločné oznámenie o odolnosti, odrádzaní a obrane: budovanie silnej kybernetickej bezpečnosti pre EÚ, JOIN(2017) 450.

IV. Ochrana všetkých v EÚ: strategické priority pre bezpečnostnú úniu

EÚ má mimoriadne dobrú pozíciu na to, aby reagovala na tieto nové globálne hrozby a výzvy. Uvedená analýza hrozieb poukazuje na štyri navzájom prepojené strategické priority, na ktorých sa bude pracovať na úrovni EÚ pri plnom rešpektovaní základných práv: i) nadčasové bezpečnostné prostredie; ii) riešenie vyvíjajúcich sa hrozieb; iii) ochrana Európanov pred terorizmom a organizovanou trestnou činnosťou; iv) pevný európsky bezpečnostný ekosystém.

1. Nadčasové bezpečnostné prostredie

Ochrana kritickej infraštruktúry a jej odolnosť

Občania sa v každodennom živote spoliehajú na kľúčové infraštruktúry, ktoré im umožňujú cestovať, pracovať, využívať základné verejné služby, ako sú nemocnice, doprava a dodávky energie, alebo si uplatňovať svoje demokratické práva. Ak tieto infraštruktúry nie sú dostatočne chránené a odolné, môžu útoky spôsobiť vážne narušenie, či už fyzické, alebo digitálne, a to v jednotlivých členských štátoch a potenciálne aj v celej EÚ.

Existujúci rámec EÚ pre ochranu a odolnosť kritickej infraštruktúry[33] už neudržiava krok s vyvíjajúcimi sa rizikami. Čoraz väčšia vzájomná závislosť znamená, že narušenie v jednom sektore môže mať priamy vplyv na fungovanie v ďalších sektoroch: útok na proces výroby elektrickej energie môže spôsobiť výpadok v oblastí telekomunikácií, nemocníc, bánk alebo letísk, zatiaľ čo útok na digitálnu infraštruktúru by mohol viesť k narušeniu elektrických alebo finančných sietí.. Keďže sa naše hospodárstvo a spoločnosť čoraz viac presúvajú do online priestoru, takéto riziká sa stávajú čoraz vážnejšími. Legislatívny rámec musí na túto zvýšenú prepojenosť a vzájomnú závislosť reagovať záznymi opatreniami na ochranu kritickej infraštruktúry a podporu jej odolnosti, a to kybernetickými aj fyzickými. Základné služby vrátane tých, ktoré sa zakladajú na vesmírnych infraštruktúrach, musia byť náležite chránené pred súčasnými a očakávanými hrozbami, a zároveň musia byť odolné. To si vyžaduje, aby bol systém schopný pripraviť sa na tieto nepriaznivé udalosti, počítať s nimi, absorbovať ich, zotaviť sa z nich a úspešnejšie sa im prispôsobiť.

Členské štáty zároveň uplatňujú svoju diskrečnú právomoc a vykonávajú existujúce právne predpisy rôznym spôsobom . Výsledná fragmentácia môže oslabiť vnútorný trh a sťažiť cezhraničnú koordináciu, a to najvýraznejšie v hraničných regiónoch. Prevádzkovatelia poskytujúci základné služby v rôznych členských štátoch musia dodržiavať rôzne režimy oznamovania. Komisia skúma, či by **nové rámce pre fyzické aj digitálne infraštruktúry** mohli priniesť viac súdržnosti a koherentnejší prístup k zabezpečeniu spoľahlivého poskytovania základných služieb. Tento rámec musia sprevádzať **sektorové iniciatívy**, ktorých cieľom je riešiť špecifické riziká, ktorým sú vystavené kritické infraštruktúry ako doprava, vesmírne systémy, energetika, financie a zdravotníctvo[34]. Vzhľadom na veľkú závislosť finančného sektora od služieb IT a jeho veľkú zraniteľnosť voči kybernetickým útokom bude prvým krokom iniciatíva zameraná na digitálnu prevádzkovú odolnosť

[33] Smernica 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016); smernica Rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu.

[34] Vzhľadom na skutočnosť, že sektor zdravotníctva čelil tlaku najmä počas krízy spôsobenej ochorením COVID-19, bude Komisia takisto zvažovať iniciatívy na posilnenie rámca EÚ pre zdravotnú bezpečnosť a zodpovedných agentúr EÚ s cieľom reagovať na závažné cezhraničné zdravotné hrozby.

finančných sektorov. V dôsledku osobitnej citlivosti a vplyvu energetického systému bude osobitná iniciatíva podporovať väčšiu odolnosť kritickej energetickej infraštruktúry voči fyzickým, kybernetickým a hybridným hrozbám, čím sa zabezpečia rovnaké podmienky pre cezhraničných prevádzkovateľov energetických sietí.

Účinky priamych zahraničných investícií z hľadiska bezpečnosti, ktoré by mohli ovplyvniť kritické infraštruktúry alebo kritické technológie, budú takisto predmetom posúdení vykonaných členskými štátmi EÚ a Komisiou podľa nového rámca na preverovanie priamych zahraničných investícií[35].

EÚ môže takisto vyvinúť nové nástroje na podporu odolnosti kritických infraštruktúr. Globálny internet zatiaľ preukazuje vysokú úroveň odolnosti, najmä pokiaľ ide o schopnosť zvládať zvýšený objem dátových prenosov. Musíme však byť pripravení na možné budúce krízy, ktoré budú ohrozovať bezpečnosť, stabilitu a odolnosť internetu. Zabezpečenie bezproblémového fungovania internetu aj v budúcnosti znamená rázne zakročenie proti kybernetickým incidentom a škodlivým činnostiam online a obmedzenie závislosti od infraštruktúr a služieb nachádzajúcich sa mimo Európy. Bude si to vyžadovať kombináciu právnych predpisov a preskúmanie existujúcich pravidiel, aby sa zabezpečila vysoká spoločná úroveň bezpečnosti sietí a informačných systémov v EÚ; navýšenie investícií do výskumu a inovácií; a preskúmanie zavádzania alebo posilnenia kľúčových internetových infraštruktúr a zdrojov, najmä systému názvov domén[36].

Základným prvokom z hľadiska ochrany kľúčových digitálnych aktív na úrovni EÚ a vnútroštátnej úrovni je ponúknuť pre kritické infraštruktúry kanál na bezpečnú komunikáciu. Komisia spolupracuje s členskými štátmi na zavádzaní certifikovanej zabezpečenej pozemnej a vesmírnej kvantovej infraštruktúry medzi koncovými zariadeniami (end-to-end) v kombinácii so zabezpečeným systémom vládnej satelitnej komunikácie stanoveným v nariadení o vesmírnom programe[37].

Kybernetická bezpečnosť

Výskyt kybernetických útokov sa neustále zvyšuje[38]. Tieto útoky sú rafinovanejšie ako kedykoľvek predtým, pochádzajú zo širokého spektra zdrojov v rámci EÚ a mimo nej a zameriavajú sa na najzraniteľnejšie oblasti. Často ide o štátnych alebo štátom podporovaných aktérov, ktorí sa zameriavajú na kľúčové digitálne infraštruktúry, ako sú hlavní poskytovatelia cloudu[39]. Kybernetické riziká takisto predstavujú značnú hrozbu pre finančné systémy. Podľa odhadov Medzinárodného menového fondu dosahujú celosvetové straty spôsobené kybernetickými útokmi každoročne výšku 9 % čistého príjmu bánk alebo

[35] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/452 z 19. marca 2019, ktorým sa ustanovuje rámec na preverovanie priamych zahraničných investícií do Únie, ktoré sa začne plne uplatňovať 11. októbra 2020, zabezpečí pre EÚ nový mechanizmus spolupráce v oblasti priamych investícií pochádzajúcich z krajín mimo EÚ, ktoré by mohli mať vplyv na bezpečnosť alebo verejný poriadok. V súlade s nariadením budú členské štáty a Komisia posudzovať potenciálne riziká spojené s takýmito PZI, a ak je to vhodné a relevantné pre viac ako jeden členský štát, navrhnú primerané opatrenia na zmiernenie týchto rizík.

[36] Systém názvov domén (DNS) je hierarchický a decentralizovaný systém prideľovania názvov pre počítače, služby alebo iné zdroje spojené s internetom alebo so súkromnou sieťou. Prevádza názvy domén na IP adresy potrebné na lokalizáciu a identifikáciu počítačových služieb a zariadení.

[37] Návrh nariadenia, ktorým sa stanovuje Vesmírny program Únie a zriaďuje Agentúra Európskej únie pre vesmírny program. COM(2018) 447.

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

[39] Útoky DDoS zostávajú neustálou hrozbou: hlavní poskytovatelia museli zmierňovať vážne útoky DDoS, ako bol útok na služby Amazon Web vo februári 2020.

približne 100 miliárd USD[40]. Prechod na prepojené zariadenia prinesie používateľom veľké výhody, ale v dôsledku uchovávania a spracúvania menšieho množstva údajov v dátových centrách a väčšieho množstva spracúvaného bližšie k používateľovi „na okraji“[41] už nebude kybernetická bezpečnosť schopná zameriavať sa na ochranu hlavných bodov.[42]

V roku 2017 EÚ predstavila prístup ku kybernetickej bezpečnosti, ktorej jadrom je budovanie odolnosti, rýchla reakcia a účinné odrádzanie.[43] EÚ teraz musí zabezpečiť, aby z hľadiska svojich spôsobilostí v oblasti kybernetickej bezpečnosti držala krok s realitou s cieľom dosiahnuť odolnosť aj reakciu. Vyžaduje si to celospoločenský prístup , v rámci ktorého inštitúcie, agentúry a orgány EÚ, členské štáty, priemysel, akademická obec a občania budú venovať prioritnú pozornosť kybernetickej bezpečnosti tak, ako je to potrebné[44]. Tento horizontálny prístup musia opäť dopĺňať sektorové prístupy ku kybernetickej bezpečnosti v oblastiach, ako je energetika, finančné služby, doprava alebo zdravotníctvo. Ďalšia fáza činnosti EÚ by mala byť zhrnutá v revidovanej stratégii kybernetickej bezpečnosti Európskej únie.

Skúmanie nových a posilnených foriem spolupráce medzi spravodajskými službami, EU INTCEN a ďalšími organizáciami pôsobiacimi v oblasti bezpečnosti by malo byť súčasťou úsilia o posilnenie kybernetickej bezpečnosti, ako aj boja proti terorizmu, extrémizmu, radikalizácii a hybridným hrozbám.

Vzhľadom na prebiehajúce zavádzanie **infraštruktúry 5G** v EÚ a potenciálnu závislosť mnohých kritických služieb od sietí 5G by boli následky systémového a rozsiahleho narušenia mimoriadne závažné. Proces stanovený v odporúčaní Komisie o kybernetickej bezpečnosti sietí 5G[45] z roku 2019 priniesol konkrétne kroky zo strany členských štátov v súvislosti s kľúčovými opatreniami stanovenými v súbore nástrojov pre 5G[46].

Jedna z najdôležitejších dlhodobých potrieb je vyvíjať kultúru **kybernetickej bezpečnosti už v štádiu návrhu**, v rámci ktorej bude bezpečnosť od začiatku zakomponovaná do výrobkov a služieb. Významne k tomu prispeje nový rámec na certifikáciu kybernetickej bezpečnosti podľa aktu o kybernetickej bezpečnosti[47]. Práca na rámci už prebieha, pričom sa už pripravujú dva certifikačné systémy a v priebehu tohto roka sa vymedzia priority pre ďalšie systémy. V tejto oblasti má kľúčový význam spolupráca medzi agentúrou EÚ pre kybernetickú bezpečnosť (ENISA), orgánmi na ochranu údajov a Európskym výborom pre ochranu údajov[48].

---

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

41 Edge computing je distribuovaná otvorená architektúra IT s decentralizovanou výpočtovou kapacitou, ktorá umožňuje prenosné výpočtové technológie a technológiu internetu vecí. V rámci edge computingu údaje spracúva samotné zariadenie alebo miestny počítač alebo server, čiže sa neprenáša do dátového centra.

42 Oznámenie Komisie Európska dátová stratégia, COM(2020) 66 final.

43 Spoločné oznámenie o odolnosti, odrádzaní a obrane: budovanie silnej kybernetickej bezpečnosti pre EÚ, JOIN(2017) 450.

44 Správa spoločného výskumného centra „Kybernetická bezpečnosť – naša digitálna opora“ prináša viacrozmerný prehľad rastu kybernetickej bezpečnosti za posledných 40 rokov.

45 Odporúčanie Komisie o kybernetickej bezpečnosti sietí 5G, COM(2019) 2335 final. V odporúčaní sa predpokladá jej preskúmanie v poslednom štvrťroku 2020.

46 Pozri správu skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti o vykonávaní súboru nástrojov z 24. júla 2020.

47 Nariadenie (EÚ) 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (akt o kybernetickej bezpečnosti).

48 Oznámenie o ochrane údajov ako pilieri posilnenia postavenia občanov a prístupu EÚ k digitálnej transformácii – dva roky uplatňovania všeobecného nariadenia o ochrane údajov COM(2020) 264.

Komisia už poukázala na potrebu zriadiť **spoločnú kybernetickú jednotku**, ktorou sa zabezpečí štruktúrovaná a koordinovaná operačná spolupráca. Mohla by zahŕňať systém vzájomnej pomoci v čase krízy na úrovni EÚ. Spoločná kybernetická jednotka by nadviazaním na vykonávanie odporúčania o koncepcii[49] mohla budovať dôveru medzi rôznymi subjektmi v európskom ekosystéme kybernetickej bezpečnosti a ponúkať členským štátom službu kľúčového významu. Komisia začne viesť diskusie s príslušnými zainteresovanými stranami (počnúc členskými štátmi) a stanoví jasný proces, míľniky a harmonogram do konca roka 2020.

Takisto sú dôležité spoločné pravidlá v oblasti informačnej bezpečnosti a kybernetickej bezpečnosti pre všetky inštitúcie, orgány a agentúry EÚ. Cieľom by malo byť vytvoriť povinné a vysoké spoločné štandardy pre bezpečnú výmenu informácií a bezpečnosť digitálnych infraštruktúr a systémov vo všetkých inštitúciách, orgánoch a agentúrach EÚ. Týmto novým rámcom by sa mala podporiť silná a účinná operačná spolupráca v oblasti kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach EÚ, pričom centrálnu úlohu by zohrával tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT-EU).

Vzhľadom na globálny charakter kybernetických útokov má zásadný význam z hľadiska ďalšieho predchádzania kybernetickým útokom, odrádzania od nich a reagovania na ne budovanie a zachovávanie **medzinárodných partnerstiev**. V rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor nástrojov kybernetickej diplomacie“)[50] sa stanovujú opatrenia v rámci spoločnej zahraničnej a bezpečnostnej politiky vrátane reštriktívnych opatrení (sankcií), ktoré môžu byť použité proti činnostiam, ktoré poškodzujú jej politické, bezpečnostné a ekonomické záujmy. Európska únia by takisto mala zintenzívniť svoju prácu prostredníctvom fondov rozvoja a spolupráce, aby zabezpečila budovanie kapacít na podporu partnerských štátov pri posilňovaní ich digitálnych ekosystémov, prijímaní vnútroštátnych legislatívnych reforiem a dodržiavaní medzinárodných noriem. To zvyšuje odolnosť celého spoločenstva a jeho schopnosť účinne bojovať proti kybernetickým hrozbám a reagovať na ne. Zahŕňa to špecifickú prácu v oblasti presadzovania noriem EÚ a príslušných právnych predpisov, ktorej cieľom je zvyšovať kybernetickú bezpečnosť partnerských krajín v susedstve[51].

Ochrana verejných priestorov

Nedávne teroristické útoky boli zamerané na **verejné priestory** vrátane miest na bohoslužby a dopravných uzlov, pričom zneužili ich otvorenosť a dostupnosť. Vzostup terorizmu vyvolaného politicky alebo ideologicky motivovaným extrémizmom závažnosť tejto hrozby ešte zvýšil. Vyžaduje si to silnejšiu fyzickú ochranu týchto miest a primerané systémy odhaľovania bez toho, aby sa oslabili slobody občanov[52]. Komisia posilní spoluprácu medzi verejným a súkromným sektorom v oblasti ochrany verejných priestorov, a to prostredníctvom finančných prostriedkov, výmeny skúseností a osvedčených postupov, konkrétnych usmernení[53] a odporúčaní[54]. Súčasťou tohto prístupu bude takisto zvyšovanie

[49] Odporúčanie Komisie (EÚ) 2017/1584 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu.

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

[51] Pozri usmernenia EÚ pre budovanie vonkajších kybernetických kapacít prijaté v Rade z 26. júna 2018.

[52] Osobitnú pozornosť si zasluhujú systémy diaľkovej biometrickej identifikácie. Prvotné názory Komisie sú formulované v bielej knihe Komisie z 19. februára 2020 o umelej inteligencii, COM(2020) 65.

[53] Ako napríklad usmernenie pre výber vhodných riešení bezpečnostných bariér na ochranu verejných priestorov (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

informovanosti, výkonnostné požiadavky, testovanie detekčných zariadení a zintenzívnenie previerok osôb s cieľom riešiť vnútorné hrozby. Dôležitým aspektom, ktorý treba zohľadniť, je to, že neúmerným spôsobom môžu byť postihnuté menšiny a zraniteľné osoby vrátane osôb, ktoré sú cieľom útokov z dôvodu svojho náboženstva alebo pohlavia, , a preto si vyžadujú osobitnú pozornosť. Regionálne a miestne verejné úrady zohrávajú dôležitú úlohu v zlepšovaní bezpečnosti verejných priestorov. Komisia takisto pomáha podporovať iniciatívy miest v oblasti bezpečnosti verejných priestorov[55]. Začiatok nového partnerstva v rámci Urbánnej agendy pre EÚ[56] zameraného na „bezpečnosť verejných priestorov“ z novembra 2018 je odrazom záväzku členských štátov, Komisie a miest lepšie riešiť bezpečnostné hrozby v mestskom prostredí.

Trh s **bezpilotnými vzdušnými prostriedkami**, ktoré majú mnohé hodnotné a legitímne spôsoby využitia, sa naďalej rozširuje. Takisto však môžu byť potenciálne zneužité páchateľmi trestných činov a teroristami, pričom osobitné ohrozené sú verejné priestory. Ich cieľom môžu byť jednotlivci, zhromaždenia, kritická infraštruktúra, orgány presadzovania práva, hranice alebo verejné priestory. Vedomosti o používaní bezpilotných vzdušných prostriedkov v konfliktoch by mohli preniknúť do Európy priamo (prostredníctvom vracajúcich sa zahraničných teroristických bojovníkov) alebo cez internet. Pravidlá, ktoré už vypracovala Európska agentúra pre bezpečnosť letectva, sú dôležitým prvým krokom v oblastiach, ako je registrácia prevádzkovateľov bezpilotných vzdušných prostriedkov a povinná diaľková identifikácia bezpilotných vzdušných prostriedkov. V dôsledku čoraz väčšej dostupnosti, cenovej prijateľnosti a väčšieho potenciálu bezpilotných vzdušných prostriedkov je potrebné prijať ďalšie opatrenia. Môže medzi ne patriť výmena informácií, poskytnutie usmernení a osvedčených postupov pre všetkých, a to aj na účely presadzovania práva, ako aj rozsiahlejšie testovanie protiopatrení týkajúcich sa bezpilotných vzdušných prostriedkov[57]. Okrem toho je potrebné podrobnejšie analyzovať a riešiť dôsledky používania bezpilotných vzdušných prostriedkov vo verejných priestoroch, pokiaľ ide o ochranu súkromia a údajov.

Kľúčové opatrenia
• právne predpisy na ochranu kritickej infraštruktúry a jej odolnosť, • revízia smernice o sieťovej a informačnej bezpečnosti, • iniciatíva zameraná na prevádzkovú odolnosť finančného sektora, • ochrana a kybernetická bezpečnosť kritickej energetickej infraštruktúry a sieťový predpis pre kybernetickú bezpečnosť cezhraničných tokov elektrickej energie, • stratégia kybernetickej bezpečnosti Európskej únie, • ďalšie kroky smerujúce k vytvoreniu spoločnej kybernetickej jednotky, • spoločné pravidlá v oblasti informačnej bezpečnosti a kybernetickej bezpečnosti pre

[54] Usmernenie pre osvedčené postupy uvedené v SWD(2019) 140 vrátane časti o spolupráci medzi verejným a súkromným sektorom. Financovanie z Fondu pre vnútornú bezpečnosť – polícia sa osobitne zameriava na zintenzívnenie spolupráce medzi verejným a súkromným sektorom.

[55] Tri mestá (Pireus v Grécku, Tampere vo Fínsku a Turín v Taliansku) budú testovať nové riešenia ako súčasť mestských inovačných opatrení spolufinancovaných zo zdrojov Európskeho fondu regionálneho rozvoja (EFRR).

[56] Urbánna agenda pre EÚ predstavuje viacúrovňovú pracovnú metódu podporujúcu spoluprácu medzi členskými štátmi, mestami, Európskou komisiou a inými zainteresovanými stranami, ktorej cieľom je podporovať rast, životaschopnosť a inovácie v európskych mestách a identifikovať a úspešne riešiť sociálne výzvy.

[57] Nedávno bol v tejto oblasti zriadený viacročný program testovania určený na podporu členských štátov pri vývoji spoločnej metodiky a testovacej platformy.

inštitúcie, orgány a agentúry EÚ,
- posilnená spolupráca v oblasti ochrany verejných priestorov vrátane miest na bohoslužby,
- výmena najlepších postupov týkajúcich sa riešenia zneužívania bezpilotných vzdušných prostriedkov.

2. Riešenie vyvíjajúcich sa hrozieb

Počítačová kriminalita

Technológie prinášajú spoločnosti nové príležitosti. Takisto ponúkajú nové nástroje pre potreby justície a presadzovania práva. Zároveň však vytvárajú priestor pre páchateľov trestných činov. Malvér, krádež osobných alebo obchodných údajov nabúraním systému a prerušenie digitálnej činnosti spôsobujúce finančnú škodu alebo poškodenie dobrého mena sú na vzostupe. Prvou obranou je odolné prostredie, ktoré tvorí silná kybernetická bezpečnosť. Orgány na presadzovanie práva musia byť schopné pracovať v oblasti digitálneho vyšetrovania s jasnými pravidlami, aby mohli vyšetrovať a stíhať trestné činy a poskytovať obetiam potrebnú ochranu. Táto práca by mala nadväzovať na činnosť spoločnej pracovnej skupiny Europolu pre boj proti počítačovej kriminalite a protokol o reakcii na núdzové situácie v rámci presadzovania práva, ktorý bol vypracovaný na koordináciu reakcií na kybernetické útoky veľkého rozsahu. Kľúčové sú takisto účinné mechanizmy umožňujúce partnerstvá a spoluprácu verejného a súkromného sektora.

Zároveň by sa boj proti počítačovej kriminalite mal stať strategickou komunikačnou prioritou v celej EÚ , aby boli Európania upozorňovaní na riziká a preventívne opatrenia, ktoré môžu prijať. Malo by to byť súčasťou proaktívneho prístupu. Kľúčovým krokom je plné vykonávanie súčasného právneho rámca[58]: Komisia bude pripravená využiť postupy v prípade nesplnenia povinnosti, ak to bude potrebné, a zároveň bude preskúmavať tento rámec, aby zabezpečila, že stále spĺňa svoj účel. Komisia spolu s Europolom a agentúrou EÚ pre kybernetickú bezpečnosť ENISA takisto preskúma realizovateľnosť systému včasného varovania v oblasti kybernetickej bezpečnosti, ktorý by mohol zabezpečiť tok informácií a rýchle reakcie v prípade výskytu kybernetických trestných činov.

Počítačová kriminalita je celosvetovou výzvou, ktorá si vyžaduje účinnú medzinárodnú spoluprácu. Európska únia podporuje Budapeštiansky dohovor Rady Európy o počítačovej kriminalite, ktorý predstavuje účinný, dobre fungujúci rámec umožňujúci krajinám určiť, ktoré systémy a komunikačné kanály musia zaviesť, aby mohli účinne spolupracovať.

Takmer polovica občanov EÚ má obavy zo zneužitia údajov[59] a **krádež totožnosti** predstavuje vážnu hrozbu.[60] Jedným z aspektov je podvodné použitie totožnosti s cieľom finančného zisku, ale môže mať aj značné osobné a psychologické následky, keďže nelegálne príspevky vytvorené osobou, ktorá totožnosť ukradla, môžu zostať v online priestore dlhé roky. Komisia preskúma možné praktické opatrenia na ochranu obetí pred

[58] Smernica 2013/40/EÚ o útokoch na informačné systémy.

[59] 46 % (Eurobarometer o postoji Európanov ku kybernetickej bezpečnosti, január 2020).

[60] Prevažná väčšina respondentov v prieskume Eurobarometer 2018 Postoj Európanov ku kybernetickej bezpečnosti (95 %) uviedla, že krádež totožnosti považuje za závažný trestný čin, a sedem z desiatich respondentov povedalo, že je to veľmi závažný trestný čin. Eurobarometer zverejnený v januári 2020 potvrdil obavy týkajúce sa počítačovej kriminality, online podvodov a krádeže totožnosti: dve tretiny respondentov uviedli, že majú obavy z bankových podvodov (67 %) alebo z krádeže totožnosti (66 %).

všetkými formami krádeže totožnosti, pričom zohľadní pripravovanú iniciatívu v oblasti digitálnej identity[61].

Boj s počítačovou kriminalitou si vyžaduje zameranie na budúcnosť. Zatiaľ čo spoločnosť využíva nové technologické výdobytky na posilnenie hospodárstva a spoločnosti, páchatelia trestných činov sa takisto môžu snažiť o využívanie týchto nástrojov na nekalé účely. Páchatelia trestných činov môžu napríklad využívať umelú inteligenciu na odhaľovanie a zisťovanie hesiel alebo na zjednodušenie vytvárania malvéru a využívanie obrazového a zvukového signálu, ktoré následne môžu použiť na krádež totožnosti alebo podvod s osobnými údajmi.

Moderné presadzovanie práva

Pracovníci v oblasti presadzovania práva a justície sa musia prispôsobiť novým technológiám. Technologický vývoj a vyvíjajúce sa hrozby si vyžadujú, aby mali orgány presadzovania práva prístup k novým nástrojom, získavali nové zručnosti a vyvíjali alternatívne vyšetrovacie techniky. Na doplnenie legislatívnych opatrení zameraných na zlepšenie cezhraničného prístupu k elektronickým dôkazom v rámci vyšetrovania trestných činov môže EÚ pomôcť orgánom presadzovania práva vyvinúť potrebnú kapacitu na identifikáciu, zabezpečenie a interpretáciu údajov potrebných na vyšetrovanie trestných činov a na využitie týchto údajov ako dôkazy na súde. Komisia preskúma opatrenia na **posilnenie kapacít v oblasti presadzovania práva pri digitálnom vyšetrovaní** a určí, ako čo najlepšie využívať výskum a vývoj na vytváranie nových nástrojov na presadzovanie práva a ako sa odbornou prípravou môže zabezpečiť správny súbor zručností v oblasti presadzovania práva a justície. Takisto to bude zahŕňať poskytovanie striktných vedeckých hodnotení a testovacích metód prostredníctvom spoločného výskumného centra Komisie.

Spoločný prístup môže zabezpečiť **integráciu umelej inteligencie, vesmírnych spôsobilostí, veľkých dát** (big data) a **vysokovýkonnej výpočtovej techniky** do bezpečnostnej politiky spôsobom, ktorý zabezpečí účinný boj proti trestnej činnosti a dodržiavanie základných práv. Umelá inteligencia by mohla fungovať ako významný nástroj na boj proti trestnej činnosti a vytvárať obrovské vyšetrovacie kapacity analýzou veľkého množstva informácií a identifikáciou modelov a anomálií.[62] Takisto môže poskytovať konkrétne nástroje, napríklad na pomoc pri identifikácii teroristického obsahu online, odhaľovaní podozrivých transakcií pri predaji nebezpečných výrobkov alebo poskytovaní pomoci občanom v núdzi. Využitie tohto potenciálu si bude vyžadovať prepojenie výskumu, inovácií a používateľov umelej inteligencie so správnou riadiacou a technickou infraštruktúrou s aktívnym zapojením súkromného sektora a akademickej obce. Takisto to znamená zabezpečenie maximálnej úrovne súladu so základnými právami a zároveň zabezpečenie účinnej ochrany občanov. Najmä rozhodnutia, ktoré sa týkajú občanov, musia byť predmetom preskúmania ľuďmi a musia byť v súlade s príslušnými platnými právnymi predpismi EÚ.[63]

Elektronické informácie a dôkazy sú potrebné približne v 85 % vyšetrovaní závažných trestných činov, zatiaľ čo 65 % všetkých požiadaviek je adresovaných poskytovateľom

[61] Oznámenie Komisie Formovanie digitálnej budúcnosti Európy z 19. februára 2020, COM(2020) 67.

[62] Napríklad v prípade hospodárskych trestných činov.

[63] Znamená to súlad s existujúcimi právnymi predpismi vrátane všeobecného nariadenia (EÚ) 2016/679 o ochrane osobných údajov, ako aj smernice (EÚ) 2016/680 o presadzovaní práva, ktorým sa upravuje spracúvanie osobných údajov na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií.

nachádzajúcim sa v inej jurisdikcii[64]. Skutočnosť, že tradičné fyzické stopy sa presunuli do online priestoru, ešte viac prehlbuje priepasť medzi schopnosťami orgánov presadzovania práva a páchateľov trestných činov. Je nevyhnutné zaviesť jasné pravidlá pre cezhraničný prístup k elektronickým dôkazom vo vyšetrovaní trestných činov. Preto je kľúčové, aby Európsky parlament a Rada rýchlo schválili návrhy týkajúce sa elektronických dôkazov, a poskytli tak pracovníkom v tejto oblasti účinný nástroj. Cezhraničný prístup k elektronickým dôkazom prostredníctvom mnohostranných a dvojstranných medzinárodných rokovaní je takisto kľúčový pre zavedenie kompatibilných pravidiel na medzinárodnej úrovni[65].

Prístup k digitálnym dôkazom takisto závisí od dostupnosti informácií. Ak sa údaje vymažú príliš rýchlo, môžu zmiznúť dôležité dôkazy, čím sa stráca možnosť identifikovať a lokalizovať podozrivých a zločinecké siete (ako aj obete). Systémy na uchovávanie údajov na druhej strane vyvolávajú otázky týkajúce sa ochrany súkromia. Komisia posúdi ďalšie smerovanie v oblasti uchovávania údajov v závislosti od výsledku konaní prebiehajúcich na Európskom súdnom dvore.

Prístup k informáciám o registrácii názvov internetových domén („údaje WHOIS“)[66] je dôležitý pre vyšetrovanie trestných činov, kybernetickú bezpečnosť a ochranu spotrebiteľov. Prístup k týmto informáciám je však čoraz ťažší, kdeže sa čaká na prijatie novej politiky v oblasti WHOIS Internetovou korporáciou pre prideľovanie mien a čísel (ICANN). Komisia bude naďalej pracovať s organizáciou ICANN a komunitou zainteresovaných strán s cieľom zabezpečiť, aby legitímni žiadatelia o prístup vrátane orgánov presadzovania práva mohli získať účinný prístup k údajom WHOIS v súlade s európskymi a medzinárodnými právnymi predpismi v oblasti ochrany údajov. Bude to zahŕňať posúdenie možných riešení vrátane toho, či by bolo potrebné prijať právne predpisy, v ktorých by sa objasnili pravidlá prístupu k takýmto informáciám.

Orgány presadzovania práva a justičné orgány musia byť takisto vybavené na to, aby mohli získavať potrebné údaje a dôkazy po tom, ako dôjde k plnému zavedeniu **architektúry 5G pre mobilné telekomunikácie** v EÚ, a to spôsobom, ktorý bude rešpektovať dôverný charakter komunikácie. Komisia bude podporovať posilnený a koordinovaný prístup pri vyvíjaní medzinárodných noriem, vymedzovaní najlepších postupov, procesov a technickej súčinnosti v kľúčových oblastiach, ako sú umelá inteligencia, internet vecí alebo technológie blockchainu.

Značná časť vyšetrovaní rôznych foriem trestných činov a terorizmu dnes zahŕňa **šifrované informácie**. Šifrovanie je pre digitálny svet nevyhnutné, keďže zabezpečuje digitálne systémy a transakcie a ochraňuje celý rad základných práv vrátane slobody prejavu, súkromia a ochrany údajov. Ak sa však využíva na kriminálne účely, môže takisto skrývať totožnosť páchateľov trestných činov a obsah ich komunikácie. Komisia bude skúmať a podporovať vyvážené technické, operačné a právne riešenia týchto výziev a bude presadzovať prístup, ktorý bude zachovávať účinnosť šifrovania v záujme ochrany súkromia a bezpečnosti komunikácie, a ktorý bude zároveň umožňovať účinnú reakciu na trestnú činnosť a terorizmus.

Boj proti nezákonnému internetovému obsahu

[64] Pracovný dokument útvarov Komisie SWD(2018) 118 final.

[65] Najmä Druhý dodatkový protokol k Budapeštianskemu dohovoru Rady Európy o kybernetickej bezpečnosti a dohoda medzi EÚ a Spojenými štátmi o cezhraničnom prístupe k elektronickým dôkazom.

[66] Uchovávané v databázach prevádzkovaných 2 500 správcami a registrátormi sídliacimi po celom svete.

Zosúladenie bezpečnosti online priestoru a fyzického prostredia znamená podniknúť ďalšie kroky v **boji proti nezákonnému internetovému obsahu**. Hlavné hrozby pre občanov, ako sú terorizmus, extrémizmus alebo sexuálne zneužívanie detí, čoraz viac závisia od digitálneho prostredia. To si vyžaduje konkrétne opatrenia a rámec, ktorých cieľom bude zabezpečiť rešpektovanie základných práv. Základným prvým krokom je rýchle uzavretie rokovaní o navrhovaných právnych predpisoch týkajúcich sa teroristického internetového obsahu[67] a zabezpečenie ich vykonávania. Posilnenie dobrovoľnej spolupráce medzi orgánmi presadzovania práva a súkromným sektorom v rámci **internetového fóra EÚ** je takisto kľúčové v boji proti zneužívaniu internetu zo strany teroristov, násilných extrémistov a páchateľov trestných činov. Jednotka EÚ pre nahlasovanie internetového obsahu agentúry Europol bude naďalej zohrávať kľúčovú úlohu v monitorovaní internetovej činnosti teroristických skupín a krokov podniknutých platformami[68], ako aj v ďalšom rozvoji **krízového protokolu EÚ**[69]. Komisia bude okrem toho naďalej spolupracovať s medzinárodnými partnermi, okrem iného aj účasťou na **globálnom internetovom fóre na boj proti terorizmu**, s cieľom riešiť tieto výzvy na globálnej úrovni. Ďalej bude podporovať rozvoj alternatívneho naratívu a protiargumentácie prostredníctvom programu na posilnenie postavenia občianskej spoločnosti[70].

S cieľom zabrániť a bojovať proti šíreniu nezákonných nenávistných prejavov na internete vydala Komisia v roku 2016 kódex správania týkajúci sa nezákonných nenávistných prejavov na internete, v rámci ktorého sa online platformy zaväzujú odstraňovať obsah s nenávistnými prejavmi. Podľa posledných hodnotení posudzujú spoločnosti 90 % nahláseného obsahu do 24 hodín a odstránia 71 % obsahu považovaného za nezákonný nenávistný prejav. Platformy však musia ďalej zlepšovať transparentnosť a spätnú väzbu pre používateľov a zabezpečiť jednotné vyhodnocovanie nahláseného obsahu[71].

Internetové fórum EÚ takisto uľahčí výmenu o existujúcich a vyvíjaných technológiách na riešenie výziev týkajúcich sa sexuálneho zneužívania detí online. Riešenie sexuálneho zneužívania detí online je jadrom novej stratégie na zintenzívnenie **boja proti sexuálnemu zneužívaniu detí**[72], ktorej cieľom bude maximalizovať používanie nástrojov dostupných na úrovni EÚ v boji proti týmto trestným činom. Spoločnosti musia byť schopné pokračovať vo svojej práci v odhaľovaní a odstraňovaní detskej internetovej pornografie a škody spôsobené týmto materiálom si vyžadujú rámec stanovujúci jasné a trvalé povinnosti zamerané na riešenie tohto problému. V stratégii sa takisto bude uvádzať, že Komisia takisto začne s prípravou sektorových právnych predpisov na účinnejší boj proti detskej internetovej pornografii pri plnom rešpektovaní základných práv.

Všeobecnejšie platí, že v nadchádzajúcom akte o digitálnych službách sa takisto objasnia a aktualizujú pravidlá týkajúce sa zodpovednosti a bezpečnosti digitálnych služieb a odstránia sa prekážky brániace prijímaniu opatrení na boj proti nezákonnému obsahu, tovaru alebo nezákonným službám.

Okrem toho bude Komisia naďalej spolupracovať s medzinárodnými partnermi a s **globálnym internetovým fórom na boj proti terorizmu**, a to aj prostredníctvom nezávislého poradného výboru, s cieľom diskutovať o riešení týchto výziev na globálnej

[67] Návrh o predchádzaní šíreniu teroristického obsahu online, COM(2018) 640, 12. september 2018.
[68] Europol, november 2019.
[69] Európa, ktorá chráni – krízový protokol EÚ: reakcia na teroristický internetový obsah, (október 2019).
[70] Spojené s prácou v rámci programu na zvyšovanie povedomia o radikalizácii, pozri oddiel IV.3.
[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf.
[72] Stratégia EÚ na účinnejší boj proti sexuálnemu zneužívaniu detí, COM(2020) 607.

úrovni pri súčasnom rešpektovaní hodnôt EÚ a základných práv. Malo by sa hovoriť aj o nových témach, ako sú algoritmy alebo online hry[73].

Hybridné hrozby

Hybridné hrozby sa v súčasnosti vyskytujú v nevídanej miere a rozmanitosti. Ešte výraznejšie sa to prejavilo počas krízy spôsobenej ochorením COVID-19. Viacero štátnych aj neštátnych subjektov sa snažilo pandémiu zneužiť, a to najmä prostredníctvom manipulácie s informačným prostredím a útokov na základné infraštruktúry. Tým sa oslabuje sociálna súdržnosť a naštrbuje dôvera v inštitúcie EÚ a verejné správy členských štátov.

Prístup EÚ k hybridným hrozbám sa stanovuje v spoločnom rámci z roku 2016[74] a v spoločnom oznámení z roku 2018 o posilňovaní odolnosti voči hybridným hrozbám[75]. Opatrenie na úrovni EÚ je podporené rozsiahlym súborom nástrojov, ktorý sa týka prepojenia medzi vnútornou a vonkajšou bezpečnosťou a vychádza z celospoločenského prístupu a úzkej spolupráce so strategickými partnermi, najmä NATO a G7. Zároveň s touto stratégiou sa zverejňuje aj správa o vykonávaní prístupu EÚ k hybridným hrozbám[76]. Na základe mapovania[77] predloženého súčasne s touto stratégiou vytvoria útvary Komisie a Európska služba pre vonkajšiu činnosť **obmedzenú online platformu**, ktorá bude obsahovať informácie pre členské štáty o nástrojoch a opatreniach na úrovni EÚ na boj proti hybridným hrozbám.

Hoci zodpovednosť za boj proti hybridným hrozbám leží v prvom rade na pleciach členských štátov, pretože prirodzene súvisí s národnou bezpečnosťou a obrannými politikami, niektoré slabé miesta majú spoločné všetky členské štáty a určité hrozby sú cezhraničné, ako napríklad zacielenie na cezhraničné siete alebo infraštruktúru. Komisia a vysoký predstaviteľ stanovia prístup EÚ k hybridným hrozbám, v ktorom sa bude hladko integrovať vonkajší aj vnútorný rozmer a v ktorom sa bude prihliadať na aspekty na úrovni jednotlivých členských štátov, ako aj celej EÚ. Musí sa týkať celého spektra opatrení, od včasného odhaľovania, analýzy, zvyšovania informovanosti, budovania odolnosti a prevencie až po reakciu na krízu a riadenie následkov.

Vzhľadom na neustály vývoj v oblasti hybridných hrozieb sa bude okrem intenzívnejšieho vykonávania klásť osobitný dôraz na **začlenenie hybridných aspektov do tvorby politík**, aby sa naďalej udržal krok s dynamickým vývojom a aby sa zabezpečilo, že sa neprehliadne žiadna potenciálne relevantná iniciatíva. Aj účinky nových iniciatív sa budú posudzovať optikou hybridných hrozieb, a to aj iniciatív v oblastiach, ktoré boli dosiaľ mimo záujmu rámca boja proti hybridným hrozbám, ako sú vzdelávanie, technológie a výskum. Pri tomto prístupe by sa využilo úsilie vyvinuté v oblasti konceptualizácie hybridných hrozieb zabezpečujúcej komplexný pohľad na rôzne nástroje, ktoré môžu nepriatelia využívať[78].

---

[73] Teroristi čoraz častejšie využívajú na vzájomnú komunikáciu systémy posielania správ na herných platformách a mladí teroristi si takisto vo videohrách prehrávajú násilné útoky.

[74] Spoločný rámec pre boj proti hybridným hrozbám – reakcia Európskej únie, JOIN(2016) 18.

[75] Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby, JOIN(2018) 16.

[76] SWD(2020) 153, správa o vykonávaní spoločného rámca pre boj proti hybridným hrozbám z roku 2016 a spoločného oznámenia o zvyšovaní odolnosti a posilňovaní spôsobilosti riešiť hybridné hrozby z roku 2018.

[77] SWD(2020) 152, Mapovanie opatrení súvisiacich s posilňovaním odolnosti a bojom proti hybridným hrozbám.

[78] *The Landscape of Hybrid Threats: A conceptual Model* (Prostredie hybridných hrozieb: koncepčný model), JRC117280, vypracované na základe spolupráce medzi Spoločným výskumným centrom a Európskym centrom excelentnosti pre boj proti hybridným hrozbám.

Cieľom by malo byť zabezpečiť podporu rozhodovacieho procesu pravidelným podávaním komplexných správ o vývoji v oblasti hybridných hrozieb na základe spravodajských informácií. To bude vo veľkej miere závisieť od spravodajských informácií členských štátov a ďalšieho posilňovania spravodajskej spolupráce s príslušnými službami členských štátov prostredníctvom centra EU INTCEN.

Na prehĺbenie **situačnej informovanosti** preskúmajú útvary Komisie a Európska služba pre vonkajšiu činnosť možnosti uľahčenia tokov informácií z rôznych zdrojov, a to aj členských štátov a agentúr EÚ ako ENISA, Europol a Frontex. Kontaktným miestom EÚ pre posudzovanie hybridných hrozieb bude naďalej stredisko EÚ pre hybridné hrozby. Z hľadiska predchádzania hybridným hrozbám a ochrany pred nimi je kľúčové **budovanie odolnosti**. Preto je mimoriadne dôležité systematicky sledovať a objektívne merať pokrok dosahovaný v tejto oblasti. Prvým krokom bude určenie odvetvových základných scenárov odolnosti voči hybridným hrozbám pre členské štáty aj inštitúcie a orgány EÚ. A napokon by sa mal v záujme zlepšenia **pripravenosti reakcie na hybridné krízy** preskúmať aj existujúci protokol vymedzený v operačnom protokole EÚ z roku 2016[79], a to tak, aby sa v ňom zohľadnilo rozsiahlejšie preskúmanie a posilnenie systému EÚ v oblasti reakcie na krízy, o ktorom sa v súčasnosti rokuje[80]. Cieľom je maximalizovať účinok opatrenia EÚ rýchlym zosúladením reakcií odvetví a zabezpečením bezproblémovej spolupráce s našimi partnermi, predovšetkým s NATO.

Kľúčové opatrenia
• zabezpečenie vykonávania právnych predpisov v oblasti počítačovej kriminality a ich vhodnosti na daný účel, • stratégia na účinnejší boj proti sexuálnemu zneužívaniu detí, • návrhy na odhaľovanie a odstraňovanie detskej pornografie, • prístup EÚ k boju proti hybridným hrozbám, • preskúmanie operačného protokolu EÚ na boj proti hybridným hrozbám (operačný protokol EÚ), • posúdenie možností posilnenia kapacity v oblasti presadzovania práva pri digitálnych vyšetrovaniach.

3. Ochrana Európanov pred terorizmom a organizovanou trestnou činnosťou

Terorizmus a radikalizácia

Teroristická hrozba v EÚ je naďalej vysoká. Útoky môžu mať stále ničivý účinok napriek tomu, že celkovo sa ich počet znížil. Radikalizácia môže spôsobovať aj širšiu polarizáciu a destabilizáciu v oblasti sociálnej súdržnosti. V boji proti terorizmu a radikalizácii nesú primárnu zodpovednosť členské štáty. Neustále sa zintenzívňujúci cezhraničný/medziodvetvový rozmer tejto hrozby si však žiada prijatie ďalších krokov v oblasti spolupráce a koordinácie na úrovni EÚ. Prioritou je účinné vykonávanie právnych

[79] Operačný protokol EÚ na boj proti hybridným hrozbám (operačný protokol EÚ), SWD(2016) 227.

[80] Po videokonferencii z 26. marca 2020 prijali členovia Európskej rady vyhlásenie o opatreniach EÚ v reakcii na pandémiu ochorenia COVID-19, v ktorom vyzvali Komisiu na predloženie návrhov ambicióznejšieho a rozsiahlejšieho systému krízového riadenia v rámci EÚ.

predpisov EÚ v oblasti boja proti terorizmu vrátane reštriktívnych opatrení[81]. Naďalej je cieľom rozšíriť mandát Európskej prokuratúry v oblasti cezhraničných trestných činov terorizmu.

Boj proti terorizmu sa začína riešením jeho základných príčin. Zraniteľnosť ľudí voči radikalizmu môžu prehlbovať faktory ako polarizácia spoločnosti, skutočná alebo pociťovaná diskriminácia a ďalšie psychologické a sociologické faktory. V tejto súvislosti je riešenie **radikalizácie** úzko spojené s posilňovaním sociálnej súdržnosti na miestnej, vnútroštátnej a európskej úrovni. Za posledných desať rokov bolo vypracovaných niekoľko iniciatív a politík s veľkým vplyvom, a to najmä vďaka sieti na zvyšovanie povedomia o radikalizácii a iniciatívy Mestá EÚ proti radikalizácii[82]. Je čas zamyslieť sa nad opatreniami na zjednodušenie politík a iniciatív EÚ, ako aj prístupu k finančným prostriedkom EÚ na riešenie radikalizácie. Takýmito opatreniami sa môže podporiť rozvoj schopností a zručností, rozšíriť spolupráca, posilniť dôkazová základňa a prispieť k hodnoteniu pokroku, pričom ich súčasťou môžu byť všetky zainteresované strany vrátane odborníkov z prvej línie, tvorcov politík a akademickej obce[83]. K predchádzaniu radikalizácii môžu prispievať aj mäkké politiky ako vzdelávanie, kultúra, mládežnícke a športové aktivity, keďže môžu predstavovať príležitosti pre ohrozenú mládež a súdržnosť v rámci EÚ[84]. K prioritným oblastiam patrí úsilie v oblasti včasného odhaľovania a riadenia rizík, budovania odolnosti a rušenia väzieb, ako aj rehabilitácie a opätovného začlenenia do spoločnosti.

Teroristi sa snažia získať a premeniť na zbraň **chemické, biologické, rádiologické a jadrové** (CBRN)[85] materiály, ako aj rozvíjať svoje poznatky a kapacity na ich používanie[86]. Potenciálu CBRN útokov je v teroristickej propagande vyhradený značný priestor. Vzhľadom na obrovské škody, ktoré môžu spôsobiť, je im potrebné venovať osobitnú pozornosť. Na základe prístupu, ktorý sa využil pri regulovaní prístupu k prekurzorom výbušnín, Komisia preskúma obmedzenie prístupu k určitým nebezpečným chemickým látkam, ktoré by bolo možné využiť na uskutočňovanie útokov. Kľúčovým bude aj rozvoj kapacít reakcie civilnej ochrany EÚ (rescEU) v oblasti CBRN. Na posilnenie spoločnej kultúry bezpečnosti a ochrany v oblasti CBRN je dôležitá aj spolupráca s tretími krajinami pri plnom využívaní globálnych CBRN centier excelentnosti EÚ. Táto spolupráca bude zahŕňať vnútroštátne posudzovanie nedostatkov a rizík, podporu vnútroštátnych a regionálnych akčných plánov v oblasti CBRN bezpečnosti, výmeny osvedčených postupov a činnosti budovania kapacít v oblasti CBRN.

EÚ vypracovala najmodernejšie právne predpisy na svete v oblasti obmedzenia prístupu k **prekurzorom výbušnín**[87] a odhaľovania podozrivých transakcií zameraných na výrobu improvizovaných výbušných zariadení. Hrozba vyplývajúca z podomácky vyrobených

[81] Rada prijala reštriktívne opatrenia, pokiaľ ide o ISIL (Dá'iš) a sieť al-Káida, ako aj osobitné reštriktívne opatrenia zamerané na určité osoby a subjekty s cieľom bojovať proti terorizmu. Prehľad všetkých reštriktívnych opatrení pozri v mape sankcií EÚ (https://www.sanctionsmap.eu/#/main).

[82] Pilotná iniciatíva Mestá EÚ proti radikalizácii má dva ciele: posilniť výmenu odborných znalostí medzi mestami EÚ a zhromažďovať spätnú väzbu o spôsoboch, akými možno najlepšie podporiť miestne komunity na úrovni EÚ.

[83] Napríklad financovanie z Európskeho fondu bezpečnosti a programu Občianstvo.

[84] Opatrenia EÚ, ako napríklad virtuálne výmeny v rámci programu Erasmus+, eTwinning.

[85] Za posledné dva roky sa vyskytlo niekoľko prípadov použitia biologických agensov (zvyčajne rastlinných toxínov) v Európe (Francúzsko, Nemecko, Taliansko) aj inde vo svete (Tunisko, Indonézia).

[86] Rada prijala reštriktívne opatrenia proti šíreniu a používaniu chemických zbraní.

[87] Chemické látky, ktoré možno zneužiť na prípravu podomácky vyrobených výbušnín. Regulujú sa v nariadení (EÚ) 2019/1148 o uvádzaní prekurzorov výbušnín na trh a ich používaní.

výbušnín však zostáva naďalej vysoká, keďže takéto výbušniny už boli viackrát použité pri útokoch v rámci EÚ[88]. Prvým krokom musí byť vykonávanie pravidiel a zabezpečenie toho, aby sa v online prostredí nedali obchádzať kontroly.

Dôležitým prvkom politiky boja proti terorizmu je aj účinné trestné stíhanie tých, ktorí trestné činy terorizmu páchajú, a to vrátane **zahraničných teroristických bojovníkov**, ktorí sa v súčasnosti nachádzajú v Sýrii a Iraku. Hoci túto problematiku riešia predovšetkým členské štáty, koordinácia a podpora na úrovni EÚ im môže pomôcť pri riešení spoločných výziev. Dôležitý krok bude predstavovať úsilie zamerané na úplné vykonanie právnych predpisov v oblasti bezpečnosti hraníc[89] a plné využívanie všetkých relevantných databáz EÚ na výmenu informácií o známych podozrivých osobách. Okrem identifikácie vysokorizikových osôb je potrebná aj politika v oblasti opätovného začlenenia do spoločnosti a rehabilitácie. Na základe medziprofesijnej spolupráce, a to aj s väzenskými a probačnými pracovníkmi, sa v súdnictve zlepší chápanie procesov radikalizácie vedúcej k násilnému extrémizmu, ako aj prístup súdnictva k vynášaniu rozsudkov a alternatívam k zadržiavaniu.

Problém zahraničných teroristických bojovníkov symbolizuje prepojenie medzi vnútornou a **vonkajšou bezpečnosťou.** Spolupráca v oblasti boja proti terorizmu, ako aj predchádzania radikalizácii a násilnému extrémizmu a boja proti nim je nevyhnutným predpokladom zaistenia bezpečnosti v rámci EÚ[90]. Je potrebné ďalej rozvíjať partnerstvá a spoluprácu v oblasti boja proti terorizmu s krajinami v susedstve aj mimo neho na základe odborných znalostí siete odborníkov EÚ na boj proti terorizmu/bezpečnosť. Vhodnou referenciou pre takúto zacielenú spoluprácu je spoločný akčný plán boja proti terorizmu na západnom Balkáne. Úsilie by sa malo vyvinúť najmä na podporu kapacity partnerských krajín pri identifikovaní a lokalizácii zahraničných teroristických bojovníkov. EÚ bude naďalej podporovať viacstrannú spoluprácu a spolupracovať s najvýznamnejšími globálnymi subjektmi v tejto oblasti, ako sú Organizácia Spojených národov, NATO, Rada Európy, Interpol a OBSE. Bude sa zapájať aj do činnosti Globálneho fóra pre boj proti terorizmu a globálnej koalície na boj proti Dá'iš, ako aj spolupracovať s príslušnými subjektmi občianskej spoločnosti. Pri spolupráci s tretími krajinami v oblasti predchádzania terorizmu a pirátstvu zohrávajú dôležitú úlohu aj nástroje vonkajšej politiky Únie vrátane rozvoja a spolupráce. Medzinárodná spolupráca je nevyhnutná aj na prerušenie všetkých zdrojov **financovania terorizmu**, napríklad prostredníctvom Finančnej akčnej skupiny.

Organizovaná trestná činnosť

Organizovaná trestná činnosť má za následok obrovské hospodárske aj osobné náklady. Hospodárske straty v dôsledku organizovanej trestnej činnosti a korupcie sa ročne odhadujú na úrovni od 218 do 282 miliárd EUR.[91] V roku 2017 bolo v Európe vyšetrovaných viac ako 5 000 organizovaných zločineckých skupín – čo je v porovnaní s rokom 2013 nárast

[88] Medzi takéto ničivé útoky patria napríklad útoky v Osle (2011), Paríži (2015), Bruseli (2016) a Manchestri (2017). Pri útoku podomácky vyrobenou výbušninou v Lyone (2019) bolo zranených 13 osôb.

[89] Vrátane nového mandátu Európskej agentúry pre pohraničnú a pobrežnú stráž (Frontex).

[90] V záveroch Rady zo 16. júna 2020 sa zdôraznila potreba ochrany občanov Únie pred terorizmom a násilným extrémizmom vo všetkých ich formách a bez ohľadu na ich pôvod, ako aj potreba ďalšieho posilnenia vonkajšieho zapojenia EÚ do boja proti terorizmu a opatrení EÚ v tejto oblasti v niektorých prioritných geografických a tematických oblastiach.

[91] V hrubom domácom produkte (HDP); správa Europolu: *Does crime still pay? – Criminal asset recovery in the EU* (Vypláca sa ešte trestná činnosť? – Vymáhanie majetku pochádzajúceho z trestnej činnosti v EÚ), 2016.

o 50 %.[92] Organizovaná trestná činnosť sa čoraz častejšie uskutočňuje cezhranične, a to aj z krajín v bezprostrednom susedstve EÚ, a preto je potrebná intenzívna operačná spolupráca a výmena informácií s partnermi v susedstve.

Vynárajú sa nové výzvy a trestná činnosť sa presúva na internet: počas pandémie ochorenia COVID-19 došlo k obrovskému nárastu online podvodov spáchaných na zraniteľných skupinách osôb, ako aj ku krádežiam a k vlámaniam v súvislosti so zdravotníckymi a hygienickými výrobkami.[93] EÚ musí zvýšiť úsilie v boji proti organizovanej trestnej činnosti, a to aj na medzinárodnej úrovni, a vypracovať viac nástrojov na rozkladanie obchodného modelu organizovanej trestnej činnosti. Boj proti organizovanej trestnej činnosti si vyžaduje aj úzku spoluprácu s miestnymi a regionálnymi verejnými správami, ako aj s občianskou spoločnosťou, teda s kľúčovými partnermi v oblasti predchádzania trestnej činnosti aj poskytovania pomoci a podpory jej obetiam, pričom je osobitne potrebné spolupracovať s verejnými správami v pohraničných regiónoch. Toto úsilie sa zlúči v **agende boja proti organizovanej trestnej činnosti**.

Viac ako tretina organizovaných zločineckých skupín pôsobiacich v EÚ je zapojená do výroby a distribúcie drog alebo obchodovania s nimi. Drogová závislosť spôsobila v roku 2019 v EÚ viac ako osemtisíc úmrtí na predávkovanie. Väčšina **obchodovania s drogami** sa uskutočňuje cezhranične, pričom veľká časť zisku sa infiltruje do legálneho hospodárstva.[94] Novou agendou EÚ v oblasti drog[95] sa posilní úsilie EÚ a jej členských štátov v oblasti znižovania dopytu po drogách a ich ponuky, keďže sa v nej vymedzia jednotné akcie na riešenie spoločného problému a posilnenie dialógu a spolupráce medzi EÚ a jej externými partnermi v drogovej problematike. Po vyhodnotení, ktoré uskutoční Európske monitorovacie centrum pre drogy a drogovú závislosť, Komisia posúdi, či je potrebné aktualizovať jej mandát, aby mohla plniť nové úlohy.

Organizované zločinecké skupiny a teroristi sú kľúčovými aktérmi aj v obchodovaní s **nelegálnymi palnými zbraňami**. V rokoch 2009 až 2018 došlo v Európe k 23 masovým streľbám, ktoré si vyžiadali viac ako 340 ľudských životov.[96] Palné zbrane sa do EÚ často dostávajú z krajín v jej bezprostrednom susedstve.[97] To poukazuje na potrebu posilniť koordináciu a spoluprácu v rámci EÚ aj s medzinárodnými partnermi, najmä Interpolom, v záujme harmonizovania získavania informácií a podávania správ o zaisteniach palných zbraní. Mimoriadne dôležité je aj zlepšiť vysledovateľnosť zbraní, a to aj na internete, a zabezpečiť výmenu informácií medzi osvedčujúcimi orgánmi a orgánmi presadzovania práva. Komisia predkladá nový **akčný plán EÚ na boj proti nedovolenému obchodovaniu s palnými zbraňami**[98] a posúdi aj to, či sú na daný účel stále vhodné pravidlá týkajúce sa vývozných povolení, ako aj opatrenia týkajúce sa dovozu a tranzitu palných zbraní[99].

---

92 Europol, Hodnotenie hrozieb závažnej a organizovanej trestnej činnosti (SOCTA), 2013 a 2017.

93 Europol, 2020.

94 Správa centra EMCDDA a Europolu o trhoch s drogami v EÚ z roku 2019 (november 2019).

95 Agenda a akčný plán EÚ v oblasti drog na roky 2021 – 2025, COM(2020) 606.

96 Flámsky mierový inštitút, *Armed to kill* (Ozbrojení a nebezpeční) (október 2019).

97 EÚ od roku 2002 financuje v regióne boj proti šíreniu ručných a ľahkých zbraní a obchodovaniu s nimi; financuje pritom najmä sieť odborníkov juhovýchodnej Európy pre strelné zbrane (SEEFEN). Od roku 2019 sú partneri zo západného Balkánu plnou súčasťou priority Strelné zbrane Európskej multidisciplinárnej platformy proti hrozbám trestnej činnosti (EMPACT).

98 COM(2020) 608.

99 Nariadenie (EÚ) č. 258/2012, ktorým sa vykonáva článok 10 Protokolu Organizácie Spojených národov proti nezákonnej výrobe a obchodovaniu so strelnými zbraňami.

Zločinecké organizácie zaobchádzajú s migrantmi a osobami, ktoré potrebujú medzinárodnú ochranu, ako s tovarom. 90 % neregulárnych migrantov do EÚ privádza zločinecká sieť.[100] Prevádzačstvo migrantov sa často prelína aj s ďalšími formami organizovanej trestnej činnosti, najmä s obchodovaním s ľuďmi[101]. Okrem obrovského množstva obetí, ktoré má na svedomí obchodovanie s ľuďmi, plynie podľa odhadov Europolu zo všetkých foriem vykorisťovania z obchodovania s ľuďmi ročný zisk na celosvetovej úrovni vo výške 29,4 miliardy EUR. Je to cezhraničná trestná činnosť, ktorá existuje v dôsledku nezákonného dopytu v rámci EÚ aj mimo nej a ktorá ovplyvňuje všetky členské štáty EÚ. Nedostatočné výsledky pri odhaľovaní, stíhaní a odsudzovaní týchto trestných činov znamenajú, že je potrebný nový prístup, ktorým sa toto opatrenie zlepší. V novom **komplexnom prístupe k obchodovaniu s ľuďmi** sa jednotlivé opatrenia zjednotia. Okrem toho Komisia predstaví aj **nový akčný plán EÚ proti prevádzačstvu migrantov** na roky 2021 – 2025. Obe oblasti činnosti sa budú zameriavať na boj proti zločineckým sieťam, posilnenie spolupráce a podporu pri presadzovaní práva.

Organizované zločinecké skupiny, ako aj teroristi hľadajú príležitosti aj v iných oblastiach, **a** to najmä také, z ktorých plynú vysoké zisky pri nízkom riziku odhalenia, ako sú **trestné činy proti životnému prostrediu**. Nezákonný lov a nezákonné obchodovanie s voľne žijúcimi druhmi, nezákonná ťažba nerastných surovín a dreva a nezákonné zneškodňovanie a preprava odpadu tvoria štvrtý najväčší nezákonný obchod na svete[102]. Na páchanie trestnej činnosti sa zneužívajú aj systémy obchodovania s emisiami a energetické certifikačné systémy a rovnako tak sa zneužívajú finančné prostriedky vyčlenené na environmentálnu odolnosť a trvalo udržateľný rozvoj. Komisia podporuje zintenzívňovanie opatrení EÚ, členských štátov a medzinárodného spoločenstva v boji proti trestným činom proti životnému prostrediu[103] a posudzuje, či je smernica o trestných činoch proti životnému prostrediu[104] stále vhodná na daný účel. Medzi najlukratívnejšie trestné činnosti patrí aj **nedovolené obchodovanie s kultúrnymi objektmi**, ktoré je momentálne na vzostupe a z ktorého sa financujú teroristi, ako aj organizovaná trestná činnosť. Mali by sa preskúmať možné kroky na zlepšenie online aj offline vysledovateľnosti kultúrnych objektov na vnútornom trhu a spolupráce s tretími krajinami, v ktorých sa kultúrne objekty lúpia, a zároveň by sa mala poskytovať aktívna podpora presadzovaniu práva a vedeckým komunitám.

Hospodárska a finančná trestná činnosť je veľmi zložitá, každoročne však ovplyvňuje milióny občanov a tisícky spoločností v EÚ. Boj proti podvodom je mimoriadne dôležitý a vyžaduje si opatrenie na úrovni EÚ. Europol spolu s Eurojustom, Európskou prokuratúrou a Európskym úradom pre boj proti podvodom podporuje členské štáty a EÚ pri ochrane hospodárskych a finančných trhov a peňazí daňovníkov EÚ. Európska prokuratúra bude plne funkčná na konci roka 2020 a bude sa venovať vyšetrovaniu, stíhaniu a podávaniu žalôb v súvislosti s trestnými činmi ohrozujúcimi rozpočet EÚ, ako sú podvod, korupcia a pranie špinavých peňazí. Riešiť bude aj cezhraničné podvody týkajúce sa DPH, ktoré stoja daňovníkov každý rok minimálne 50 miliárd EUR.

[100] Zdroj: Europol.
[101] Europol, EMSC, 4. výročná správa.
[102] UNEP-INTERPOL, hodnotenie rýchlej reakcie: Nárast trestných činov proti životnému prostrediu, jún 2016.
[103] Pozri Európska zelená dohoda, COM(2019) 640 final.
[104] Smernica 2008/99/ES o ochrane životného prostredia prostredníctvom trestného práva.

Komisia bude podporovať aj rozvoj odborných znalostí a vypracovanie legislatívneho rámca v oblasti nových rizík, ako sú kryptoaktíva a nové platobné systémy. Konkrétne sa bude Komisia zaoberať reakciou na vznik kryptoaktív, ako je bitcoin, a vplyvom, ktorý budú mať tieto nové technológie na vydávanie, výmenu, zdieľanie a sprístupňovanie finančných aktív.

V Európskej únii by mala byť nulová tolerancia nelegálnych peňazí. Za tridsať rokov vypracovala EÚ pevný regulačný rámec na predchádzanie **praniu špinavých peňazí** a financovaniu terorizmu a boj proti nim, ktorý plne vyhovuje potrebe ochrany osobných údajov. Panuje však zhoda v tom, že vykonávanie súčasného rámca je potrebné podstatne zlepšiť. Takisto je potrebné vyriešiť aj veľké rozdiely v spôsobe jeho uplatňovania, ako aj závažné nedostatky pri presadzovaní pravidiel. Ako bolo podrobne vysvetlené v akčnom pláne z mája 2020[105], prebieha posudzovanie možností zlepšenia rámca EÚ v oblasti boja proti praniu špinavých peňazí a financovaniu terorizmu. Medzi oblasti, ktoré sa majú preskúmať, patrí aj vzájomné prepojenie národných centralizovaných registrov bankových účtov, ktorým by sa mohol do veľkej miery zrýchliť prístup finančných spravodajských jednotiek a príslušných orgánov k finančným informáciám.

Zisky organizovaných zločineckých skupín v EÚ sa odhadujú na 110 miliárd EUR ročne. Aktuálnu reakciu tvoria harmonizované právne predpisy o konfiškácii a vymáhaní majetku[106] na zlepšenie zaistenia a konfiškácie majetku pochádzajúceho z trestnej činnosti v EÚ a na uľahčenie vzájomnej dôvery a účinnej cezhraničnej spolupráce medzi členskými štátmi. Skonfiškuje sa však iba 1 % týchto ziskov[107], čo organizovaným zločineckým skupinám umožňuje investovať do rozširovania svojich trestných činností a infiltrovať sa do legálneho hospodárstva, pričom hlavným cieľom prania špinavých peňazí sú malé a stredné podniky, ktoré majú ťažkosti s prístupom k úverom. Komisia bude analyzovať vykonávanie právnych predpisov[108] a prípadnú potrebu ďalších spoločných pravidiel vrátane pravidiel týkajúcich sa konfiškácie bez odsudzujúceho rozsudku. Aj úrady pre vyhľadávanie majetku[109], ktoré predstavujú kľúčových aktérov v procese vymáhania majetku, by mohli byť vybavené lepšími nástrojmi na rýchlejšie identifikovanie a vysledovanie majetku v EÚ v záujme zvýšenia miery konfiškácie.

Medzi organizovanou trestnou činnosťou a **korupciou** existuje silné prepojenie. Podľa približných odhadov stojí len samotná korupcia hospodárstvo EÚ ročne 120 miliárd EUR.[110] Predchádzanie korupcii a boj proti nej budú naďalej predmetom pravidelného monitorovania na základe mechanizmu právneho štátu, ako aj európskeho semestra. V rámci európskeho semestra sa posúdili výzvy v oblasti boja proti korupcii, akými sú verejné obstarávanie, verejná správa, podnikateľské prostredie alebo zdravotná starostlivosť. Nová výročná správa Komisie o právnom štáte sa bude týkať boja proti korupcii a umožní sa ňou preventívny dialóg s vnútroštátnymi orgánmi a zainteresovanými stranami na úrovni EÚ aj na vnútroštátnej úrovni. Organizácie občianskej spoločnosti môžu takisto zohrávať kľúčovú

[105] Akčný plán predchádzania praniu špinavých peňazí a financovaniu terorizmu, COM(2020) 2800.

[106] Podľa práva EÚ sa vyžaduje, aby boli vo všetkých členských štátoch zriadené úrady pre vyhľadávanie majetku.

[107] Správa o vymáhaní majetku a konfiškácii: zabezpečenie, aby sa trestná činnosť nevyplácala, COM(2020) 217 final.

[108] Smernica 2014/42/EÚ o zaistení a konfiškácii prostriedkov a príjmov z trestnej činnosti v Európskej únii.

[109] Rozhodnutie Rady 2007/845/SVV o spolupráci medzi úradmi pre vyhľadávanie majetku v členských štátoch pri vypátraní a identifikácii príjmov z trestnej činnosti alebo iného majetku súvisiaceho s trestnou činnosťou.

[110] Odhadnutie celkových hospodárskych nákladov korupcie je zložité, hoci z úsilia orgánov ako Medzinárodná obchodná komora, Transparency International, globálny pakt OSN a Svetové ekonomické fórum v tejto oblasti vyplýva, že korupcia je na úrovni 5 % svetového HDP.

úlohu pri motivovaní subjektov verejného sektora k prijímaniu opatrení na predchádzanie organizovanej trestnej činnosti a korupcii a boj s nimi, pričom tieto skupiny by mohli prakticky spolupracovať v spoločnom fóre. Vzhľadom na ich cezhraničnú povahu je ďalším kľúčovým rozmerom spolupráca a pomoc v otázkach organizovanej trestnej činnosti a korupcie so susednými regiónmi EÚ.

Kľúčové opatrenia
• protiteroristická agenda pre EÚ vrátane obnovených opatrení proti radikalizácii v EÚ, • nová spolupráca s kľúčovými tretími krajinami a medzinárodnými organizáciami v boji proti terorizmu, • agenda boja proti organizovanej trestnej činnosti vrátane obchodovania s ľuďmi, • agenda v oblasti drog a akčný plán EÚ na roky 2021 – 2025, • posúdenie vykonané Európskym monitorovacím centrom pre drogy a drogovú závislosť, • akčný plán EÚ na boj proti nedovolenému obchodovaniu s palnými zbraňami na roky 2020 – 2025, • preskúmanie právnych predpisov o zaistení a konfiškácii majetku, ako aj o úradoch pre vyhľadávanie majetku, • posúdenie smernice o trestných činoch proti životnému prostrediu, • akčný plán EÚ proti prevádzačstvu migrantov na roky 2021 – 2025.

4. Pevný európsky bezpečnostný ekosystém

O budovanie skutočnej a účinnej bezpečnostnej únie sa musia snažiť všetky zložky spoločnosti. Verejné správy, orgány presadzovania práva, súkromný sektor, vzdelávacie inštitúcie a občania samotní musia byť zapojení, vybavení a riadne prepojení, aby mohli budovať pripravenosť a odolnosť pre všetkých, najmä však pre tých najzraniteľnejších, obete a svedkov.

Všetky politiky musia mať bezpečnostný rozmer, ku ktorému môže EÚ prispievať na všetkých úrovniach. K najzávažnejším bezpečnostným rizikám v domácnosti patrí domáce násilie. V EÚ zažilo násilie zo strany svojho intímneho partnera 22 % žien[111]. Pristúpenie EÚ k Istanbulskému dohovoru o predchádzaní násiliu na ženách a domácemu násiliu a o boji proti nemu zostáva kľúčovou prioritou. Ak by boli rokovania naďalej blokované, Komisia prijme iné opatrenia na dosiahnutie cieľov dohovoru, ku ktorým bude patriť aj návrh na začlenenie násilia na ženách do zoznamu trestných činov EÚ, ktoré sú vymedzené v zmluve.

Spolupráca a výmena informácií

Jedným z najvýznamnejších spôsobov, ako môže EÚ prispieť k ochrane občanov, je zabezpečenie dobrej spolupráce tých, ktorí sú za bezpečnosť zodpovední. Najsilnejšími nástrojmi na boj proti trestnej činnosti a terorizmu a na dosahovanie spravodlivosti sú spolupráca a výmena informácií. Ak majú byť účinné, musia byť cielené a včasné. A ak majú byť dôveryhodné, musia byť doplnené o spoločné záruky a kontroly.

Na účely ďalšieho rozvoja **operačnej spolupráce členských štátov pri presadzovaní práva** bolo zavedených viacero nástrojov EÚ a odvetvových stratégií[112]. Jedným z hlavných

[111] Únia rovnosti: stratégia pre rodovú rovnosť na roky 2020 – 2025, COM(2020) 152.

[112] Napríklad akčný plán stratégie námornej bezpečnosti EÚ, ktorý viedol k významným úspechom v spolupráci medzi príslušnými agentúrami EÚ pri činnostiach pobrežnej stráže.

nástrojov EÚ na podporu spolupráce členských štátov pri presadzovaní práva je Schengenský informačný systém, ktorý sa používa na výmenu údajov v reálnom čase o hľadaných a nezvestných osobách a predmetoch. Výsledky jeho používania sú viditeľné v počte zadržaní páchateľov, záchytov drog a záchran potenciálnych obetí.[113] Úroveň spolupráce je však stále možné zlepšiť zjednodušením a inováciou dostupných nástrojov. Väčšia časť právneho rámca EÚ tvoriaceho základ operačnej spolupráce pri presadzovaní práva bola navrhnutá pred 30 rokmi. Zložitá sieť dvojstranných dohôd medzi členskými štátmi, z ktorých mnohé sú zastarané alebo sa takmer nevyužívajú, predstavuje riziko fragmentácie. V menších alebo vo vnútrozemských krajinách musia príslušníci orgánov presadzovania práva, ktorí pracujú cezhranične, vykonávať operačné činnosti v niektorých prípadoch až podľa siedmich rôznych súborov pravidiel: preto sa niektoré operácie, ako napríklad cezhraničné sledovanie podozrivých, jednoducho neuskutočňujú. Súčasťou aktuálneho rámca EÚ nie je ani operačná spolupráca v oblasti nových technológií, ako sú napríklad drony.

Operačnú účinnosť je možné podporiť konkrétnou spoluprácou pri presadzovaní práva, čo môže pomôcť aj pri poskytovaní kľúčovej podpory iným politickým cieľom, ako je napríklad poskytovanie bezpečnostných informácií na účely nového posúdenia priamych zahraničných investícií. Komisia bude skúmať, ako môže tieto činnosti podporiť kódex policajnej spolupráce. Orgány presadzovania práva v členských štátoch čoraz častejšie využívajú podporu a odborné znalosti na úrovni EÚ, pričom kľúčovú úlohu pri podpore výmeny strategických spravodajských informácií medzi spravodajskými a bezpečnostnými službami členských štátov zohráva centrum EU INTCEN poskytujúce inštitúciám EÚ situačnú informovanosť na základe spravodajských informácií[114]. Aj **Europol** môže zohrávať kľúčovú úlohu pri rozširovaní spolupráce s tretími krajinami v oblasti boja proti trestnej činnosti a terorizmu v súlade s ďalšími externými politikami a nástrojmi EÚ. Europol však v súčasnosti čelí množstvu závažných obmedzení, najmä v oblasti priamej výmeny osobných údajov so súkromnými stranami, čo mu bráni účinne podporovať členské štáty v boji proti terorizmu a trestnej činnosti. Mandát Europolu sa v súčasnosti posudzuje s cieľom zistiť, ako ho možno zlepšiť, aby mohla agentúra v plnej miere plniť svoje úlohy. V tejto súvislosti by mali užšie spolupracovať a zlepšiť výmenu informácií aj príslušné orgány na úrovni EÚ (ako napríklad OLAF, Europol, Eurojust a Európska prokuratúra).

Ďalšou kľúčovou súvislosťou je intenzívnejší rozvoj **Eurojustu** v záujme maximalizovania synergie medzi spoluprácou pri presadzovaní práva a justičnou spoluprácou. EÚ by mala prospech aj zo strategickejšej súdržnosti: **EMPACT**[115], cyklus politík EÚ na boj proti organizovanej a závažnej medzinárodnej trestnej činnosti, poskytuje orgánom metodiku na základe spravodajských informácií o kriminalite s cieľom spoločne riešiť najzávažnejšie hrozby trestnej činnosti postihujúce EÚ. Za posledných desať rokov priniesol významné operačné výsledky[116]. Na základe skúseností odborníkov by sa mal existujúci mechanizmus zefektívniť a zjednodušiť tak, aby v novom cykle politík na roky 2022 – 2025 umožňoval lepšie riešenie najakútnejších a vyvíjajúcich sa hrozieb trestnej činnosti.

Pre každodenné úsilie v oblasti stíhania trestnej činnosti sú najdôležitejšie včasné a relevantné **informácie**. Napriek tomu, že na úrovni EÚ boli vytvorené nové databázy pre oblasť riadenia bezpečnosti a hraníc, väčšina informácií sa stále nachádza vo vnútroštátnych

[113] Boj EÚ proti organizovanej trestnej činnosti v roku 2019 (Rada 2020).
[114] EU INTCEN je jediným sprostredkovateľom poskytovania situačnej informovanosti na základe spravodajských informácií Európskej únii spravodajskými a bezpečnostnými službami členských štátov.
[115] EMPACT označuje Európsku multidisciplinárnu platformu proti hrozbám trestnej činnosti.
[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

databázach alebo sa vymieňa mimo týchto nástrojov. Spôsobuje to značnú dodatočnú pracovnú záťaž, oneskorenia a väčšie riziko, že budú chýbať kľúčové informácie. Lepšie, rýchlejšie a zjednodušené procesy, do ktorých sa zapája celé bezpečnostné spoločenstvo, by priniesli lepšie výsledky. Ak má výmena informácií plniť pri účinnom stíhaní trestnej činnosti svoj cieľ, sú potrebné správne nástroje s potrebnými zárukami, aby sa pri výmene údajov dodržiavali právne predpisy o ochrane údajov a základné práva. Vzhľadom na vývoj v oblasti technológií, forenznej vedy a ochrany údajov, ako aj na zmenené operačné potreby, by mohla EÚ zvážiť, či je potrebné modernizovať nástroje, ako sú **prümské rozhodnutia z roku 2008**, zavedenie automatizovanej výmeny údajov o DNA, údajov o odtlačkoch prstov a údajov o evidencii vozidiel na účely umožnenia automatizovanej výmeny dodatočných kategórií údajov, ktoré sú už dostupné v kriminálnych alebo iných databázach členských štátov na účely vyšetrovania trestných činov. Okrem toho bude Komisia skúmať možnosť výmeny záznamov vedených v registri trestov, aby bolo možné zistiť, či o danej osobe existuje záznam vedený v registri trestov v inom členskom štáte, a ak áno, aby bolo možné uľahčiť prístup k týmto záznamom so všetkými potrebnými zárukami.

Informácie o cestujúcich pomáhajú zlepšovať kontroly hraníc, znižovať neregulárnu migráciu a identifikovať osoby predstavujúce bezpečnostné riziká. Vopred poskytované informácie o cestujúcich sú biografické údaje o jednotlivých cestujúcich, ktoré získavajú leteckí dopravcovia počas odbavenia a vopred ich posielajú orgánom hraničnej kontroly v cieľovej krajine. Revízia právneho rámca[117] by mohla umožniť účinnejšie využívanie informácií, pri ktorom by sa zároveň dodržal súlad s právnymi predpismi o ochrane údajov a uľahčoval tok cestujúcich. Záznamy o cestujúcich (PNR) sú údaje, ktoré zadávajú cestujúci pri objednávaní letov. Vykonávanie smernice o záznamoch o cestujúcich[118] je kľúčové, preto ho bude Komisia naďalej podporovať a presadzovať. Okrem toho začne Komisia ako opatrenie v polovici trvania skúmať súčasný prístup k **prenosu záznamov o cestujúcich do tretích krajín**.

Justičná spolupráca je nevyhnutným doplnkom policajného úsilia v oblasti boja proti cezhraničnej trestnej činnosti. Za posledných 20 rokov prešla justičná spolupráca veľmi výraznou zmenou. Orgány ako **Európska prokuratúra** a **Eurojust** potrebujú mať prostriedky na to, aby mohli naplno fungovať alebo posilňovať svoje činnosti. Takisto by sa mohla rozšíriť spolupráca medzi justičnými odborníkmi z praxe, a to vykonaním ďalších krokov v oblasti vzájomného uznávania súdnych rozhodnutí, odbornej justičnej prípravy a výmeny informácií. Cieľom by malo byť zvýšenie vzájomnej dôvery medzi sudcami a prokurátormi, ktorá je nevyhnutným predpokladom bezproblémových cezhraničných konaní. Efektívnosť našich justičných systémov možno zlepšiť aj využívaním **digitálnych technológií**. Na prenos európskych vyšetrovacích príkazov, žiadostí o vzájomnú právnu pomoc a súvisiacej komunikácie medzi členskými štátmi sa zavádza nový digitálny systém výmeny informácií podporovaný Eurojustom. Komisia bude s členskými štátmi spolupracovať na zrýchlení zavádzania potrebných IT systémov na vnútroštátnej úrovni.

Medzinárodná spolupráca je kľúčová aj pre účinné presadzovanie práva a justičnú spoluprácu. Dvojstranné dohody s kľúčovými partnermi zohrávajú kľúčovú úlohu pri zabezpečovaní informácií a dôkazov z krajín mimo EÚ. Významnú úlohu zohráva **Interpol**, jedna z najväčších medzivládnych organizácií kriminálnej polície. Komisia preskúma možné spôsoby posilnenia spolupráce s Interpolom vrátane možného prístupu do databáz Interpolu

[117] Smernica Rady 2004/82/ES o povinnosti dopravcov oznamovať údaje o cestujúcich.

[118] Smernica 2016/681 o využívaní údajov zo záznamov o cestujúcich (PNR) na účely prevencie, odhaľovania, vyšetrovania a stíhania teroristických trestných činov a závažnej trestnej činnosti.

a posilnenia operačnej a strategickej spolupráce. Orgány presadzovania práva v EÚ sa pri odhaľovaní a vyšetrovaní páchateľov a teroristov spoliehajú na kľúčové partnerské krajiny. **Partnerstvá medzi EÚ a tretími krajinami v oblasti bezpečnosti** by sa mohli prehĺbiť v záujme zintenzívnenia spolupráce v boji proti spoločným hrozbám, akými sú terorizmus, organizovaná trestná činnosť, počítačová kriminalita, sexuálne zneužívanie detí a obchodovanie s ľuďmi. Takýto prístup by sa zakladal na spoločných bezpečnostných záujmoch a vychádzal by z nadviazanej spolupráce a bezpečnostných dialógov.

Okrem informácií môže mať veľký význam pri zlepšovaní pripravenosti orgánov presadzovania práva na **netradičné hrozby** aj výmena odborných znalostí. Komisia bude podporovať výmeny najlepších postupov a preskúma možný **mechanizmus koordinácie policajných síl na úrovni EÚ** pre prípady vyššej moci, medzi ktoré patrí napríklad pandémia. Pandémia ukázala aj to, že nevyhnutným predpokladom boja proti trestnej činnosti a terorizmu bude aj policajná kontrola digitálneho spoločenstva spolu s právnymi rámcami na uľahčenie policajnej kontroly online. Offline aj online partnerstvami medzi políciou a spoločenstvom možno zabrániť trestnej činnosti a zmierniť vplyv organizovanej trestnej činnosti, radikalizácie a teroristických činností. Kľúčovým faktorom úspechu pre bezpečnostnú úniu EÚ ako celok je prepojenie od miestnych a regionálnych až po celoštátne a celoúnijné policajné riešenia.

Príspevok silných vonkajších hraníc

Moderné a efektívne riadenie vonkajších hraníc prináša dvojakú výhodu: udržanie celistvosti schengenského priestoru a zaistenie bezpečnosti našich občanov. Zapojenie všetkých príslušných aktérov do úsilia o zaistenie čo najväčšej bezpečnosti na hraniciach môže mať reálny vplyv na predchádzanie cezhraničnej trestnej činnosti a terorizmu. Spoločné operačné činnosti nedávno posilnenej európskej pohraničnej a pobrežnej stráže[119] prispievajú k predchádzaniu a odhaľovaniu cezhraničnej trestnej činnosti na **vonkajších hraniciach** a mimo EÚ. Činnosti v colnej oblasti pri odhaľovaní rizík týkajúcich sa ochrany a bezpečnosti v prípade všetkých tovarov ešte pred ich príchodom do EÚ a v prípade kontroly tovarov po ich príchode tvoria mimoriadne dôležitú súčasť boja proti cezhraničnej trestnej činnosti a terorizmu. V nadchádzajúcom akčnom pláne pre colnú úniu budú oznámené opatrenia, ktorými sa takisto posilní riadenie rizík a zlepší vnútorná bezpečnosť. Budú zahŕňať najmä posúdenie uskutočniteľnosti prepojenia medzi príslušnými informačnými systémami na účely analýzy bezpečnostných rizík.

Rámec **interoperability medzi informačnými systémami EÚ** v oblasti spravodlivosti a vnútorných vecí bol prijatý v máji 2019. Cieľom tejto novej architektúry je zlepšenie efektívnosti a účinnosti nových alebo inovovaných informačných systémov.[120] Zabezpečí sa ňou rýchlejšie a systematickejšie poskytovanie informácií príslušníkom orgánov presadzovania práva, príslušníkom pohraničnej stráže a migračným úradníkom. Pomôže pri správnej identifikácii a bude prispievať k boju proti podvodom s osobnými údajmi. Na realizáciu tohto riešenia je potrebné, aby sa vykonanie interoperability stalo prioritou na politickej aj technickej úrovni. Pri dosahovaní cieľa úplnej interoperability do roku 2023 bude najdôležitejšia úzka spolupráca medzi agentúrami EÚ a všetkými členskými štátmi.

[119] Skladá sa z Európskej agentúry pre pohraničnú a pobrežnú stráž (Frontex) a z orgánov pohraničnej a pobrežnej stráže členských štátov.

[120] Systém vstup/výstup (EES), Európsky systém pre cestovné informácie a povolenia (ETIAS), rozšírený európsky informačný systém registrov trestov (ECRIS-TCN), Schengenský informačný systém, vízový informačný systém a budúci aktualizovaný systém Eurodac.

Podvody týkajúce sa cestovných dokladov sa považujú za najčastejšie páchané trestné činy. Umožňuje sa nimi utajený pohyb páchateľov a teroristov a zohrávajú kľúčovú úlohu pri obchodovaní s ľuďmi a v obchode s drogami.[121] Komisia preskúma spôsoby rozšírenia súčasného úsilia v oblasti bezpečnostných noriem týkajúcich sa pobytu v EÚ a cestovných dokladov, a to aj prostredníctvom digitalizácie. Od augusta 2021 začnú členské štáty vydávať preukazy totožnosti a doklady o pobyte podľa harmonizovaných bezpečnostných noriem, teda aj s čipom obsahujúcim biometrické identifikačné znaky, ktoré budú môcť overiť všetky pohraničné orgány v EÚ. Komisia bude monitorovať vykonávanie týchto nových pravidiel, ako aj postupnú výmenu v súčasnosti používaných dokladov.

Posilnenie výskumu a inovácií v oblasti bezpečnosti

Úsilie o zaistenie kybernetickej bezpečnosti a boj proti organizovanej trestnej činnosti, počítačovej kriminalite a terorizmu sa do veľkej miery opiera o vývoj budúcich nástrojov: na pomoc pri vytváraní bezpečnejších a zabezpečenejších nových technológií, na riešenie výziev, ktoré technológie prinášajú, a na podporu úsilia orgánov presadzovania práva. To však závisí od súkromných partnerov a subjektov odvetvia.

Inovácie by sa mali považovať za strategický nástroj boja proti súčasným hrozbám a predvídania budúcich rizík a príležitostí. Inovačné technológie môžu priniesť nové nástroje na pomoc orgánom presadzovania práva a ďalším aktérom v oblasti bezpečnosti. V prípade umelej inteligencie a analýzy veľkých dát by sa mohla využívať vysokovýkonná výpočtová technika s cieľom ponúknuť lepšie odhaľovanie a rýchlu komplexnú analýzu[122]. Základným predpokladom vývoja spoľahlivých technológií sú vysokokvalitné súbory údajov, ktoré majú príslušné orgány k dispozícii na trénovanie, testovanie a overovanie algoritmov[123]. Všeobecnejšie platí, že v súčasnosti existuje vysoké riziko závislosti od technológií – EÚ je napríklad čistým dovozcom produktov a služieb v oblasti kybernetickej bezpečnosti, pričom toto všetko má vplyv na hospodárstvo a kritické infraštruktúry. Ak chce Európa uchopiť technológie a zaručiť kontinuitu dodávok aj v prípade nepriaznivých udalostí a kríz, musí byť súčasťou kritických častí príslušných hodnotových reťazcov a musí mať na to kapacitu.

Výskum, inovácie a technologický vývoj EÚ ponúkajú príležitosť zohľadniť rozmer bezpečnosti už pri samotnom vývoji týchto technológií a ich uplatňovania. Hlavným stimulom môže byť nová generácia návrhov na financovanie z prostriedkov EÚ[124]. Pri iniciatívach týkajúcich sa európskych dátových priestorov a cloudových infraštruktúr sa s bezpečnosťou počíta od samého začiatku. Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier[125] majú za cieľ zaviesť účinnú a efektívnu štruktúru na združovanie a spoločné využívanie kapacít a výsledkov v oblasti výskumu kybernetickej

[121] Prepojenie medzi podvodmi v oblasti dokladov a obchodovaním s ľuďmi sa uvádza v druhej správe o pokroku dosiahnutom v boji proti obchodovaniu s ľuďmi, COM(2018) 777, v sprievodnom pracovnom dokumente útvarov Komisie SWD(2018) 473 a v situačnej správe Europolu z roku 2016 Obchodovanie s ľuďmi v EÚ.

[122] Toto by malo vychádzať aj zo stratégie Komisie týkajúcej sa umelej inteligencie.

[123] Európska dátová stratégia, COM(2020) 66 final.

[124] V návrhoch programu Horizont Európa, Fondu pre vnútornú bezpečnosť, Fondu pre integrované riadenie hraníc, programu EUInvest, Európskeho fondu regionálneho rozvoja a programu Digitálna Európa, ktoré vypracovala Komisia, sa bude podporovať vývoj a zavádzanie inovačných bezpečnostných technológií a riešení v celom bezpečnostnom hodnotovom reťazci.

[125] Návrh z 12. septembra 2018, ktorým sa zriaďuje Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier, COM(2018) 630.

bezpečnosti. V rámci Vesmírneho programu Únie sa poskytujú služby, ktorými sa podporuje bezpečnosť EÚ, jej členských štátov a jednotlivcov[126].

Výskum v oblasti bezpečnosti financovaný z prostriedkov EÚ predstavuje so svojimi 600 realizovanými projektmi od roku 2007 v celkovej hodnote takmer 3 miliardy EUR kľúčový nástroj stimulovania technológií a znalostí na podporu riešení v oblasti bezpečnosti. V rámci skúmania mandátu Europolu sa bude Komisia zaoberať aj vytvorením **európskeho inovačného centra pre vnútornú bezpečnosť**[127], ktorého úlohou by bolo všetkým prinášať riešenia spoločných výziev a príležitostí v oblasti bezpečnosti, ktoré členské štáty nemusia byť schopné využívať samy. Spolupráca je základným predpokladom čo najúčinnejšieho zamerania investícií a vývoja inovačných technológií s bezpečnostným aj hospodárskym úžitkom.

Rozvíjanie zručností a zvyšovanie informovanosti

Informovanosť o bezpečnostných problémoch a získavanie zručností na riešenie možných hrozieb predstavujú základný predpoklad budovania odolnejšej spoločnosti s lepšie pripravenými podnikmi, verejnými správami a jednotlivcami. Výzvy v oblasti IT infraštruktúry a elektronických systémov odhalili potrebu zlepšovať ľudské kapacity v oblasti pripravenosti a reakcie v rámci kybernetickej bezpečnosti. Pandémia zdôraznila aj dôležitosť digitalizácie vo všetkých oblastiach hospodárstva a spoločnosti EÚ.

Už aj **základné vedomosti o bezpečnostných hrozbách** a spôsobe ich potláčania sa môžu reálne prejaviť na odolnosti spoločnosti. Pri potláčaní kybernetických útokov zohráva svoju úlohu okrem ochrany, ktorú zabezpečujú poskytovatelia služieb, aj uvedomovanie si rizík počítačovej kriminality a potreba chrániť sa pred nimi. Informácie o nebezpečenstvách a rizikách obchodovania s drogami môžu páchateľom sťažovať dosahovanie úspechov. EÚ môže stimulovať šírenie najlepších postupov, napríklad prostredníctvom siete centier pre bezpečnejší internet[128], a zabezpečovať začleňovanie takýchto cieľov do vlastných programov.

Budúci akčný plán digitálneho vzdelávania by mal obsahovať cielené opatrenia na vytváranie IT zručností v oblasti bezpečnosti pre všetkých obyvateľov. V nedávno prijatom programe v oblasti zručností[129] sa podporuje budovanie zručností počas celého života. Tento program obsahuje aj špecializované opatrenia na zvýšenie počtu absolventov vedeckých, technologických, inžinierskych, umeleckých a matematických odborov, ktorí sú potrební v špičkových oblastiach, medzi aké patrí aj kybernetická bezpečnosť. Ďalšie opatrenia, ktoré sa financujú z programu Digitálna Európa, umožnia odborníkom udržať krok s vývojom v oblasti panorámy bezpečnostných hrozieb a zároveň zmierniť nedostatky v tejto oblasti na trhu práce EÚ. Celkovo sa tým jednotlivcom umožní získať zručnosti na riešenie bezpečnostných hrozieb a podnikom nájsť odborníkov, ktorých v tejto oblasti potrebujú.

[126] V rámci programu Copernicus sa napríklad poskytujú služby umožňujúce dozor nad vonkajšími hranicami EÚ a námorný dozor, ktoré pomáhajú podniknúť kroky proti pirátstvu a pašovaniu, ako aj podporiť kritické infraštruktúry. Po plnom sfunkčnení pôjde o kľúčový predpoklad realizácie civilných aj vojenských misií a operácií.

[127] Fungovalo by to aj v prípade agentúr EBCGA/Frontex, CEPOL, eu-LISA a Spoločného výskumného centra.

[128] Pozri www.betterinternetforkids.eu: ústredný portál a národné centrá pre bezpečnejší internet sú v súčasnosti financované v rámci NPE pre telekomunikácie a do budúcnosti sa ich financovanie navrhuje v rámci programu Digitálna Európa.

[129] Európsky program v oblasti zručností pre udržateľnú konkurencieschopnosť, sociálnu spravodlivosť a odolnosť, COM(2020) 274 final.

V budúcom Európskom výskumnom priestore a európskom vzdelávacom priestore sa tiež budú podporovať povolania v oblasti vedy, technológie, inžinierstva, umenia a matematiky.

Dôležitý je aj prístup **obetí** k svojim právam; musia získať nevyhnutnú pomoc a podporu, ktorú vzhľadom na osobitné okolnosti, v ktorých sa ocitli, potrebujú. Osobitné úsilie sa vyžaduje v prípade menšín a najzraniteľnejších obetí, ako sú deti alebo ženy, ktoré sa stali predmetom obchodovania na účely sexuálneho vykorisťovania, alebo ktoré sú vystavené domácemu násiliu.[130]

Osobitný význam majú rozšírené **zručnosti v oblasti presadzovania práva**. Súčasné aj nové technologické hrozby si vyžadujú väčšie investície do zvyšovania úrovne zručností pracovníkov orgánov presadzovania práva v počiatočnej fáze ich kariéry, ako aj počas celého jej priebehu. Najdôležitejším partnerom členských štátov pri plnení tejto úlohy je CEPOL. Neoddeliteľnou súčasťou kultúry bezpečnosti EÚ musí byť odborná príprava v oblasti presadzovania práva zameraná na rasizmus, xenofóbiu a všeobecnejšie na práva občanov. Aj vnútroštátne justičné systémy a odborníci pôsobiaci v oblasti justície musia mať príslušné zručnosti, aby sa dokázali prispôsobiť bezprecedentným výzvam a vedeli na ne reagovať. Odborná príprava je dôležitá, aby orgánom v teréne umožnila využívať tieto nástroje v operačných situáciách. Okrem toho by sa malo všetko úsilie venovať posilňovaniu uplatňovania hľadiska rodovej rovnosti a účasti žien na presadzovaní práva.

Kľúčové opatrenia
• posilnenie mandátu Europolu, • preskúmanie kódexu policajnej spolupráce EÚ a policajnej koordinácie v čase krízy, • posilnenie Eurojustu s cieľom prepojiť justičné orgány a orgány presadzovania práva, • revízia smernice o vopred poskytovaných informáciách o cestujúcich, • oznámenie o vonkajšom rozmere záznamov o cestujúcich, • posilnenie spolupráce medzi EÚ a Interpolom, • rámec na rokovanie o výmene informácií s kľúčovými tretími krajinami, • lepšie bezpečnostné normy týkajúce sa cestovných dokladov, • preskúmanie možnosti vytvorenia európskeho inovačného centra pre vnútornú bezpečnosť.

V. Závery

Európska únia sa vo všeobecnosti považuje za jedno z najbezpečnejších miest aj v dnešnom čoraz nepokojnejšom svete. Nemožno to však považovať za samozrejmosť.

Novou stratégiou bezpečnostnej únie sa kladú základy bezpečnostného ekosystému, ktorý obsiahne celú európsku spoločnosť. Vychádza z poznatku, že bezpečnosť je spoločnou zodpovednosťou. Bezpečnosť je problém, ktorý sa týka každého. Všetky štátne orgány, podniky, sociálne organizácie, inštitúcie a občania si musia plniť svoje povinnosti, aby boli naše spoločnosti bezpečnejšie.

Na bezpečnostné problémy je v súčasnosti potrebné nazerať z oveľa širšej perspektívy ako v minulosti. Je potrebné prekonať nesprávne rozdelenie na fyzické a digitálne. V stratégii EÚ pre bezpečnostnú úniu sa odzrkadľuje celá škála potrieb v oblasti bezpečnosti, pričom stratégia samotná sa zameriava na oblasti, ktoré budú v najbližších rokoch pre bezpečnosť

[130] Pozri stratégiu pre rodovú rovnosť, COM(2020) 152; stratégiu v oblasti práv obetí, COM(2020) 258; a Európsku stratégiu vytvárania lepšieho internetu pre deti, COM(2012) 196.

EÚ najkritickejšie. Takisto sa v nej uznáva, že bezpečnostné hrozby nepoznajú geografické hranice a že prepojenie medzi vnútornou a vonkajšou bezpečnosťou je čoraz intenzívnejšie[131]. V tejto súvislosti bude dôležité, aby EÚ spolupracovala s medzinárodnými partnermi pri zaisťovaní bezpečnosti všetkých občanov EÚ a túto stratégiu vykonávala v úzkej koordinácii s vonkajšou činnosťou EÚ.

Naša bezpečnosť úzko súvisí s našimi základnými hodnotami. Vo všetkých navrhovaných opatreniach a iniciatívach v rámci tejto stratégie sa plne rešpektujú základné práva a naše európske hodnoty. Tie tvoria základ nášho európskeho spôsobu života a musia zostať ústrednou myšlienkou všetkého nášho úsilia.

Napokon je potrebné uviesť, že Komisia si plne uvedomuje skutočnosť, že všetky politiky či opatrenia sú len také dobré ako ich vykonávanie. Preto je potrebné neúnavne zdôrazňovať riadne vykonávanie a presadzovanie súčasných aj budúcich právnych predpisov. To sa bude monitorovať na základe pravidelných správ o bezpečnostnej únii a Komisia bude v plnom rozsahu informovať Európsky parlament, Radu a zainteresované strany, pričom ich bude zapájať do všetkých relevantných činností. Okrem toho je Komisia pripravená zúčastňovať sa na spoločných rozpravách s inštitúciami o stratégii bezpečnostnej únie a organizovať ich, aby bolo možné spoločne vyhodnotiť dosiahnutý pokrok a preskúmať výzvy, ktoré nás ešte čakajú.

Komisia vyzýva Európsky parlament a Radu, aby schválila túto stratégiu bezpečnostnej únie ako základ spolupráce a spoločnej činnosti v oblasti bezpečnosti na nasledujúcich päť rokov.

[131] Pozri globálnu stratégiu EÚ.