Rada
Európskej únie

V Bruseli 27. mája 2022
(OR. en)

9563/22

JAI 761	**DROIPEN 69**
COSI 149	**COPEN 210**
ENFOPOL 298	**FREMP 110**
ENFOCUSTOM 89	**JAIEX 61**
IXIM 145	**CFSP/PESC 705**
CT 99	**COPS 238**
CRIMORG 81	**HYBRID 49**
FRONT 218	**DISINFO 47**
ASIM 47	**TELECOM 248**
VISA 87	**DIGIT 108**
CYBER 191	**COMPET 408**
DATAPROTECT 175	**RECH 307**
CATS 30	

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	25. mája 2022
Komu:	Generálny sekretariát Rady
Č. dok. Kom.:	COM(2022) 252 final
Predmet:	OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE o štvrtej správe o pokroku pri vykonávnaní stratégie EÚ pre bezpečnostnú úniu

Delegáciám v prílohe zasielame dokument COM(2022) 252 final.

Príloha: COM(2022) 252 final

EURÓPSKA
KOMISIA

V Bruseli 25. 5. 2022
COM(2022) 252 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU A RADE

o štvrtej správe o pokroku pri vykonávnaní stratégie EÚ pre bezpečnostnú úniu

I. ÚVOD

Ruská útočná vojna proti Ukrajine je v súčasnosti najvýznamnejším problémom v oblasti bezpečnosti EÚ. Táto vojna nielenže ohrozuje Ukrajinu, ale má za cieľ aj narušiť globálnu stabilitu a bezpečnosť. V rámci EÚ prináša celý rad rizík ohrozujúcich bezpečnosť občanov. Spôsobila nové neistoty v súvislosti s dodávkami energie a iných surovín a kritická infraštruktúra sa môže stať terčom kybernetických útokov. Vnútornú ochranu a bezpečnosť EÚ ohrozujú potenciálne útoky alebo nehody prameniace z chemických, biologických, rádiologických alebo otravných látok vo vojnovej zóne. Zraniteľnosť miliónov ľudí utekajúcich pred vojnou možno ľahko zneužiť na organizovanú trestnú činnosť prostredníctvom obchodovania so ženami a s deťmi, ktorým hrozí mimoriadne riziko.

Vzhľadom na tieto nové a potenciálne hrozby zostáva EÚ rozhodná a jednotná. Hoci vplyv vojny sa zatiaľ v zásade obmedzuje len na územie Ukrajiny, EÚ zintenzívnila *ostražitosť a koordináciu* s dôkladnejším monitorovaním panorámy hrozieb a pracuje na posilnení odolnosti s cieľom zaistiť *pripravenosť*.

Vo vyhlásení z Versailles z 10. a 11. marca 2022[1] európski predstavitelia zdôraznili potrebu pripraviť sa na rýchlo sa objavujúce výzvy, a to aj tým, že „sa budeme chrániť pred stále intenzívnejšou hybridnou vojnou, posilníme našu kybernetickú odolnosť, budeme chrániť našu infraštruktúru – najmä kritickú infraštruktúru – a budeme bojovať proti dezinformáciám“.

Hlavným pilierom na zaistenie bezpečnosti v celej EÚ je rámec bezpečnostnej únie. Štyri strategické priority stanovené v stratégii EÚ pre bezpečnostnú úniu[2] zostávajú naďalej priamo relevantné pre túto úlohu v súčasnom geopolitickom kontexte: i) nadčasové bezpečnostné prostredie; ii) riešenie vyvíjajúcich sa hrozieb; iii) ochrana Európanov pred terorizmom a organizovanou trestnou činnosťou; iv) pevný európsky bezpečnostný ekosystém. Vojna zdôraznila potrebu toho, aby EÚ a jej členské štáty v plnej miere využívali legislatívne a politické nástroje, ktoré už majú k dispozícii v rámci stratégie EÚ pre bezpečnostnú úniu, ktoré sú základom koordinovanej podpory EÚ poskytovanej členským štátom v otázkach siahajúcich od organizovanej trestnej činnosti a terorizmu po kybernetickú bezpečnosť a hybridné hrozby.

Európske agentúry v oblasti spravodlivosti a vnútorných vecí takisto zintenzívnili svoje úsilie v reakcii na vojnu na Ukrajine, pričom zohrávajú kľúčovú úlohu v posudzovaní hrozieb a v podpore operačných reakcií[3]. Ďalším dôležitým faktorom je neustále posilňovanie prevádzkovej praxe a riadenia Schengenského priestoru.

Táto štvrtá správa o pokroku v oblasti bezpečnostnej únie je zameraná na vývoj za posledné mesiace od vypuknutia ruskej útočnej vojny proti Ukrajine. Uvádza sa v nej prehľad opatrení prijatých vo všetkých oblastiach bezpečnostnej únie a skúmajú sa potreby súvisiace s pripravenosťou vyplývajúce z potenciálnych bezpečnostných hrozieb prameniacich z vojny na Ukrajine. Pokrok v rámci iných spisov týkajúcich sa bezpečnostnej únie sa nachádza v prílohe.

---

1 https://www.consilium.europa.eu/media/54784/20220311-versailles-declaration-sk.pdf.

2 COM(2020) 605.

3 Spoločné vyhlásenie agentúr EÚ pre spravodlivosť a vnútorné veci o Ukrajine | Agentúra Európskej únie pre azyl (europa.eu).

II. KYBERNETICKÁ BEZPEČNOSŤ A KRITICKÁ INFRAŠTRUKTÚRA

Od vypuknutia vojny súkromní aktéri a zločinecké skupiny informovali verejnosť o tom, že vykonávajú kybernetické činnosti na podporu jednej alebo druhej strany. Hacktivizmus[4] predstavuje hrozbu, a to vzhľadom na riziko účinkov presahovania na kritické služby v EÚ, riziko útokov pochádzajúcich z oficiálnych sietí alebo iné nepredvídané účinky presahovania. Hoci sa vojna zatiaľ prevažne vedie konvenčnými prostriedkami a účinky presahovania sú len obmedzené, riziko eskalácie v tejto oblasti je reálne.

EÚ preto zintenzívnila svoju koordináciu a pripravenosť. Hrozby prameniace z vojny podčiarkujú potrebu vytvoriť kultúru výmeny informácií a odborných znalostí medzi EÚ, členskými štátmi a komunitami v oblasti kybernetickej bezpečnosti. Zahŕňa to zvyšovanie integrovanej situačnej informovanosti medzi inštitúciami, orgánmi a agentúrami EÚ a členskými štátmi, najmä pokiaľ ide o kritickú infraštruktúru, od ktorej závisí bezproblémové fungovanie vnútorného trhu.

Páchanie kybernetických útokov proti Ukrajine

Kybernetické útoky na samotnú Ukrajinu začali ešte pred ruskou agresiou a počas prvých dní vojny[5] mali za cieľ napádať používateľské kontá ukrajinského armádneho personálu a narušiť základné služby vrátane hraničných kontrol a telekomunikácií.

Vysoký predstaviteľ vydal 14. januára 2022 vyhlásenie[6] v mene Európskej únie, v ktorom odsúdil kybernetické útoky na Ukrajinu a opätovne potvrdil jednoznačnú podporu Ukrajiny zo strany EÚ.

Dňa 10. mája Európska únia a jej členské štáty spolu s medzinárodnými partnermi dôrazne odsúdili[7] škodlivú kybernetickú činnosť z 24. februára namierenú proti Ukrajine, ktorá zasiahla satelitnú sieť KA-SAT vlastnenú spoločnosťou Viasat, a priamo pripísali útok Ruskej federácii. Tento kybernetický útok mal vážne dôsledky a spôsobil nediferencované výpadky a narušenia komunikácie viacerých verejných orgánov, podnikov a používateľov na Ukrajine, pričom zasiahol aj niekoľko členských štátov EÚ.

---

4 Nedávnym príkladom hacktivizmu je používanie „protestvéru“ na šírenie malvéru na ruských IP adresách prostredníctvom populárneho balíka z otvoreného zdroja, ktoré by mohlo viesť k ohrozeniu dodávateľských reťazcov a strate dôvery v komunitu otvorených zdrojov. Komisia jasne vyhlásila, že kybernetické útoky (aj keď majú dobrý úmysel) na Rusko sú nezákonné.

5 Osobitná správa spoločnosti Microsoft: *An overview of Russia's cyberattack activity in Ukraine* (Prehľad činností Ruska v oblasti kybernetických útokov na Ukrajine); *The hybrid war in Ukraine – Microsoft On the Issues* (Hybridná vojna na Ukrajine – vyjadrenie spoločnosti Microsoft k týmto otázkam).

6 https://www.consilium.europa.eu/sk/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/.

7 Ruské kybernetické operácie proti Ukrajine: vyhlásenie vysokého predstaviteľa v mene Európskej únie – Consilium (europa.eu)

Ostražitosť a koordinácia

Od vypuknutia ruskej útočnej vojny proti Ukrajine sa zintenzívnilo monitorovanie situácie v oblasti kybernetickej bezpečnosti v inštitúciách členských štátov a EÚ. Agentúra EÚ pre kybernetickú bezpečnosť ENISA, Európske centrum boja proti počítačovej kriminalite Europolu a tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach CERT-EU, ako aj Spravodajské a situačné centrum EÚ (EU INTCEN) spolu prispievajú k spoločnej situačnej informovanosti EÚ okrem iného zabezpečovaním pravidelného monitorovania podozrivej kybernetickej činnosti, a to aj v špecifických odvetviach, ako sú energetika, doprava a letectvo, a poskytujú posudky na usmerňovanie preventívnych opatrení.

Takisto sa zintenzívnila koordinácia a výmena informácií so sieťami kybernetickej bezpečnosti, ako je sieť styčných organizácií pre kybernetické krízy (CyCLONe), ktorú tvoria vnútroštátne agentúry pôsobiace v oblasti kybernetickej bezpečnosti, Komisia a ENISA. Tento prístup na vnútornej úrovni v inštitúciách EÚ odzrkadľuje koordinačný mechanizmus – jednotka pre kybernetické krízy, ktorá umožňuje výmenu informácií medzi všetkými relevantnými útvarmi a orgánmi a agentúrami vrátane ENISA, Európskeho centra boja proti počítačovej kriminalite Europolu a CERT-EU. Treba vyvíjať nepretržité úsilie o zabezpečenie komunikačných kanálov medzi politickou, operačnou a technickou úrovňou, ako aj o zintenzívnenie spolupráce so sieťou jednotiek pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT).

Europol takisto aktivoval protokol o reakcii na núdzové situácie v rámci presadzovania práva EÚ, ktorý umožňuje posilnené monitorovanie kybernetických hrozieb a výmenu informácií medzi celým radom zainteresovaných strán s cieľom vytvoriť si komplexný obraz o spravodajských informáciách z kybernetickej oblasti.

Okrem kybernetických hrozieb členské štáty, ESVČ a útvary Komisie zintenzívnili ostražitosť, pokiaľ ide o vystavenie kritických infraštruktúr nekybernetickým, fyzickým hrozbám. Kritické infraštruktúry a subjekty, ktoré ich prevádzkujú, môžu byť vystavené fyzickým hrozbám, ako je sabotáž zo strany štátnych alebo štátom sponzorovaných aktérov v rámci možných odvetných opatrení proti EÚ.

Pripravenosť

Keďže Európa je v dôsledku vojny vystavená väčšiemu množstvu výziev, pripravenosť v oblasti kybernetickej bezpečnosti a bezpečnosti kritickej infraštruktúry je kľúčovejšia než kedykoľvek predtým. Úsilie o posilnenie pripravenosti zahŕňa viacero priamych opatrení vrátane opatrení, ktoré sa plánovali už pred ruskou agresiou proti Ukrajine. Patria medzi ne cvičenia, usmernenia, legislatívne opatrenia, zvyšovanie odolnosti v kritických sektoroch a práca s partnermi.

Francúzske predsedníctvo Rady Európskej únie spolu s Európskou službou pre vonkajšiu činnosť (ESVČ) a Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) zorganizovalo začiatkom roka 2022 cvičenie založené na scenári s názvom EU CyCLES (Prepájajúce kybernetické krízové cvičenie solidarity) s cieľom zvýšiť informovanosť na politickej úrovni a posilniť spoluprácu medzi operačnou a politickou úrovňou v prípade kybernetického útoku veľkého rozsahu.

ENISA a CERT-EU vo februári vydali **usmernenia** o tom, ako zvýšiť odolnosť a pripravenosť v EÚ[8]. V týchto usmerneniach sa všetky organizácie verejného a súkromného sektora v EÚ vyzývajú, aby prijali minimálny súbor najlepších postupov v oblasti kybernetickej bezpečnosti v záujme výrazného zlepšenia kultúry kybernetickej bezpečnosti. Tím CERT-EU v marci zverejnil nadväzné technické usmernenia s podporou ENISA[9], ako aj bezpečnostné usmernenia na posilnenie konfigurácie aplikácií Signal[10] s viacerými praktickými odporúčaniami organizáciám na zlepšenie ich stavu kybernetickej bezpečnosti.

Legislatívne iniciatívy

Súčasná situácia zdôrazňuje naliehavosť **vykonávania existujúcich právnych predpisov** a urýchlenia **prijatia pripravovaných iniciatív**.

Komisia pomáha členským štátom pri vykonávaní **smernice NIS**[11], v ktorej sa od členských štátov vyžaduje, aby mali primerané vybavenie, napríklad jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT), a aby určili príslušné orgány. Smernica poskytuje základ pre účinnú spoluprácu medzi členskými štátmi. Politická dohoda, ktorú dosiahli spoluzákonodarci ohľadne **smernice NIS 2**[12], je ďalším prelomom v zabezpečení pevného rámca pripravenosti EÚ.

Smernica NIS 2 – Ďalšie posilnenie pripravenosti

- Nová smernica o sieťach a informačných systémoch sa bude zaoberať nedostatkami predchádzajúcej smernice NIS s cieľom prispôsobiť ju súčasným potrebám a zabezpečiť jej nadčasovosť. Stanovujú sa v nej minimálne pravidlá pre regulačný rámec, ako aj mechanizmy na účinnú spoluprácu medzi príslušnými orgánmi v každom členskom štáte.
- Rozširuje sa ňou rozsah pôsobnosti pravidiel doplnením nových sektorov kritických pre hospodárstvo a spoločnosť (napríklad farmaceutický sektor a sektor zdravotníckych pomôcok alebo potravinárska výroba). Všetky stredné a veľké subjekty pôsobiace v daných sektoroch alebo poskytujúce služby, na ktoré sa vzťahuje smernica, budú patriť do rozsahu jej pôsobnosti. Takisto sa vzťahuje na subjekty verejnej správy na úrovni ústrednej štátnej správy (s výnimkou súdnictva, parlamentov a centrálnych bánk) a na regionálnej úrovni. Členské štáty sa okrem toho môžu rozhodnúť, že sa bude uplatňovať na tieto subjekty aj na miestnej úrovni.
- Smernica NIS 2 bude východiskom pre opatrenia na riadenie kybernetickobezpečnostných rizík a formálne sa ňou zriadi Európska sieť styčných organizácií pre kybernetické krízy EU-CyCLONe, ktorá bude podporovať koordinované riadenie kybernetickobezpečnostných incidentov veľkého rozsahu.
- V tomto návrhu sa takisto zavádzajú presnejšie ustanovenia o postupe nahlasovania incidentov, obsahu správ a harmonogramoch a ustanovujú sa nápravné opatrenia a sankcie na zabezpečenie presadzovania.
- Členské štáty budú mať na začlenenie ustanovení do svojho vnútroštátneho práva 21 mesiacov od nadobudnutia účinnosti smernice.

---

8 *Boosting your Organisation's Cyber Resilience* (Posilnite kybernetickú bezpečnosť svojej organizácie) – spoločná publikácia, 14. 2. 2022.

9 *Security Guidance 2022-01 – Cybersecurity mitigation measures against critical threats* (Bezpečnostné usmernenia 2022-01 – Opatrenia na zmiernenie kritických hrozieb ohrozujúcich kybernetickú bezpečnosť).

10 *CERT-EU Security Guidance 22-002 – Hardening Signal* (Bezpečnostné usmernenia CERT-EU 22-002 – Sprísnenie služby Signal).

11 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

12 COM(2020) 823.

Na pokrok v oblasti smernice NIS 2 by malo čo najskôr nadviazať ukončenie rokovaní o návrhu **smernice o odolnosti kritických subjektov**[13] (ďalej len „smernica CER“), po ktorej prijatí a vykonaní by sa mala zvýšiť odolnosť kritických subjektov voči celému radu hrozieb vrátane teroristických útokov, vnútorných hrozieb alebo sabotáže. Takisto je kľúčové, aby smernica o odolnosti kritických subjektov bola rovnako ambiciózna ako návrh Komisie a aby sa zachoval súlad s politickým kompromisom dosiahnutým v súvislosti so smernicou NIS 2. Kombináciou týchto opatrení sa posilní odolnosť a pripravenosť tým, že sa zavedie súdržnejší a spoľahlivejší systém, a to aj prostredníctvom vnútroštátnych plánov reakcie na incidenty a krízy. Tieto opatrenia boli takisto súčasťou odporúčania Komisie z minulého roka[14] o vytvorení **spoločnej kybernetickej jednotky**, v ktorom sa stanovuje, ako majú jednotliví (diplomatickí, policajní, civilní a v prípade potreby obranní) aktéri ekosystému kybernetickej bezpečnosti spolupracovať na operačnej úrovni. Súčasná panoráma hrozieb zdôrazňuje hodnotu takejto účinnej spolupráce medzi kľúčovými aktérmi.

Komisia naďalej monitoruje vykonávanie súboru nástrojov pre kybernetickú bezpečnosť **5G**[15]. V tejto súvislosti skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti prijala 11. mája správu o bezpečnosti otvorenej rádiovej prístupovej siete (Open RAN)[16]. Takisto pokračuje v spolupráci s členskými štátmi zameranej na plné sprevádzkovanie Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti.

Komisia 22. marca 2022 navrhla **nové pravidlá, ktorými sa majú zriadiť spoločné opatrenia v oblasti kybernetickej a informačnej bezpečnosti vo všetkých inštitúciách, orgánoch a agentúrach EÚ**. Tieto pravidlá zvýšia odolnosť správy EÚ a schopnosť reagovať na kybernetické hrozby a incidenty. Začlenením týchto činností do spoločného rámca sa posilní medziinštitucionálna spolupráca a minimalizuje sa vystavenie rizikám. Návrhom **nariadenia o kybernetickej bezpečnosti pre inštitúcie, orgány a agentúry EÚ**[17] sa posilní mandát CERT-EU a vytvorí sa nová Medziinštitucionálna rada pre kybernetickú bezpečnosť, posilnia sa kapacity v oblasti kybernetickej bezpečnosti a bude sa stimulovať pravidelné posudzovanie vyspelosti a lepšia kybernetická hygiena. Navrhovaným **nariadením o informačnej bezpečnosti**[18] sa vytvorí minimálny súbor pravidiel a noriem informačnej bezpečnosti pre bezpečnú manipuláciu s informáciami všetkých inštitúcií, orgánov a agentúr EÚ a ich bezpečnú výmenu s cieľom lepšie a konzistentne chrániť informácie pred vyvíjajúcimi sa hrozbami. Komisia vyzýva Európsky parlament a Radu, aby tieto opatrenia rýchlo prijali.

Komisia už ukončila svoju verejnú konzultáciu o opatreniach na posilnenie **kybernetickej odolnosti** digitálnych výrobkov a pripravuje návrh, ktorý uverejní túto jeseň[19]. Tento návrh sa bude zaoberať zraniteľnosťami digitálnych produktov a doplnkových služieb, ktoré, hoci vytvárajú príležitosti pre hospodárstva a spoločnosti EÚ, takisto vedú k novým výzvam, keďže čím viac je všetko prepojené, tým ľahšie kybernetickobezpečnostný incident zasiahne celý systém, a tak naruší aj hospodárske a sociálne činnosti.

---

13 COM(2020) 829.

14 Odporúčanie o vybudovaní spoločnej kybernetickej jednotky | Formovanie digitálnej budúcnosti Európy (europa.eu).

15 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

16 Skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, Správa o kybernetickej bezpečnosti siete Open RAN, 11. mája 2022.

17 COM(2022) 122.

18 COM(2022) 119.

19 Akt o kybernetickej odolnosti – nové pravidlá kybernetickej bezpečnosti pre digitálne produkty a doplnkové služby.

Ministri EÚ zodpovední za telekomunikácie 9. marca 2022 jednohlasne prijali výzvu z Nevers na posilnenie schopností EÚ v oblasti kybernetickej bezpečnosti, ktorá zahŕňala „vykonávanie nového fondu reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti, ktorý zavedie Komisia“[20]. Komisia diskutuje o čo najlepšom využití existujúcich finančných prostriedkov na podporu preventívnych a reakčných opatrení.

Kritické sektory

Bezpečnosť dodávok **energie** do EÚ je kľúčová pre blaho občanov a pre bezproblémové fungovanie našich hospodárstiev a súčasná situácia zdôraznila potrebu jasných pravidiel pre kybernetickú bezpečnosť v tomto sektore. Komisia v súčasnosti pripravuje sieťový predpis pre kybernetickú bezpečnosť cezhraničných tokov elektrickej energie podľa požiadaviek nariadenia o elektrine[21] s cieľom stanoviť pravidlá pre posudzovanie rizika, spoločné minimálne požiadavky, plánovanie, monitorovanie, podávanie správ a krízové riadenie. Od vypuknutia ruskej útočnej vojny proti Ukrajine sú ciele sieťového predpisu pre kybernetickú bezpečnosť ešte relevantnejšie. Komisia takisto začala štrukturálnu spoluprácu medzi ENISA, ENTSO-E[22], ENTSOG[23] a Energetickým spoločenstvom v oblasti pravidelného monitorovania kybernetickobezpečnostnej situácie v sektore energetiky.

EÚ sa usiluje chrániť bezpečnosť partnerov bez toho, aby sa sama vystavovala novým rizikám. V marci 2022 došlo k núdzovej synchronizácii elektrizačných sústav Ukrajiny a Moldavska s kontinentálnou európskou sústavou po prijatí opatrení na zmiernenie rizika, najmä pokiaľ ide o kybernetickú bezpečnosť.

Vojna a sankcie takisto viedli k novým výzvam pre **dopravu** EÚ, od bezpečnostných rizík pre civilné letectvo EÚ a šoférov nákladných vozidiel, ktorí uviazli v konfliktných zónach, po ničenie ukrajinskej dopravnej infraštruktúry, odrezanie od dodávateľských reťazcov a ohrozenie svetovej potravinovej bezpečnosti. Agentúra Európskej únie pre bezpečnosť letectva v úzkej spolupráci s Komisiou a Európskou organizáciou pre bezpečnosť leteckej prevádzky Eurocontrol od začiatku vojny odporúča prevádzkovateľom, aby neprevádzkovali lety vo vzdušnom priestore Ukrajiny a vyhli sa využívaniu vzdušného priestoru do 100 námorných míľ od bielorusko-ukrajinskej a rusko-ukrajinskej hranice.

Komisia takisto vyvíja úsilie o posilnenie pripravenosti a odolnosti sektora dopravy EÚ. Konkrétne nový pohotovostný plán pre dopravu[24] prijatý 23. mája vychádza z poznatkov získaných z pandémie COVID-19 aj z vojenskej agresie Ruska proti Ukrajine. Navrhuje sa v ňom súbor desiatich opatrení na usmerňovanie EÚ a jej členských štátov pri zavádzaní núdzových opatrení v reakcii na krízovú situáciu vrátane zaistenia minimálnej prepojenosti, zlepšovania odolnosti voči kybernetickým a hybridným hrozbám a zintenzívnenia spolupráce s medzinárodnými partnermi v oblasti pripravenosti a reakcie na krízu. Takisto sa v ňom zdôrazňuje význam pravidelného testovania odolnosti pre rôzne krízové scenáre, pričom sa spájajú príslušné agentúry EÚ alebo iní aktéri a nadväzuje sa na existujúce postupy.

---

20 8. 3. 2022 – Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique – Presse – Ministère des Finances (economie.gouv.fr).

21 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/943 z 5. júna 2019 o vnútornom trhu s elektrinou (Ú. v. EÚ L158, 14.6.2019, s. 54). Návrh v súčasnosti skúma Agentúra pre spoluprácu regulačných orgánov v oblasti energetiky.

22 Európska sieť prevádzkovateľov prenosových sústav pre elektrinu.

23 Európska sieť prevádzkovateľov prepravných sietí pre plyn.

24 COM(2022) 21.

Podľa rámca **EÚ pre zdravotnú bezpečnosť** treba výmenu informácií vychádzajúcich zo systému včasného varovania a reakcie vrátane podpory lekárskych evakuácií z Ukrajiny chrániť pred kybernetickými útokmi, čím sa posilní bezpečnosť tohto systému.

Spolupráca s partneri

EÚ naďalej spolupracuje so svojimi medzinárodnými partnermi na predchádzaní a zamedzovaní škodlivému správaniu v kybernetickom priestore, odrádzaní od neho a reakcii naň. Pre ruskú útočnú vojnu proti Ukrajine je spolupráca v tejto oblasti dôležitejšia než kedykoľvek predtým. ESVČ v tejto súvislosti pracuje na výmene informácií v oblasti situačnej informovanosti a koordinácii reakcie na škodlivé kybernetické činnosti zamerané proti Ukrajine, ako aj na podpore Ukrajiny a iných krajín regiónu, a to spoluprácou s partnermi vrátane USA a NATO, s cieľom zaistiť doplnkovosť a zabrániť prekrývaniu.

Úzka spolupráca s USA sa takisto zintenzívnila v kontexte Rady EÚ a USA pre obchod a technológie. V spoločnom vyhlásení[25], ktoré nadväzovalo na stretnutie ministrov v Paríži v máji, sa zdôraznila ústredná úloha Rady EÚ a USA pre obchod a technológie v obnovenom transatlantickom partnerstve, ktorého cieľom je koordinovať spoločné opatrenia EÚ a USA súvisiace s ruskou agresiou proti Ukrajine. Obe strany sa zhodli, že úzka spolupráca v oblasti posilnenia odolnosti dodávateľských reťazcov je dôležitejšia než kedykoľvek predtým. Okrem toho sa zriadila osobitná pracovná skupina zameraná na verejné financovanie bezpečnej a odolnej digitálnej infraštruktúry v tretích krajinách, ktorá takisto pripraví pôdu pre financovanie digitálnych projektov v tretích krajinách z verejných zdrojov USA a EÚ na základe súboru spoločných všeobecných zásad.

Strategický kompas prijatý v marci 2022 (pozri oddiel VII) ešte viac posilní súbor nástrojov kybernetickej diplomacie EÚ a bude rozvíjať obrannú politiku EÚ v oblasti kybernetickej bezpečnosti tak, aby bola lepšie pripravená na kybernetické útoky a lepšie na ne reagovala, a to v rámci všeobecnejšej stratégie zameranej na posilnenie schopnosti EÚ konať v krízových situáciách a chrániť svoje záujmy.

Podpora kybernetickej bezpečnosti Ukrajiny a susedných krajín

EÚ podporovala kybernetickú odolnosť Ukrajiny už pred vojnou. Už v júni 2021 sa uskutočnil prvý kybernetický dialóg medzi EÚ a Ukrajinou a EÚ poskytla Ukrajine podporu v oblasti kybernetickej bezpečnosti a odolnej digitálnej transformácie z programu EU4Digital v hodnote 25 miliónov EUR. Twinningový program v objeme 1,5 milióna EUR je takisto určený na to, aby pomáhal ukrajinským inštitúciám pôsobiacim v oblasti kybernetickej bezpečnosti dosiahnuť súlad s normami EÚ.

Od vypuknutia vojny EÚ podporuje spoluprácu medzi kybernetickými expertmi z EÚ a Ukrajiny a koordinuje poskytovanie technickej pomoci, vybavenia, softvéru a príslušných služieb s cieľom posilniť kybernetickú odolnosť a kybernetickú obranu Ukrajiny.

EÚ okrem toho pracuje na posúdení možnej strednodobej podpory Moldavska, Gruzínska a západného Balkánu. Dňa 3. – 4. marca 2022 sa uskutočnila spoločná misia v Moldavsku na posúdenie potrieb v oblasti kybernetickej bezpečnosti, ktorá viedla k prijatiu osobitného opatrenia na reakciu na krízové situácie v záujme rýchleho posilnenia kybernetickej bezpečnosti v krajine. Podobná podpora v oblasti rýchlej reakcie sa pripravuje aj pre viaceré vybrané krajiny západného Balkánu, ktoré sa považujú za vystavené mimoriadnemu riziku v dôsledku ich podpory

[25] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_3108.

sankcií EÚ. Takisto sa posudzuje možnosť dodatočnej pomoci Moldavsku z Európskeho mierového nástroja.

III. ORGANIZOVANÁ TRESTNÁ ČINNOSŤ A TERORIZMUS

Ruská útočná vojna proti Ukrajine donútila milióny ľudí opustiť svoje domovy, čo viedlo k nesmiernemu zvýšeniu pohybu cez vonkajšie hranice EÚ. K 18. máju prišlo do EÚ takmer 6 miliónov ľudí z Ukrajiny a Moldavska a k dnešnému dňu sa 2,8 milióna ľudí v EÚ zaregistrovalo ako žiadatelia o dočasnú ochranu. EÚ sa usiluje zabezpečiť čo najrýchlejšie a najflexibilnejšie prijatie osôb utekajúcich pred vojnou bez toho, aby bola ohrozená bezpečnosť na vonkajšej hranici EÚ. EÚ prijala bezprecedentné opatrenia na to, aby osobám utekajúcim pred vojnou poskytla dočasnú ochranu, a zaviazala sa pristupovať k všetkým novým prišelcom bez diskriminácie. Zároveň však nemožno zabúdať na potenciálne riziká vyplývajúce z takého veľkého množstva premiestňujúcich sa ľudí a EÚ so silnou podporou príslušných agentúr EÚ zostáva ostražitá v súvislosti s novým vývojom v oblasti organizovanej trestnej činnosti a terorizmu.

Silný Schengenský priestor v čase zvýšených hrozieb

Zaistenie vysokej úrovne bezpečnosti v **Schengenskom** priestore a v rámci EÚ nikdy nebolo také dôležité ako v atmosfére zvýšených hrozieb prameniacich z vojny priamo za vonkajšou hranicou EÚ.

V rámci plnenia ambiciózneho programu pre Schengenský priestor uvedeného v stratégii z júna 2021 Komisia v máji prijala prvú správu o stave Schengenského priestoru[26]. Každoročný schengenský cyklus predstavuje nový model riadenia Schengenského priestoru s pravidelnou kontrolou dobrého stavu Schengenu. Prispeje tak k rýchlej identifikácii nedostatkov a zabezpečeniu efektívnych nadväzných postupov s cieľom posilniť a zvýšiť odolnosť Schengenského priestoru.

V prvej správe sa uznáva potreba zintenzívniť úsilie o vykonávanie kľúčových iniciatív na úrovni EÚ vrátane systematických kontrol všetkých cestujúcich na vonkajších hraniciach, pričom sa bude v plnej miere využívať mandát Frontextu a Europolu, ako aj navrhované a dostupné nástroje cezhraničnej policajnej spolupráce.

Konkrétne nová architektúra informačných systémov EÚ pre hranice, migráciu a bezpečnosť a ich interoperabilita sú základným kameňom úsilia o zlepšenie vnútornej bezpečnosti a správy hraníc. Kľúčové bude účinné vykonávanie všetkých prvkov rámca interoperability v súlade s dohodnutým harmonogramom.

Ostražitosť a koordinácia

Intenzívnejšia spolupráca v oblasti presadzovania práva vo všetkých členských štátoch a s tretími krajinami je kľúčová na zaistenie informovanosti o vznikajúcich hrozbách v oblasti trestnej činnosti a terorizmu a opatrení proti sietiam a jednotlivcom vykonávajúcim trestnú činnosť, ktorí sa môžu pokúsiť využiť vojnu proti Ukrajine. Členské štáty a operační partneri si aktívne vymieňajú príslušné dostupné informácie a spravodajské informácie o trestnej

[26] COM(2022) 301.

činnosti s Europolom, ktorý vykonáva krížovú kontrolu týchto informácií, analyzuje ich a premieňa ich na realizovateľné operatívne upozornenia spravodajských služieb, ako sú oznámenia o včasnom varovaní a posúdenia hrozieb, ktoré sa poskytujú aj partnerom.

Organizovaná trestná činnosť

Organizovaná trestná činnosť už našla spôsoby, ako využiť súčasnú situáciu. Počiatočnou analýzou spravodajských informácií sa odhalili určité druhy trestnej činnosti vo viacerých oblastiach vrátane obchodovania s ľuďmi, nesprávneho deklarovania dovážaného a vyvážaného tovaru, online podvodov, počítačovej kriminality a obchodovania so strelnými zbraňami. Existujú aj dôkazy o páchateľoch počítačovej trestnej činnosti, ktorí predstierajú, že zabezpečujú získavanie finančných prostriedkov pre Ukrajinu s cieľom kradnúť peniaze a kryptomenu[27]. Zločinecké organizácie z Ukrajiny sa môžu v dôsledku súčasnej situácie pokúsiť o presídlenie a vykonávanie svojich činností v EÚ.

Komisia a francúzske predsedníctvo Rady spolu s agentúrami SVV EÚ, najmä Europolom, spolupracovali na mobilizácii Európskej multidisciplinárnej platformy proti hrozbám trestnej činnosti (**EMPACT**) s cieľom posúdiť a predvídať existujúce alebo vznikajúce hrozby v oblasti závažnej a organizovanej trestnej činnosti, predchádzať im a bojovať proti nim. Dňa 7. apríla 2022 Europol zorganizoval stretnutie platformy EMPACT, na ktorom sa zišli predstavitelia a odborníci z členských štátov EÚ a bezpečnostnej komunity EÚ s cieľom zamerať sa na hrozby v oblasti závažnej a organizovanej trestnej činnosti, ktoré vznikajú v dôsledku vojny na Ukrajine. Medzi konkrétne kroky, o ktorých sa diskutovalo, patrilo získanie väčšieho množstva spravodajských informácií, vykonávanie núdzových operačných opatrení a zmena zamerania existujúcich opatrení, ako aj dni spoločnej aktivity *ad hoc*.

CELBET (Skupina colných odborníkov pre východnú a juhovýchodnú pozemnú hranicu) – kolaboratívny projekt financovaný z prostriedkov Európskej komisie – sleduje vývoj na hranici v rámci svojej misie, ktorej cieľom je poskytovať operačnú podporu a usmernenia colníkom, a monitoruje prípady colného zhabania na hraničných prechodoch na hranici EÚ (Poľsko, Slovensko, Maďarsko a Rumunsko) s Ukrajinou.

Trestná a teroristická činnosť

Hoci z ruskej invázie na Ukrajinu zatiaľ pre EÚ nevyplýva žiadna bezprostredná teroristická hrozba, je jednoznačne potrebná ostražitosť.

Zvýšené riziko trestnej a teroristickej činnosti podčiarkuje význam toho, aby členské štáty využívali príslušné databázy EÚ, ako je Schengenský informačný systém, a aby do nich v prípade potreby zaznamenávali údaje a vyhľadávali v nich informácie počas kontrol osôb vstupujúcich do EÚ. Pomôže to zabezpečiť, aby jednotlivci, ktorí predstavujú hrozbu pre vnútornú bezpečnosť EÚ, boli identifikovaní na vonkajších hraniciach. Agentúra Európskej únie na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti EU-LISA naďalej zabezpečuje úplnú dostupnosť a efektívnosť

[27] Skupina pre analýzu hrozieb spoločnosti Google zaznamenala rastúci počet aktérov predstavujúcich hrozbu, ktorí využívajú vojnu na Ukrajine ako návnadu na phishingové a malvérové kampane. Výskumníci spoločnosti Cyren pôsobiacej v oblasti internetovej bezpečnosti hlásia nárast podvodov v súvislosti s kryptomenami, pri ktorých sa využíva konflikt používaním falošných darcovských webových sídiel.

systémov EÚ na riadenie hraníc. V usmerneniach[28] adresovaných členským štátom sa objasnilo, ako dosiahnuť rovnováhu medzi potrebou zaistiť bezproblémové vybavovanie prišelcov na vonkajšej hranici a zároveň vykonať potrebné bezpečnostné kontroly.

Pripravenosť

Okrem usmerňovania a koordinácie sa pripravenosť EÚ posilnila nasadením zamestnancov agentúr EÚ.

Europol vyslal operačné tímy do členských štátov EÚ susediacich s Ukrajinou. Tieto tímy sa skladali z prizvaných príslušníkov pohraničnej stráže z členských štátov a expertov Europolu v Maďarsku, Litve, Poľsku, Rumunsku a na Slovensku, ako aj v Moldavsku[29]. Prizvaní príslušníci pohraničnej stráže Europolu podporujú vnútroštátne orgány pri bezpečnostných kontrolách v druhej línii na vonkajších hraniciach EÚ. Experti Europolu poskytujú podporu získavaním a posudzovaním informácií na odhaľovanie teroristických hrozieb a hrozieb trestnej činnosti, na podporu vyšetrovaní a na identifikáciu jednotlivcov, ktorí predstavujú riziko snahou o vstup do EÚ. Tieto operačné tímy získavajú informácie, z ktorých vychádzajú posúdenia hrozieb trestnej činnosti dostupné členským štátom. Takéto získavanie spravodajských informácií umožňuje Europolu predvídať vývoj a koordinovať operačné činnosti s členskými štátmi EÚ v reakcii na činnosti zločineckých skupín, ktoré sa usilujú využiť vojnu na Ukrajine, a s cieľom nadviazať na aktívne zapájanie sa Europolu do presadzovania ukrajinského práva prostredníctvom ukrajinského styčného dôstojníka prítomného v sídle Europolu v Holandsku.

V členských štátoch a susedných krajinách EÚ je takisto prítomná **Európska agentúra pre pohraničnú a pobrežnú stráž (Frontex)**, ktorá podporuje činnosti kontroly hraníc: v celej EÚ, na západnom Balkáne a v Moldavsku je v súčasnosti nasadených viac než 2 100 príslušníkov pohraničnej stráže. **Agentúra Európskej únie pre azyl (EUAA)** vyslala takmer 750 pracovníkov do južných členských štátov EÚ a do Litvy na podporu operačných činností, posilnenie prijímacích kapacít a pomoc pri azylových postupoch.

V nadväznosti na nedávne **prümské rozhodnutie**[30] tvoriace rámec, na základe ktorého členské štáty vysielajú pracovníkov orgánov presadzovania práva na spoločné operácie, ako sú spoločné hliadky, Komisia a francúzske predsedníctvo Rady Európskej únie odoslali všetkým členským štátom list s cieľom identifikovať potreby, v ktorom žiadali o vyslanie príslušníkov polície v záujme spustenia spoločných hliadok v členských štátoch EÚ v prvej línii, ktoré sú najviac zasiahnuté hromadnými prechodmi cez hranice v dôsledku vojny. Komisia bude financovať tieto vyslania z Fondu pre vnútornú bezpečnosť – polícia.

Riešenie problematiky obchodovania s ľuďmi

EÚ bola od prvých dní vojny v stave pohotovosti v súvislosti s rizikami v jednej konkrétnej oblasti trestnej činnosti, v rámci ktorej sa môže využiť intenzívny pohyb ľudí hľadajúcich

[28] Oznámenie Komisie, ktorým sa poskytujú operačné usmernenia týkajúce sa riadenia vonkajších hraníc s cieľom uľahčiť prekračovanie hraníc medzi EÚ a Ukrajinou (2022/C 104 I/01).

[29] K 3. máju Europol vyslal jedného pracovníka Europolu a troch prizvaných príslušníkov pohraničnej stráže na Slovensko, jedného pracovníka Europolu do Poľska, jedného pracovníka Europolu a štyroch prizvaných príslušníkov pohraničnej stráže do Rumunska a dvoch prizvaných príslušníkov pohraničnej stráže do Maďarska. Jeden pracovník Europolu a dvaja prizvaní príslušníci pohraničnej stráže boli vyslaní do Moldavska.

[30] 2008/615/SVV a 2008/616/SVV.

bezpečie v EÚ. Je kľúčové predchádzať tomu, aby obchodníci s ľuďmi zameraní na zraniteľných ľudí, ktorí sa premiestňujú a ktorými sú hlavne **ženy a deti**, využívali napríklad falošné ponuky prepravy alebo ubytovania.

Europol a Eurojust v marci vydali príslušným vnútroštátnym orgánom oznámenia o včasnom varovaní o potenciálnom obchodovaní s ľuďmi a zneužívaní obetí prichádzajúcich z Ukrajiny. Eurojust prispieva k zintenzívňovaniu výmeny informácií a urýchľovaniu súdnej spolupráce aj s Ukrajinou, pričom vyšetrovania obchodovania s ľuďmi postupuje agentúre pre koordináciu.

Koordinátor EÚ pre boj proti obchodovaniu s ľuďmi sa zúčastnil na stretnutiach so sieťou národných spravodajcov alebo rovnocenných mechanizmov EÚ, agentúrami pre spravodlivosť a vnútorné veci a s platformou občianskej spoločnosti EÚ proti obchodovaniu s ľuďmi zameranými na výmenu informácií o opatreniach potrebných na predchádzanie zneužívania obetí, na boj proti ich zneužívaniu a na ich ochranu. Vo viacerých členských štátoch sa začali vyšetrovania potenciálnych prípadov.

EÚ rýchlo a energicky zabezpečuje koordinovanú reakciu na túto reálnu hrozbu pre ľudí, ktorí potrebujú pomoc EÚ. Členské štáty vykonávajúce smernicu o dočasnej ochrane rýchlo dostali operačné usmernenia[31] týkajúce sa okrem iného výzvy obchodovania s ľuďmi, ktoré im majú pomôcť podporovať ľudí utekajúcich pred vojnou na Ukrajine. V rámci desaťbodového plánu pre silnejšiu európsku koordináciu vítania ľudí utekajúcich z Ukrajiny pred vojnou[32] predloženého v Rade pre spravodlivosť a vnútorné veci 28. marca 2022 koordinátor EÚ pre boj proti obchodovaniu s ľuďmi v spolupráci s agentúrami EÚ a členskými štátmi vypracoval spoločný plán boja proti obchodovaniu s ľuďmi[33] na predchádzanie obchodovaniu s ľuďmi a na pomoc obetiam. Osobitný dôraz sa kladie na registráciu subjektov a jednotlivcov (vrátane dobrovoľníkov), ktorí majú záujem poskytovať ubytovanie, prepravu a pomoc iného druhu, ako aj vykonávanie previerok osôb. Komisia takisto spolupracuje s EUAA na podpore identifikácie obetí obchodovania s ľuďmi pri zabezpečovaní zdravotných kontrol v prijímacích centrách. Maloletým bez sprievodu alebo odlúčeným deťom hrozí mimoriadne riziko zneužívania, sexuálneho vykorisťovania alebo nútenej trestnej činnosti. Spomínané operačné usmernenia obsahujú aj usmernenia, ktoré majú členským štátom pomôcť vybavovať príchod, prijímanie a podporu detí, najmä maloletých bez sprievodu. Na účely zvyšovania informovanosti medzi ohrozenými osobami Komisia takisto spustila špeciálne webové sídlo s časťou venovanou praktickým radám o tom, ako sa vyhnúť obchodníkom s ľuďmi.

Hoci niektoré kroky na zvýšenie pripravenosti sa prijali konkrétne v reakcii na nové podmienky vyplývajúce z vojny, ďalšie kľúčové opatrenia vyplývajú z **legislatívnych iniciatív**, ktoré sa už pripravovali pred ruskou útočnou vojnou proti Ukrajine.

Komisia víta dohodu o revidovanom mandáte **Europolu** z februára 2022[34], po ktorého vykonaní bude Europol môcť lepšie podporovať členské štáty v boji proti organizovanej trestnej činnosti a terorizmu. Agentúra tak bude mať správne nástroje a záruky na podporu policajných zložiek pri

31 C/2022/1806, EUR-Lex – 52022XC0321(03) – SK – EUR-Lex (europa.eu).

32 https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en.

33 https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en.

34 COM(2020) 796.

analýze veľkých dát na účely vyšetrovania trestných činov a pri rozvíjaní priekopníckych metód na boj proti kybernetickej trestnej činnosti. Tieto zmeny vyplývajú z posilneného rámca ochrany údajov, ako aj z dôkladnejšieho parlamentného dohľadu a zodpovednosti.

Balík týkajúci sa **policajnej spolupráce**, ktorý Komisia predložila 8. decembra 2021[35] a o ktorom sa v súčasnosti rokuje, posilní spoluprácu medzi úradníkmi z orgánov presadzovania práva v jednotlivých členských štátoch tým, že urýchli, uľahčí a zvýši bezpečnosť výmeny údajov, ako aj posilnením a zefektívnením operačnej policajnej spolupráce v teréne. Komisia vyzýva Európsky parlament a Radu, aby tento balík rýchlo prijali.

Po prijatí a vykonaní budú tieto legislatívne návrhy podporovať presadzovanie práva v boji proti cezhraničnej organizovanej trestnej činnosti. To bude mimoriadne dôležité v súvislosti s tým, že zločinecké organizácie z Ukrajiny sa môžu v dôsledku súčasnej situácie pokúsiť o presídlenie a vykonávanie svojich činností v EÚ.

Poradná misia EÚ na Ukrajine podporuje reformu presadzovania práva a inštitúcií právneho štátu v krajine od roku 2014. V marci 2022 bol mandát misie revidovaný tak, aby umožňoval podporu na ukrajinských hraničných prechodoch na hraniciach s Poľskom, Rumunskom a so Slovenskom, čím prispieva k situačnej informovanosti o cezhraničnej trestnej činnosti vrátane obchodovania s ľuďmi a o toku humanitárneho tovaru na Ukrajinu.

IV. ZBRANE, NEBEZPEČNÝ MATERIÁL A KRITICKÉ INCIDENTY

V dôsledku vojny sa výrazne zvýšil počet strelných a iných zbraní v obehu priamo na Ukrajine, čo predstavuje nové riziká pre EÚ a iné štáty susediace s Ukrajinou.

Ostražitosť a koordinácia

Operačné usmernenia vydané v marci obsahovali rady členským štátom o tom, ako bojovať proti výzve zvýšeného počtu strelných zbraní v obehu v čase hromadných príchodov na vonkajšiu hranicu EÚ[36]. V týchto usmerneniach sa zdôrazňuje, že prítomnosť strelných zbraní by sa mala priebežne kontrolovať a nikomu by bez oprávnenia nemal byť umožnený vstup do EÚ so strelnou zbraňou. Ak ktorékoľvek z týchto strelných zbraní ukrajinské úrady nahlásia ako nezvestné, členské štáty by ich mali nahlásiť v Schengenskom informačnom systéme.

Je kľúčové, aby sa všetky zásielky strelných zbraní na Ukrajinu riadne zaznamenávali, a to so všetkými relevantnými informáciami (vrátane druhu, krajiny a roku výroby, značky, výrobcu, kalibru, sériového čísla) s cieľom uľahčiť vysledovateľnosť týchto strelných zbraní na Ukrajine aj v EÚ.

EÚ verejne odsúdila bezohľadné ruské vojenské útoky na civilné jadrové, biologické a chemické zariadenia na Ukrajine a v ich bezprostrednej blízkosti, ako aj všetky útoky ohrozujúce bezpečnosť týchto zariadení. Komisia situáciu na Ukrajine monitoruje, pričom osobitnú pozornosť venuje rádiologickej hrozbe, ktorá z hľadiska vnútornej bezpečnosti EÚ

[35] COM(2021) 780, COM(2021) 782, COM(2021) 784.

[36] Oznámenie Komisie, ktorým sa poskytujú operačné usmernenia týkajúce sa riadenia vonkajších hraníc s cieľom uľahčiť prekračovanie hraníc medzi EÚ a Ukrajinou (2022/C 104 I/01).

vyvoláva najväčšie obavy[37]. Komisia takisto monitoruje potenciálne chemické hrozby a zriadila interný koordinačný mechanizmus pre prípad potreby rýchleho posúdenia rizika.

Pripravenosť

Ukrajina už je jednou z krajín identifikovaných ako kľúčová pre konkrétne opatrenia na vonkajšej úrovni v Akčnom pláne EÚ na boj proti nedovolenému obchodovaniu so strelnými zbraňami na roky 2020 – 2025. V regióne zahŕňajúcom Ukrajinu sa už vykonávajú špecifické operačné opatrenia v rámci sekcie platformy EMPACT pre strelné zbrane. Vzhľadom na riziká zneužívania strelných zbraní však budú potrebné osobitné projekty financované z prostriedkov EÚ, ako aj operačná spolupráca s agentúrami Europol, Frontex a sekciou platformy EMPACT pre strelné zbrane. Komisia v blízkej budúcnosti predloží návrh na revíziu nariadenia o strelných zbraniach[38] týkajúceho sa vývozu, dovozu a tranzitu civilných strelných zbraní, ktorý sa začlení do celkového právneho a operačného rámca na predchádzanie obchodovaniu so strelnými zbraňami, na jeho odhaľovanie, vyšetrovanie a trestné stíhanie.

Na účely zlepšenia pripravenosti a reakcie EÚ na riziká pre verejné zdravie, ako sú hrozby CBRN, Komisia vytvára strategické rezervy reakčných kapacít v rámci mechanizmu Únie v oblasti civilnej ochrany financované z prostriedkov Úradu pre pripravenosť a reakcie na núdzové zdravotné situácie (HERA)[39]. Útvary Komisie spolupracujú na vytvorení strategických zásob v systéme rescEU v objeme 540,5 milióna EUR. Tieto zásoby sa budú skladať z vybavenia a liekov, očkovacích látok a iných terapeutík na liečbu pacientov vystavených chemickým, biologickým, rádiologickým a jadrovým látkam, ako aj z dekontaminačnej rezervy rescEU na zabezpečenie dekontaminačného vybavenia a odborných zásahových tímov. Ako prvý okamžitý krok EÚ zmobilizovala svoju rezervu zdravotníckeho vybavenia v systéme rescEU na zaobstaranie tabliet jodidu draselného, ktoré môžu ľudia použiť na ochranu pred škodlivými účinkami radiácie, ako aj iných položiek súrne potrebných na Ukrajine. Na Ukrajinu boli s pomocou Francúzska a Španielska prostredníctvom mechanizmu Únie v oblasti civilnej ochrany dodané takmer 3 milióny jódových tabliet.

V. KOORDINOVANÉ OPATRENIA NA ZAISTENIE ZODPOVEDANIA SA RUSKA ZA AGRESIU

EU zohráva rozhodujúcu úlohu v opatreniach medzinárodného spoločenstva, ktorými sa vyvíja na Rusko tlak, aby ukončilo svoju agresiu proti Ukrajinskému štátu a civilistom, ktorí sa ocitli uprostred konfliktu, ktorá je neprijateľná a v rozpore s medzinárodným právom. Tento tlak zahŕňa opatrenia na stanovenie dôsledkov pre páchateľov vrátane prísnych sankcií a opatrení na identifikáciu a uľahčenie trestného stíhania vojnových zločinov.

Reštriktívne opatrenia a konfiškácia

---

37 V spolupráci s partnermi z USA Komisia zorganizuje seminár zameraný na riziká súvisiace s rádiologickým materiálom nachádzajúcim sa v nemocniciach, ktorý nepodlieha regulačnej kontrole.

38 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 258/2012 zo 14. marca 2012, ktorým sa vykonáva článok 10 Protokolu Organizácie Spojených národov proti nezákonnej výrobe a obchodovaniu so strelnými zbraňami, ich súčasťami a komponentmi a strelivom doplňujúceho Dohovor Organizácie spojených národov proti nadnárodnému organizovanému zločinu (protokol OSN o strelných zbraniach) a ktorým sa ustanovujú vývozné povolenia a opatrenia týkajúce sa dovozu a tranzitu strelných zbraní, ich súčastí a častí a streliva.

39 Pracovný plán úradu Hera na rok 2022 (europa.eu).

Odvtedy, ako 21. februára 2022 Rusko uznalo vládou nekontrolované územie Doneckej a Luhanskej oblasti na Ukrajine, a od inváziena Ukrajinu 24. februára 2022 uložila EÚ Rusku dosiaľ najväčší súbor reštriktívnych opatrení. Doteraz bolo prijatých päť balíkov sankcií. Tieto opatrenia sa zameriavajú na kľúčové sektory vrátane financií, obchodu, dopravy, obrany a médií a sú namierené proti politickej a armádnej elite, ako aj popredným ruským a bieloruským oligarchom. Zoznamy už obsahujú viac ako 1 000 jednotlivcov a 80 subjektov. Rada práve rokuje o šiestom balíku sankcií.

Vplyv týchto a predchádzajúcich reštriktívnych opatrení proti jednotlivcom a spoločnostiam z Ruska a Bieloruska bude závisieť od toho, ako dôrazne sa budú presadzovať. Koordinácia EÚ môže významným dielom prispieť k preklenutiu potenciálnych medzier a Komisia poskytla zainteresovaným stranám rozsiahlu podporu prostredníctvom písomných usmernení, stretnutí so zainteresovanými stranami a osobitnej expertnej skupiny, ako aj celý súbor zdrojov na uľahčenie dodržiavania predpisov.

Komisia okrem toho zriadila osobitnú skupinu s názvom Freeze and Seize (Zmraziť a zaistiť), na ktorej sa spoločne podieľajú útvary Komisie, členské štáty, Eurojust a Europol. Členské štáty doteraz nahlásili zmrazenie aktív v hodnote 9,89 miliardy EUR[40]. Dňa 11. apríla Europol spolu s členskými štátmi a agentúrami Eurojust a Frontex spustil operáciu Oscar na podporu finančných vyšetrovaní a vyšetrovaní trestných činov zameranú na majetok pochádzajúci z trestnej činnosti vo vlastníctve jednotlivcov a právnych subjektov, na ktoré sa vzťahujú sankcie EÚ súvisiace s ruskou vojnou proti Ukrajine. Osobitná skupina EÚ Freeze and Seize úzko spolupracuje s osobitnou skupinou s názvom Russian Elites, Proxies, and Oligarchs (Ruské elity, zástupcovia a oligarchovia), ktorú zriadili krajiny G7 (Francúzsko, Japonsko, Kanada, Nemecko, Spojené kráľovstvo, Spojené štáty a Taliansko), a s podobne zmýšľajúcimi krajinami, ako je Austrália, ako aj s osobitnou skupinou KleptoCapture z USA a ukrajinskou osobitnou skupinou.

Osobitná skupina Freeze and Seize slúži ako platforma na koordináciu a uľahčenie výmeny informácií a skúseností medzi jednotlivými členskými štátmi a na poskytovanie usmernení o vykonávaní sankcií, ako aj uľahčenie výmeny najlepších postupov v oblasti vyšetrovania trestných činov a konfiškácie. Dôležité je najmä to, že orgány presadzovania práva sú v stave ostražitosti a proaktívne, pokiaľ ide o potenciálne trestné činy páchané sankcionovanými jednotlivcami a subjektmi. Cieľom osobitnej skupiny je takisto podnecovať diskusie o možnom použití zabavených finančných prostriedkov, napríklad na pomoc pri rekonštrukcii Ukrajiny.

Komisia v súčasnosti prijíma balík na **vymáhanie majetku a konfiškáciu**[41], v ktorom sa zohľadňujú poznatky získané z vykonávania reštriktívnych opatrení Únie proti jednotlivcom a subjektom z Ruska a Bieloruska. Balík uľahčí účinné vykonávanie reštriktívnych opatrení EÚ v celej Únii tým, že umožní rýchle vysledovanie a identifikáciu majetku vlastneného alebo ovládaného osobami alebo subjektmi, na ktoré sa tieto opatrenia vzťahujú. Posilnený rámec na vymáhanie majetku a konfiškáciu sa takisto bude vzťahovať na porušovanie reštriktívnych opatrení, a tak zaistí účinné sledovanie, zmrazovanie, správu a konfiškáciu príjmov prameniacich z porušovania reštriktívnych opatrení. Aby sa zabezpečilo, že majetok jednotlivcov a subjektov, ktorí(-é) porušujú reštriktívne opatrenia, možno skutočne skonfiškovať, Komisia v súčasnosti prijíma takisto návrhy rozhodnutia Rady o doplnení

[40] Takisto boli zablokované aktíva Ruskej centrálnej banky v hodnote približne 23 miliárd EUR.

[41] COM(2022) 245.

zoznamu trestných činov EÚ v článku 83 ods. 1 ZFEÚ[42] o porušenie sankcií, ku ktorému je priložené oznámenie[43], s cieľom navrhnúť smernicu na aproximáciu vymedzenia trestných činov a sankcií za porušovanie reštriktívnych opatrení.

Zo všeobecnejšieho hľadiska je tento balík kľúčovým krokom v boji proti organizovanej trestnej činnosti. Nadväzuje na záväzky Komisie prijaté v rámci stratégie EÚ pre bezpečnostnú úniu a stratégie EÚ na boj proti organizovanej trestnej činnosti na roky 2020 – 2025[44]. Reviduje sa ním smernica o konfiškácii z roku 2014, rozhodnutie Rady o úradoch pre vyhľadávanie majetku z roku 2007 a rámcové rozhodnutie o konfiškácii príjmov, nástrojov a majetku z trestnej činnosti z roku 2005 s cieľom posilniť schopnosti v oblasti vypátrania a identifikácie a v konečnom dôsledku konfiškácie nezákonných ziskov a zároveň riešiť veľmi nízku úroveň konfiškácie v EÚ[45]. Balíkom sa rozširuje rozsah predmetných trestných činov a rozsah pôsobnosti pravidiel pre konfiškáciu v prípadoch, v ktorých nie je možné odsúdenie za konkrétny trestný čin, no v ktorých majetok jednoznačne pochádza z trestnej činnosti. Revíziou sa takisto posilňuje účinná správa zmrazeného a skonfiškovaného majetku a posilňuje sa kapacita úradov pre vyhľadávanie majetku, pokiaľ ide o sledovanie a identifikáciu nezákonného majetku. Nový rámec EÚ na vymáhanie majetku je navrhnutý tak, aby riešil komplexný spôsob činnosti zločineckých organizácií, ktoré často pôsobia cezhranične a na utajenie svojho majetku používajú rôzne metódy vrátane kryptoaktív.

Koordinovaná reakcia súdnictva

Na úrovni EÚ sa vyvíja úsilie o zabezpečenie koordinovanej reakcie súdnictva na **medzinárodné trestné činy** údajne spáchané na Ukrajine, aby za ne páchatelia niesli zodpovednosť.

Dva členské štáty a Ukrajina zriadili spoločný vyšetrovací tím na vyšetrovanie vojnových zločinov, zločinov proti ľudskosti a iných medzinárodných trestných činov údajne spáchaných na ukrajinskom území. Tomuto spoločnému vyšetrovaciemu tímu poskytuje právnu, analytickú, finančnú a logistickú podporu Eurojust. Dňa 25. apríla 2022 sa k spoločnému vyšetrovaciemu tím pripojil ako účastník Úrad prokurátora Medzinárodného trestného súdu[46] a očakáva sa, že v budúcnosti sa pripoja ďalší účastníci.

Komisia 25. apríla 2022 predložila návrh na zmenu nariadenia o Eurojuste[47], na základe ktorej by Eurojust uchovával, analyzoval a ukladal dôkazy o najzávažnejších medzinárodných trestných činoch. Eurojust a Europol budú naďalej úzko spolupracovať počas celého tohto procesu. Kľúčovú úlohu v koordinácii reakcie súdnictva takisto zohráva sieť pre vyšetrovanie genocídy, ktorej sekretariát sídli v Eurojuste, ktorá vypracovala atlas mimovládnych organizácií aktuálne pôsobiacich na Ukrajine a ktorá podporuje vnútroštátnych odborníkov z členských štátov a Ukrajiny pri riešení aktívnych prípadov súvisiacich s vojnou.

Rada v apríli 2022 ďalej revidovala mandát **poradnej misie EÚ na Ukrajine**, čím pripravila podmienky na podporu ukrajinských orgánov zo strany misie pri vyšetrovaní a trestnom stíhaní všetkých medzinárodných trestných činov spáchaných v rámci ruskej vojenskej

42 COM(2022) 247.
43 COM(2022) 249.
44 COM(2021) 170.
45 Podľa odhadov Europolu sú zmrazené len 2 % (2,4 miliardy EUR) majetku pochádzajúceho z trestnej činnosti a skonfiškované je len 1 % (1,2 miliardy EUR) takéhoto majetku, zatiaľ čo príjmy z trestnej činnosti na hlavných zločineckých trhoch v EÚ predstavovali v roku 2019 139 miliárd EUR (1 % HDP EÚ).
46 https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine.
47 COM(2022) 187 final.

agresie. Misia bude ukrajinským orgánom poskytovať strategické poradenstvo o vyšetrovaní a trestnom stíhaní medzinárodných trestných činov, potrebných zmenách ukrajinských právnych predpisov, komunikačnej stratégii, ako aj odbornej príprave o súvisiacich záležitostiach. Misia je súčasťou súboru koordinačných iniciatív v tomto kontexte a spolu s delegáciou EÚ je súčasťou poradnej skupiny USA a EÚ pre masové zverstvá na Ukrajine.

VI. ZAHRANIČNÁ MANIPULÁCIA S INFORMÁCIAMI A ZAHRANIČNÉ ZASAHOVANIE

Súčasný geopolitický vývoj podčiarkol riziko zahraničného zasahovania. Ruskú vojenskú agresiu proti Ukrajine sprevádzajú činnosti spočívajúce v **manipulácii s informáciami a zasahovaní**. Na odôvodnenie brutálnych útokov na Ukrajinu sa používajú neopodstatnené obvinenia ukrajinskej vlády z „nacizmu“ a „genocídy“, operácie pod falošnou vlajkou a nepodložené obvinenia proti NATO a západu, zatiaľ čo v Rusku sa potláča sloboda prejavu a nezávislé spravodajstvo. Pretrváva riziko prameniace zo zmanipulovaného audiovizuálneho materiálu a z dezinformácií, ktoré sa Rusko môže pokúsiť použiť ako zámienku na ďalšie vojenské útoky alebo ktorými sa môže pokúsiť oslabiť odhodlanie ukrajinského odporu, rozdeliť medzinárodné spoločenstvo, ktoré je proti vojne, alebo zasiať pochybnosti o porušovaní medzinárodného práva zo strany Ruska. EÚ sa v Strategickom kompase zaviazala dôrazne reagovať na zahraničnú manipuláciu s informáciami a zahraničné zasahovanie a posilniť svoju odolnosť a schopnosť bojovať proti týmto hrozbám.[48] Manipulácia demokratickej diskusie v rámci EÚ je predmetom akčného plánu pre európsku demokraciu, koordinovaného plánu Komisie na riešenie dezinformácií a posilnenie demokratickej odolnosti[49].

Ostražitosť a koordinácia

Európska únia reagovala na dezinformačnú kampaň Ruska v kontexte ruskej vojenskej agresie proti Ukrajine ráznymi a koordinovanými opatreniami. EÚ úzko spolupracuje so svojimi členskými štátmi prostredníctvom systému včasného varovania a s medzinárodnými partnermi, ako sú NATO, USA, Kanada a mechanizmus rýchlej reakcie skupiny G7, pokiaľ ide o výmenu informácií o vývoji a taktikách v oblasti manipulácie, ktoré používa Kremeľ. Zintenzívnilo sa úsilie o narušenie manipulácie zo strany Kremľa, a to najmä prostredníctvom webového sídla EUvsDisinfo, ktoré v angličtine, ruštine, ukrajinčine a iných jazykoch vysiela faktické informácie v rámci EÚ, na Ukrajine a v regióne, ako aj v rámci Ruska. V dôsledku reštriktívnych opatrení, ktoré prijala EÚ, bol 2. marca zastavený prenos a vysielanie kanálov ruského štátneho média RT a kanálu Sputnik v EÚ alebo určených EÚ. Online platformy, popredné sociálne siete, zadávatelia reklamy a signatári Kódexu postupov proti šíreniu dezinformácií[50] z odvetvia reklamy prijímajú naliehavé opatrenia na obmedzenie dezinformácií súvisiacich s ruskou agresiou proti Ukrajine. Komisia a ESVČ toto úsilie monitorujú. Z poskytnutých informácií vyplýva, že platformy v súvislosti s vojnou posilnili svoje nástroje na monitorovanie a zásah.

Okrem toho sa rýchlo zavádzajú opatrenia na podporu krajín v Strednej Ázii a na západnom Balkáne pri posilňovaní informačnej odolnosti a boji proti zahraničnej manipulácii s informáciami a proti dezinformáciám.

---

48 https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/sk/pdf.

49 COM(2020) 790.

50 https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

Pripravenosť

Vzhľadom na otvorené využívanie zahraničnej manipulácie s informáciami a zahraničného zasahovania vrátane dezinformácií ako jedného z nástrojov hybridných hrozieb je nadviazanie na akčný plán pre európsku demokraciu ešte naliehavejšie. V uplynulých mesiacoch inštitúcie EÚ podporovali členské štáty pri boji proti zahraničnej manipulácii s informáciami a zahraničnému zasahovaniu, a to najmä v rámci systému včasného varovania, výmenou informácií o taktikách používaných aktérmi vykonávajúcimi zahraničnú manipuláciu s informáciami a zahraničné zasahovanie a o stratégiách reakcie. Prebiehajú diskusie o ďalšom posilnení celkovej reakcie EÚ na zahraničnú manipuláciu s informáciami a zahraničné zasahovanie na základe koncepčného dokumentu o vypracovaní špeciálneho **súboru nástrojov** na riešenie tejto výzvy, ktorý predložila ESVČ. Zastrešuje existujúce vnútorné opatrenia a nové nástroje spoločnej zahraničnej a bezpečnostnej politiky EÚ. Takisto bude využívať výhody zintenzívnených opatrení pracovnej skupiny Európskej služby pre vonkajšiu činnosť Stratcom[51] aj Komisie.

Európske stredisko pre monitorovanie digitálnych médií (EDMO) po vypuknutí vojny na Ukrajine zriadilo osobitnú skupinu pre dezinformácie a koordinuje opatrenia prostredníctvom overovateľov faktov a výskumníkov zo svojej siete. Analyzovalo, ako šíritelia konšpiračných teórií o ochorení COVID-19 rýchlo začali šíriť proruské hoaxy, pričom tento posun pozorovalo vo viacerých členských štátoch[52].

Cieľom návrhu aktu o digitálnych službách je prispôsobiť sa rýchlo sa vyvíjajúcim digitálnym technológiám a skúma sa v ňom, čo to znamená v súvislosti s technologickými a demokratickými výzvami, ako sú nenávistné prejavy, dezinformácie na internete a stratégie zamerané na destabilizáciu. Významný pokrok v rokovaniach Európskeho parlamentu a Rady by mal umožniť rýchle prijatie balíka.

VII. VŠEOBECNEJŠIA PRIPRAVENOSŤ

V čase návratu vojny do Európy, ako aj čase významných geopolitických posunov sa zvýšila úroveň bezpečnostnej koordinácie v EÚ na základe iniciatív, ktoré sa pripravovali už pred ruskou útočnou vojnou proti Ukrajine. Iniciatívy zamerané hlavne na vonkajšiu bezpečnosť EÚ majú významné dôsledky pre internú agendu bezpečnostnej únie.

Komisia 15. februára 2022 predložila **obranný balík**[53] obsahujúci viaceré iniciatívy v oblastiach kritických pre obranu a bezpečnosť v EÚ. Tento príspevok Komisie k európskej obrane a bezpečnosti pokrýva celú škálu výziev. Navrhujú sa v ňom konkrétne kroky na dosiahnutie väčšej integrovanosti a konkurencieschopnosti európskeho obranného trhu, najmä posilnením spolupráce s EÚ a dosahovaním úspor z rozsahu. Takisto zahŕňa plán týkajúci sa kritických technológií pre bezpečnosť a obranu zameraný na posilnenie výskumu, technologického vývoja a inovácií v týchto sektoroch a na zníženie závislosti v oblasti

[51] Útvar pre strategickú komunikáciu, osobitné skupiny a analýzu informácií Európskej služby pre vonkajšiu činnosť poskytuje strategickú komunikačnú podporu pri vykonávaní zahraničnej a bezpečnostnej politiky EÚ v príslušných prioritných regiónoch (južné a východné susedstvo, západný Balkán) tým, že vypracúva a vykonáva osobitné komunikačné opatrenia zamerané na podporu politík, hodnôt, cieľov a záujmov EÚ.

[52] https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/.

[53] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en.

kritických technológií a hodnotových reťazcov. Cieľom balíka je aj posilniť obranný rozmer vesmíru na úrovni EÚ. Okrem toho sa v balíku skúma, ako by Komisia mohla posilniť svoje opatrenia na boj proti hybridným hrozbám, a to aj v kybernetickej oblasti, zvýšiť vojenskú mobilitu v rámci Európy a mimo nej a ďalej sa zaoberať výzvami v oblasti zmeny klímy súvisiacimi s obranou. Na doplnenie tohto úsilia sa v spoločnom oznámení o **analýze nedostatku investícií do obrany a ďalšom postupe**[54] z 18. mája analyzujú nedostatky v spôsobilostiach a priemysle, ktoré je potrebné riešiť, s cieľom podporovať najviac ohrozené členské štáty EÚ a identifikovať opatrenia na zmiernenie identifikovaných nedostatkov.

Odolnosť EÚ voči týmto hrozbám si takisto vyžaduje prístupy zamerané na spôsobilosť v jednotlivých sektoroch bezpečnosti, ako sa uvádza v akčnom pláne Komisie pre synergie medzi civilným, obranným a vesmírnym priemyslom[55]. V súčasnosti sa pracuje na podpore prístupov zameraných na spôsobilosť v oblasti vnútornej bezpečnosti a presadzovania práva.

Rada 21. marca 2022 prijala **Strategický kompas pre bezpečnosť a obranu**[56], ktorý krátko nato schválila Európska rada. Kompas obsahuje ambiciózny akčný plán na posilnenie bezpečnostnej a obrannej politiky EÚ do roku 2030. Cieľom je dosiahnuť, aby bola EÚ silnejším a schopnejším garantom bezpečnosti, ktorý chráni svojich občanov a prispieva k medzinárodnému mieru a bezpečnosti. Obsahuje konkrétne návrhy s veľmi presným harmonogramom vykonávania s cieľom zlepšiť schopnosť EÚ rázne konať v krízových situáciách.

Jedným z cieľov strategického kompasu je vytvoriť **súbor hybridných nástrojov EÚ**, ktorý by mal tvoriť rámec pre koordinovanú reakciu na hybridné kampane zasahujúce EÚ a jej členské štáty, vrátane vnútorných a vonkajších opatrení. Po identifikácii východísk sektorovej odolnosti vykonanej začiatkom roka 2022[57] bude treba uskutočniť analýzu nedostatkov a potrieb. Práve v tomto rámci bude EÚ pokračovať v zlepšovaní pripravenosti, odolnosti a reakcie na hrozby vyplývajúce z ruskej agresie a iných pokusov o destabilizáciu demokracií a multilaterálneho poriadku založeného na pravidlách.

VIII. VÝHĽAD DO BUDÚCNOSTI

Pokiaľ ide o budúcnosť, EÚ bude musieť byť naďalej mimoriadne ostražitá v súvislosti s vyvíjajúcimi sa hrozbami a zlepšovať **pripravenosť na všetky možnosti a odolnosť voči nim**. Dosahy vojny môžu mať rôzne podoby a nie všetky z nich zatiaľ možno vyhodnotiť.

Rozsah vysídlenia ukrajinských zločineckých sietí zatiaľ nie je známy. Z doterajšej judikatúry Eurojustu vyplýva trend obchodovania s heroínom z Afganistanu do EÚ cez Ukrajinu, ako potvrdilo Európske monitorovacie centrum pre drogy a drogovú závislosť (EMCDDA)[58]. Vzhľadom na nestabilnú situáciu sa môže boj proti obchodovaniu s heroínom na tejto trase sťažiť, čím sa zvýši riziko možného zvýšenia toku drog do EÚ.

---

54 JOIN(2022) 24.

55 COM(2021) 70.

56 Strategický kompas pre bezpečnosť a obranu – za Európsku úniu, ktorá chráni svojich občanov, hodnoty a záujmy a prispieva k medzinárodnému mieru a bezpečnosti. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/sk/pdf.

57 SWD(2022) 21 final.

58 *Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data)* [Správa o situácii na Ukrajine v oblasti drog a alkoholu za rok 2020 (podľa údajov z roku 2019)], OEDT, *Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of*

Niektoré riziká hroziace EÚ sa na konci alebo počas potenciálnych prerušení bojov pravdepodobne zvýšia. S mimoriadnou pozornosťou sa budú sledovať strelné zbrane v obehu, pričom riziko sa zvýši, keď boje na Ukrajine poľavia. Zo skúseností z minulosti takisto vyplýva, že existuje riziko, že návrat zahraničných bojovníkov, ktorí získali bojové skúsenosti a ktorí sa môžu dostať do kontaktu s extrémistickými skupinami, môže neskôr do EÚ vniesť teroristickú činnosť. Tento potenciálny jav by sa mal dôkladne monitorovať a Komisia v súčasnosti už sprostredkúva diskusie medzi členskými štátmi o výzvach, ktoré predstavuje návrat zahraničných bojovníkov s násilnou extrémistickou minulosťou.

Vzhľadom na tieto možné hrozby je dôležité pokračovať vo vykonávaní stratégie pre bezpečnostnú úniu, a to aj prostredníctvom vykonávania kľúčových stratégií, ako sú stratégia kybernetickej bezpečnosti EÚ, stratégia EÚ na boj proti organizovanej trestnej činnosti (2020 – 2025), program EÚ v oblasti boja proti terorizmu (2020 – 2025), akčný plán EÚ na boj proti nedovolenému obchodovaniu so strelnými zbraňami (2020 – 2025), stratégia EÚ v oblasti boja proti obchodovaniu s ľuďmi (2021 – 2025) a protidrogová stratégia EÚ (2021 – 2025).

Naďalej sa bude vyvíjať úsilie o vytvorenie potrebného legislatívneho rámca pre EÚ. Komisia v súčasnosti napríklad pripravuje posúdenie vplyvu návrhu týkajúceho sa regulácie uvádzania vysokorizikových chemických látok na trh a ich používania.

IX. ZÁVER

Bezpečnostná únia naďalej zohráva dôležitú úlohu v príprave EÚ a jej členských štátov na boj proti existujúcim a potenciálnym hrozbám. Ruská útočná vojna proti Ukrajine odhalila, ako rýchlo sa teoretické hrozby môžu stať skutočnými, a zdôrazňuje význam ostražitosti, koordinácie a pripravenosti.

Táto štvrtá správa o pokroku pri vykonávaní stratégie EÚ pre bezpečnostnú úniu je dôkazom toho, že EÚ je schopná prispôsobiť sa dokonca aj mimoriadnym a neočakávaným hrozbám, ako sú hrozby vyplývajúce z ruskej útočnej vojny proti Ukrajine. Odhodlanie vo vykonávaní stratégie EÚ pre bezpečnostnú úniu je dôležitejšie než kedykoľvek predtým.

---

a controlled delivery (Zastavenie obchodovania s náhradou heroínu vo Francúzsku, v Poľsku a na Ukrajine vrátane plánovania a uskutočnenia kontrolovanej dodávky), 2021/00446, Eurojust, máj 2020.