



Brusel 27. května 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	

#### PRŮVODNÍ POZNÁMKA

---

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	25. května 2022
Příjemce:	Generální sekretariát Rady
Č. dok. Komise:	COM(2022) 252 final
Předmět:	SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ o čtvrté zprávě o pokroku v provádění strategie bezpečnosti unie EU

---

Delegace naleznou v příloze dokument COM(2022) 252 final.

---

Příloha: COM(2022) 252 final



V Bruselu dne 25.5.2022  
COM(2022) 252 final

**SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ**  
**o čtvrté zprávě o pokroku v provádění strategie bezpečnosti unie EU**

## I. ÚVOD

Bezpečnostní agendě EU v současné době dominuje vojenská agrese Ruska vůči Ukrajině. Válka neohrožuje pouze Ukrajinu, jejím cílem je narušit celosvětovou stabilitu a bezpečnost. To vnáší do EU řadu rizik pro bezpečnost občanů. Objevují se nové nejistoty ohledně dodávek energií a dalších surovin, přičemž cílem kybernetických útoků může být také kritická infrastruktura. Vnitřní bezpečnost EU a její ochrana jsou ohroženy možnými útoky nebo haváriemi způsobenými chemickými, biologickými, radiologickými nebo chemickými látkami ve válečné zóně. Zranitelnost milionů lidí, kteří před válkou uprchli, může být rychle zneužita organizovaným zločinem prostřednictvím obchodování se ženami a dětmi, jež jsou obzvláště ohroženy.

Tváří v tvář těmto novým a potenciálním hrozbám zůstala EU odhodlaná a sjednocená. Přestože dopad války zůstal prozatím omezen hlavně na území Ukrajiny, EU zvýšila *ostrážitost a koordinaci* a posílila sledování oblasti hrozeb a pracuje na zvýšení odolnosti, aby zajistila svoji *přípravenost*.

Ve Versailleském prohlášení ze dne 10. a 11. března 2022<sup>1</sup> evropská lídř zdůraznili, že je třeba se připravit na rychle se objevující výzvy tím, že „se budeme chránit před rostoucím nebezpečím hybridní války, posílíme naši kybernetickou odolnost, budeme chránit naši infrastrukturu – zejména kritickou – a budeme bojovat proti dezinformacím“.

Bezpečnostní rámec unie má zásadní význam pro zajištění bezpečnosti v celé EU. V současném geopolitickém kontextu jsou v souvislosti s tímto úkolem stále aktuální čtyři strategické priority stanovené ve strategii bezpečnostní unie<sup>2</sup>: i) bezpečnostní prostředí, které ob stojí v budoucnu; ii) potírání vyvíjejících se hrozeb; iii) ochrana Evropanů před terorismem a organizovaným zločinem a iv) silný evropský bezpečnostní ekosystém. Válka zviditelnila potřebu, aby EU a její členské státy plně využívaly právní a politické nástroje, které jsou již k dispozici v rámci strategie bezpečnostní unie, a které jsou základem koordinované podpory EU členskými státy při řešení otázek od organizovaného zločinu a terorismu až po kybernetickou bezpečnost a hybridní hrozby.

V reakci na válku na Ukrajině zvýšily své úsilí také evropské agentury působící v oblasti spravedlnosti a vnitřních věcí, které hrají klíčovou roli při posuzování hrozeb a podpoře operativních reakcí<sup>3</sup>. Dalším důležitým faktorem je neustálé posilování operativních postupů a správy schengenského prostoru.

Tato čtvrtá zpráva o pokroku na cestě k bezpečnostní unii se zaměřuje na vývoj v posledních několika měsících od doby, kdy začala ruská útočná válka proti Ukrajině. Poskytuje přehled opatření přijatých ve všech oblastech bezpečnostní unie a posuzuje potřeby týkající se připravenosti, které vyplývají z potenciálních bezpečnostních hrozeb vyvstávajících v souvislosti s válkou na Ukrajině. Pokrok v dalších tématech bezpečnostní unie je uveden v příloze.

---

<sup>1</sup> <https://www.consilium.europa.eu/media/54804/20220311-versailles-declaration-cs.pdf>

<sup>2</sup> COM(2020) 605.

<sup>3</sup> [Společné prohlášení agentur EU pro spravedlnost a vnitřní věci k Ukrajině | Agentura Evropské unie pro otázky azylu \(europa.eu\)](#)

## II. KYBERNETICKÁ BEZPEČNOST A KRITICKÁ INFRASTRUKTURA

Od vypuknutí války dávají soukromé subjekty a pachatelé zločineckých operací na vědomí, že provádějí činnosti v kyberprostoru na podporu jedné či druhé strany. Hacktivismus<sup>4</sup> představuje hrozbu kvůli riziku vedlejších účinků na kritické služby v EU, riziku útoků pocházejících z oficiálních sítí nebo jiným nepředvídaným vedlejšími účinkům. Ačkoli dosud byla válka vedena převážně konvenčními prostředky a její vedlejší účinky byly omezené, riziko eskalace v této oblasti je reálné.

EU proto posílila svou koordinaci a připravenost. Hrozby plynoucí z války zdůrazňují potřebu vybudovat kulturu sdílení informací a odborných znalostí mezi EU, členskými státy a napříč komunitami působícími v oblasti kybernetické bezpečnosti. To zahrnuje budování integrovaného situačního povědomí, které sdílejí orgány, instituce a agentury EU a členské státy, zejména pokud jde o kritickou infrastrukturu, na níž závisí hladké fungování vnitřního trhu.

### **Připisování kybernetických útoků proti Ukrajině**

Kybernetické útoky na samotnou Ukrajinu začaly ještě před ruskou agresí a v prvních dnech války<sup>5</sup> se zaměřovaly na ohrožování uživatelských účtů ukrajinských vojenských složek a na narušení fungování základních služeb včetně kontroly hranic a telekomunikací.

Dne 14. ledna 2022 učinil vysoký představitel jménem Evropské unie prohlášení,<sup>6</sup> v němž odsoudil kybernetické útoky proti Ukrajině a znovu potvrdil jednoznačnou podporu EU Ukrajině.

Dne 10. května Evropská unie a její členské státy společně s mezinárodními partnery ostře odsoudily<sup>7</sup> nepřátelskou činnost v kyberprostoru namířenou proti Ukrajině ze dne 24. února, jejímž cílem byla satelitní síť KA-SAT, kterou vlastní společnost Viasat, a útok přímo připisaly Ruské federaci. Tento kybernetický útok měl závažný dopad a způsobil plošné výpadky a narušení fungování komunikace u několika orgánů veřejné správy, podniků a uživatelů na Ukrajině a zasáhl i několik členských států EU.

### ***Ostražitost a koordinace***

<sup>4</sup> Nedávným příkladem hacktivismu je použití „protestního softwaru“ k šíření škodlivého softwaru na ruské IP adresy prostřednictvím populárního balíčku s otevřeným zdrojovým kódem, což by mohlo vést k rizikům pro dodavatelský řetězec a ke ztrátě důvěry v komunitě uživatelů softwaru s otevřeným zdrojovým kódem. Komise dala jasně najevo, že (i dobře míněné) kybernetické útoky na Rusko jsou nezákonné.

<sup>5</sup> Zvláštní zpráva společnosti Microsoft: [Přehled kybernetických útoků Ruska na Ukrajině](#); [Hybridní válka na Ukrajině – Vyjádření společnosti Microsoft k problémům](#)

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

<sup>7</sup> [Ruské kybernetické operace namířené proti Ukrajině: prohlášení vysokého představitele jménem Evropské unie – Rada \(europa.eu\)](#)

Od doby, co začala ruská útočná válka proti Ukrajině, se v členských státech a orgánech EU zintenzivnilo sledování situace v oblasti kybernetické bezpečnosti. ENISA, Agentura Evropské unie pro kybernetickou bezpečnost, Evropské centrum pro boj proti kyberkriminalitě při Europolu a skupina pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (CERT-EU), a Zpravodajské a informační centrum EU (EU INTCEN) přispěly ke sdílenému situačnímu povědomí v EU, mimo jiné tím, že pravidelně sledovaly podezřelé činnosti v kyberprostoru, včetně konkrétních odvětví, jako je energetika, doprava a letectví, a předkládaly posouzení, která sloužila k nasměrování preventivních opatření.

Zintenzivnila se rovněž koordinace a výměna informací se sítěmi pro kybernetickou bezpečnost, jako je síť styčných organizací pro kybernetické krize (CyCLONe), kterou tvoří vnitrostátní agentury působící v oblasti kybernetické bezpečnosti, Komise a agentura ENISA. Aby se tento přístup promítl i uvnitř orgánů EU, koordinační mechanismus, pracovní skupina pro řešení kybernetických krizí, umožňuje sdílení informací mezi všemi příslušnými službami a orgány a agenturami, včetně agentury ENISA, Evropského centra pro boj proti kyberkriminalitě v rámci Europolu a skupiny CERT EU. Je třeba neustále usilovat o zajištění komunikačních kanálů mezi politickou, operační a technickou úrovní, jakož i o posílení spolupráce se sítí skupin pro reakce na počítačové bezpečnostní incidenty (CSIRT).

Europol rovněž spustil nouzový protokol pro reakci prostřednictvím prosazování práva, který umožňuje důkladněji sledovat kybernetické hrozby a sdílet informace v širokém okruhu zúčastněných stran, a jehož cílem je vytvořit v oblasti kybernetické bezpečnosti komplexní zpravodajský obraz.

Kromě kybernetických hrozeb jsou členské státy, služba ESVČ a útvary Komise stále ostražitější, pokud jde o vystavení kritických infrastruktur nekybernetickým fyzickým hrozbám. Kritické infrastruktury a subjekty, jež je provozují, mohou být vystaveny fyzickým rizikům, jako je sabotáž ze strany státu nebo státem sponzorovaných aktérů v rámci možných odvetných opatření proti EU.

### ***Přípravenost***

Přípravenost v oblasti kybernetické bezpečnosti a bezpečnosti kritické infrastruktury má vzhledem ke zvýšené expozici Evropy vůči kumulaci hrozeb v důsledku války zásadnější význam než kdykoli předtím. Úsilí o zvýšení připravenosti zahrnovalo řadu přímých opatření, včetně těch, která byla plánována již před ruskou agresí vůči Ukrajině. Patří mezi ně cvičení, pokyny, legislativní opatření, zvyšování odolnosti v kritických odvětvích a spolupráce s partnery.

Francouzské předsednictví Rady Evropské unie společně s Evropskou službou pro vnější činnost (ESVČ) a Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) uspořádalo na začátku roku 2022 cvičení založené na scénáři nazvané EU CyCLES (Cyber Crisis Linking Exercise on Solidarity / Cvičení solidarity pro řešení kybernetických krizí), jehož cílem bylo zvýšit informovanost na politické úrovni a posílit spolupráci mezi operativní a politickou úrovní v případě rozsáhlého kybernetického útoku.

Agentura ENISA a skupina CERT-EU zveřejnily v únoru **pokyny**, jak zvýšit odolnost a připravenost v EU<sup>8</sup>. Tyto pokyny vyzývají všechny organizace ve veřejném i soukromém sektoru v EU, aby v oblasti kybernetické bezpečnosti přijaly minimální soubor osvědčených postupů a výrazně tak zlepšily kulturu kybernetické bezpečnosti. V březnu skupina CERT-EU za podpory agentury ENISA zveřejnila navazující technické pokyny<sup>9</sup> a bezpečnostní pokyny pro posílení konfigurace aplikací Signal<sup>10</sup> s řadou praktických doporučení pro organizace ke zlepšení jejich postoje ke kybernetické bezpečnosti.

### *Iniciativy legislativní povahy*

Ze současné situace vyvstává naléhavost, pokud jde o **provádění stávajících právních předpisů** a urychlení **přijetí připravovaných iniciativ**.

Komise podporuje členské státy při provádění **směrnice o bezpečnosti sítí a informací**<sup>11</sup>, která vyžaduje, aby členské státy byly náležitě vybaveny, disponovaly například skupinou pro reakce na počítačové bezpečnostní incidenty (CSIRT), a měly vymezené příslušné orgány. Je základem pro účinnou spolupráci mezi členskými státy. Politická shoda, kterou spolunormotvůrci našli ohledně **směrnice NIS2**<sup>12</sup>, představuje další průlom při zajišťování pevného rámce připravenosti EU.

### **NIS 2 - další posílení připravenosti**

- Nová směrnice o bezpečnosti sítí a informačních systémů bude řešit nedostatky předchozí směrnice NIS s cílem přizpůsobit ji současným potřebám a zajistit, aby obstála i v budoucnu. Stanoví minimální pravidla pro regulační rámec a mechanismy pro účinnou spolupráci mezi příslušnými orgány v jednotlivých členských státech.
- Rozšiřuje oblast působnosti pravidel a doplňuje nová odvětví, která mají zásadní význam pro hospodářství a společnost (například odvětví farmaceutických výrobků a zdravotnických prostředků nebo výroby potravin). Směrnice se bude vztahovat na všechny střední a velké subjekty, které jsou činné v příslušných odvětvích nebo které poskytují služby, jež směrnice zahrnuje. Zahrnuty jsou rovněž ústřední subjekty veřejné správy (vyjma soudnictví, parlamentů a centrálních bank) a na regionální úrovni. Členské státy mohou navíc rozhodnout, že se na tyto subjekty směrnice použije na místní úrovni.
- NIS2 stanoví základ pro opatření k řízení kybernetických bezpečnostních rizik a formálně zřizuje Evropskou síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe), která bude podporovat koordinované řízení rozsáhlých kybernetických bezpečnostních incidentů.
- Návrh rovněž zavádí přesnější ustanovení o postupu hlášení incidentů, obsahu hlášení a lhůtách a dále stanoví opravné prostředky a sankce k zajištění jejich prosazování.
- Členské státy budou mít od vstupu směrnice v platnost 21 měsíců na to, aby dotyčná ustanovení začlenily do svého vnitrostátního práva.

<sup>8</sup> Zvýšení kybernetické odolnosti vaší organizace – společná publikace, 14. února 2022.

<sup>9</sup> Bezpečnostní pokyny 2022-01 – Opatření ke zmírnění kritických hrozeb v oblasti kybernetické bezpečnosti.

<sup>10</sup> Bezpečnostní pokyny CERT-EU 22-002 – Posílení zabezpečení aplikace Signal.

<sup>11</sup> Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

<sup>12</sup> COM(2020) 823.

Na dosažený pokrok v souvislosti se směrnicí NIS 2 by mělo co nejdříve navazovat dokončení jednání o navrhované **směrnici o odolnosti kritických subjektů**<sup>13</sup>, díky které by se po jejím přijetí a provedení měla zvýšit odolnost kritických subjektů vůči řadě hrozeb, včetně teroristických útoků, vnitřních hrozeb nebo sabotáží. Je rovněž nezbytné, aby úroveň ambicí týkající se směrnice o posílení odolnosti kritických subjektů odpovídala úrovni návrhu Komise a aby byl zachován soulad s politickým kompromisem, který byl dosažen v případě směrnice NIS2. Společně tato opatření zvýší odolnost a připravenost zavedením soudržnějšího a spolehlivějšího systému a mimo jiné také prostřednictvím národních plánů reakce na incidenty a krize. Ty byly rovněž součástí doporučení Komise z loňského roku<sup>14</sup>, kterým se zřizuje **Společná kybernetická jednotka** a v němž se stanoví, jak mají jednotliví aktéři ekosystému kybernetické bezpečnosti (diplomacie, policie, civilní aktéři a případně ozbrojené složky) spolupracovat na operační úrovni. Současná podoba hrozeb vyzdvihuje hodnotu takové účinné spolupráce mezi klíčovými hráči.

Komise pokračuje ve sledování provádění souboru opatření pro kybernetickou bezpečnost **5G**<sup>15</sup>. V této souvislosti dne 11. května přijala skupina pro spolupráci v oblasti bezpečnosti sítí a informací zprávu o bezpečnosti sítě Open RAN<sup>16</sup>. Pokračuje rovněž ve spolupráci s členskými státy na zajištění plné funkčnosti Evropského centra kompetencí pro kybernetickou bezpečnost.

Dne 22. března 2022 Komise předložila **návrh nových pravidel, jimiž se mají zřídit společná opatření v oblasti kybernetické bezpečnosti a zabezpečení informací ve všech orgánech, institucích a jiných subjektech EU**. Tato pravidla posílí odolnost správy EU a její schopnost reagovat na kybernetické hrozby a incidenty. Zařazením těchto činností do společného rámce se posílí interinstitucionální spolupráce a minimalizuje se vystavení rizikům. Navrhované **nařízení o kybernetické bezpečnosti pro orgány, instituce a jiné subjekty EU**<sup>17</sup> posílí mandát skupiny CERT-EU a povede k vytvoření nového interinstitucionálního výboru pro kybernetickou bezpečnost, posílí kapacity v oblasti kybernetické bezpečnosti a podníká provádění pravidelného posouzení vyspělosti a zlepšení kybernetické hygieny. Navrhované **nařízení o zabezpečení informací**<sup>18</sup> vytvoří minimální soubor pravidel a norem pro zabezpečení informací za účelem bezpečného nakládání s informacemi a jejich bezpečné výměny mezi všemi orgány, institucemi a jinými subjekty EU, jimiž se má zajistit zvýšená a důsledná ochrana před vyvíjejícími se hrozbami pro jejich informace. Komise vyzývá Evropský parlament a Radu, aby tato opatření urychleně přijaly.

Komise nyní uzavřela veřejnou konzultaci o opatřeních ke zvýšení **kybernetické odolnosti** digitálních produktů a připravuje návrh, který bude zveřejněn na podzim tohoto roku<sup>19</sup>. Ten bude řešit zranitelnost digitálních produktů a doplňkových služeb, které sice vytvářejí

---

<sup>13</sup> COM(2020) 829.

<sup>14</sup> [Doporučení k vytvoření Společné kybernetické jednotky | Formování digitální budoucnosti Evropy \(europa.eu\)](https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-opatření)

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

<sup>16</sup> Skupina pro spolupráci v oblasti bezpečnosti sítí a informací, Zpráva o kybernetické bezpečnosti sítě Open RAN, 11. května 2022.

<sup>17</sup> COM(2022) 122.

<sup>18</sup> COM(2022) 119.

<sup>19</sup> [Akt o kybernetické odolnosti – nová pravidla kybernetické bezpečnosti pro digitální produkty a podpůrné služby \(europa.eu\)](#)

příležitosti pro hospodářství a společnosti EU, ale zároveň přináší nové výzvy, neboť čím více je vše propojeno, tím snáze může kybernetický bezpečnostní incident ovlivnit celý systém a narušit tak hospodářské i sociální činnosti.

Dne 9. března 2022 ministři EU odpovědní za telekomunikace jednomyslně přijali Neversovu výzvu k posílení kapacit EU v oblasti kybernetické bezpečnosti, která zahrnovala „zavedení nového fondu odezvy na mimořádné události v oblasti kybernetické bezpečnosti, který má být zřízen Komisí“<sup>20</sup>. Komise zvažuje, jak nejlépe využít stávající finanční prostředky na podporu preventivních opatření a opatření týkajících se reakce.

### *Kritická odvětví*

Bezpečnost dodávek **energií** v EU má zásadní význam pro blaho občanů a hladké fungování našich hospodářství a současná situace zdůraznila potřebu jasných pravidel v oblasti kybernetické bezpečnosti v tomto odvětví. Komise pracuje na kodexu sítě pro kybernetickou bezpečnost přeshraničních toků elektřiny, jak požaduje nařízení o elektřině<sup>21</sup>, aby byla stanovena pravidla pro posuzování rizik, společné minimální požadavky, plánování, sledování, podávání zpráv a řešení krizí. Vzhledem k ruské útočné válce proti Ukrajině se cíle zamýšlené pro kodex sítě pro kybernetickou bezpečnost stávají ještě aktuálnějšími. Komise rovněž zahájila strukturální spolupráci mezi agenturou ENISA, sítí ENTSO-E<sup>22</sup>, sítí ENTSOG<sup>23</sup> a Energetickým společenstvím při pravidelném sledování situace v oblasti kybernetické bezpečnosti v odvětví energetiky.

EU se snaží chránit bezpečnost svých partnerů, aniž by sama pro sebe vytvářela nová rizika. Nouzová synchronizace elektrizačních soustav Ukrajiny a Moldavska se soustavou kontinentální Evropy, zejména z hlediska kybernetické bezpečnosti, proběhla v březnu 2022 po přijetí opatření ke zmírnění rizik.

Válka a sankce rovněž způsobily řadu problémů v **dopravě** EU, od bezpečnostních rizik pro civilní letectví EU a řidičů nákladních vozidel, kteří uvízli v konfliktních zónách, až po zničení ukrajinské dopravní infrastruktury, přerušení dodavatelských řetězců a ohrožení celosvětového potravinového zabezpečení. Agentura Evropské unie pro bezpečnost letectví v úzké spolupráci s Komisí a agenturou Eurocontrol, Evropskou organizací pro bezpečnost letového provozu, doporučuje od začátku války provozovatelům, aby neprovozovali lety ve vzdušném prostoru Ukrajiny a vyhýbali se používání vzdušného prostoru v okruhu 100 námořních mil od hranic s Běloruskem a hranice Ruska s Ukrajinou.

Komise rovněž pracuje na posílení připravenosti a odolnosti odvětví dopravy v EU. Zejména nový pohotovostní plán pro dopravu<sup>24</sup>, přijatý 23. května, čerpá poučení jak z pandemie COVID-19, tak z vojenské agrese Ruska proti Ukrajině. Navrhuje soubor deseti opatření, jimiž by se EU a její členské státy měly řídit při zavádění opatření pro reakci na krizové

---

<sup>20</sup> [08/03/2022 – Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique – Presse – Ministère des Finances \(economie.gouv.fr\)](#)

<sup>21</sup> Nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou, Úř. věst. L 158, 14.6.2019, s. 54. Návrh je v současné době přezkoumáván Agenturou pro spolupráci energetických regulačních orgánů.

<sup>22</sup> Evropská síť provozovatelů elektroenergetických přenosových soustav.

<sup>23</sup> Evropská síť provozovatelů plynárenských přepravních soustav.

<sup>24</sup> COM(2022) 21.

situace, včetně zajištění minimální konektivity, budování odolnosti vůči kybernetickým a hybridním hrozbám a posílení spolupráce s mezinárodními partnery v oblasti připravenosti na krize a reakce na ně. Zdůrazňuje také význam pravidelného testování odolnosti založeného na různých krizových scénářích, propojování příslušných agentur EU nebo jiných aktérů a navazování na stávající procesy.

Podle rámce **EU pro zdravotní bezpečnost** musí být výměna informací založená na systému včasného varování a reakce, včetně podpory zdravotnických odsunů z Ukrajiny, chráněna před kybernetickými útoky, a proto se bezpečnost systému posiluje.

### *Spolupráce s partnery*

EU pokračuje ve spolupráci se svými mezinárodními partnery v otázkách předcházení nepřátelskému chování v kyberprostoru, odrazování a odstrašování od takového chování a reakce na něj. Vlivem ruské agresivní války proti Ukrajině se spolupráce v této oblasti stala důležitější než kdykoli předtím. V tomto ohledu pracuje ESVČ na výměně informací o situaci a koordinaci reakce na nepřátelské kybernetické činnosti cílící na Ukrajinu, jakož i na podpoře Ukrajiny a dalších zemí v regionu ve spolupráci s partnery, včetně USA a NATO, s cílem zajistit doplňkovost a zabránit překrývání.

Úzká spolupráce s USA se zintenzivnila také v rámci Rady EU–USA pro obchod a technologie (TTC). Ve společném prohlášení<sup>25</sup>, které navazovalo na květnové zasedání ministrů v Paříži, byla zdůrazněna ústřední role rady TTC pro obnovené transatlantické partnerství, které slouží ke koordinaci společných opatření EU a USA v souvislosti s ruskou agresí proti Ukrajině. Obě strany se shodly, že úzká spolupráce na zvýšení odolnosti dodavatelských řetězců je důležitější než kdykoli předtím. Kromě toho byla zřízena specializovaná pracovní skupina pro veřejné financování bezpečné a odolné digitální infrastruktury ve třetích zemích, jejímž úkolem je připravit základy pro společné veřejné financování digitálních projektů ve třetích zemích z prostředků USA–EU na základě souboru společných zastřešujících zásad.

Strategický kompas přijatý v březnu 2022 (viz oddíl VII) dále posílí soubor nástrojů EU pro diplomacii v oblasti kybernetiky EU a rozvine politiku pro kybernetickou obranu EU, aby byla lépe připravena na kybernetické útoky a lépe na ně reagovala, a to v rámci širší strategie pro posílení schopnosti EU jednat v krizových situacích a hájit své zájmy.

### **Podpora Ukrajiny a sousedních zemí v oblasti kybernetické bezpečnosti**

EU podporovala kybernetickou odolnost Ukrajiny už před válkou. Již v červnu 2021 uspořádaly EU a Ukrajina první kybernetický dialog a EU poskytla zemi prostřednictvím programu EU4Digital Ukraine podporu na kybernetickou bezpečnost a odolnou digitální transformaci ve výši 25 milionů EUR. Další twinningový program v hodnotě 1,5 milionu EUR má pomoci ukrajinským institucím v oblasti kybernetické bezpečnosti dosáhnout souladu s normami EU.

Po vypuknutí války EU podporuje spolupráci mezi odborníky na kybernetiku z EU a Ukrajiny a koordinuje poskytování technické pomoci, vybavení, softwaru a příslušných služeb s cílem posílit kybernetickou odolnost a kybernetickou obranu Ukrajiny.

<sup>25</sup> [https://ec.europa.eu/commission/presscorner/detail/cs/STATEMENT\\_22\\_3108](https://ec.europa.eu/commission/presscorner/detail/cs/STATEMENT_22_3108)

Kromě toho EU pracuje na posouzení možné střednědobé podpory pro Moldavsko, Gruzii a západní Balkán. Ve dnech 3. a 4. března 2022 se uskutečnila společná hodnotící mise Moldavska zaměřená na potřeby v oblasti kybernetické bezpečnosti, která vedla k přijetí zvláštního opatření pro krizovou reakci s cílem rychle zvýšit kybernetickou bezpečnost v zemi. Podobná podpora rychlé reakce se připravuje i pro vybrané země západního Balkánu, u nichž je úroveň rizika považována za zvláště vysokou v důsledku toho, že se na ně vztahují sankce EU. Posuzuje se také možná další pomoc Moldavsku prostřednictvím Evropského mírového nástroje.

### III. ORGANIZOVANÝ ZLOČIN A TERORISMUS

Ruská agresivní válka proti Ukrajině donutila miliony lidí opustit své domovy a výrazně zvýšila pohyb přes vnější hranice EU. Do 18. května přišlo do EU téměř 6 milionů osob z Ukrajiny a Moldavska a do dnešního dne se 2,8 milionu osob zaregistrovalo pro dočasnou ochranu v EU. EU se snaží zajistit co nejrychlejší a nejpružnější přijetí těchto osob přechajících před válkou, aniž by tím ohrozila bezpečnost na vnější hranici EU. EU přijala bezprecedentní opatření, aby mohla lidem přechajícím před válkou poskytnout dočasnou ochranu, a zavázala se, že se všemi nově příchozími bude jednat bez diskriminace. Současně však nelze opomíjet potenciální rizika, která mohou vzniknout v souvislosti s takovým množstvím lidí v pohybu, a EU – za výrazné podpory příslušných agentur EU – zůstává ostražitá, pokud jde o nový vývoj v oblasti organizovaného zločinu a terorismu.

#### Silný Schengen v době zvýšených hrozeb

Zajištění vysoké úrovně bezpečnosti v **schengenském** prostoru a v rámci EU nebylo nikdy tak důležité jako v atmosféře zvýšených hrozeb, které přináší válka těsně za vnější hranici EU.

V rámci plnění ambiciózního programu pro schengenský prostor stanoveného ve strategii z června 2021 přijala Komise v květnu první zprávu o stavu Schengenu<sup>26</sup>. Roční schengenský cyklus zavádí nový model správy schengenského prostoru a v jeho rámci probíhá pravidelná kontrola stavu Schengenu. To pomůže zajistit rychlou identifikaci nedostatků a účinné návazné postupy, aby se schengenský prostor stal silnějším a odolnějším.

Tato první zpráva uznává, že je třeba zintenzivnit úsilí o provádění klíčových iniciativ na úrovni EU, včetně systematických kontrol všech cestujících na vnějších hranicích za plného využití mandátu agentur Frontex a Europol, jakož i navrhovaných a dostupných nástrojů přeshraniční policejní spolupráce.

Základem úsilí o zlepšení vnitřní bezpečnosti a správy hranic je zejména nová architektura informačních systémů EU pro ochranu hranic, řízení migrace a zajišťování bezpečnosti a jejich interoperabilita. Zásadní význam bude mít účinné provedení všech prvků rámce interoperability v souladu s dohodnutými časovými harmonogramy.

<sup>26</sup> COM(2022) 301.

## *Ostražitost a koordinace*

Intenzivnější spolupráce v oblasti prosazování práva napříč členskými státy a s třetími zeměmi má klíčový význam, pokud jde o zajištění informovanosti o nově se objevujících hrozbách teroristických útoků a trestných činů a schopnosti zasáhnout proti zločineckým sítím a jednotlivcům, kteří se mohou pokusit využít války proti Ukrajině ve svůj prospěch. Členské státy a operační partneři aktivně sdílejí relevantní dostupné informace a zpravodajské informace o trestné činnosti s Europolem, který provádí křížovou kontrolu těchto informací, analyzuje je a přetváří ve využitelná provozní zpravodajská oznámení, jako například oznámení včasného varování a hodnocení hrozeb, která jsou sdílena s partnery.

## *Organizovaná trestná činnost*

Organizovaná trestná činnost již hledá způsoby, jak současné situace využít. Prvotní zpravodajská analýza odhalila vzorce trestné činnosti v řadě oblastí, včetně obchodování s lidmi, nepravdivých prohlášení o dovezeném a vyvezeném zboží, internetových podvodů, kyberkriminality a nedovoleného obchodování s palnými zbraněmi. Existují také důkazy o pachatelích kybernetických trestných činů, kteří se vydávají za shromažďovatele veřejných prostředků na podporu Ukrajiny, aby zcizili peníze a kryptoměny<sup>27</sup>. Zločinná spolčení z Ukrajiny se mohou vzhledem k současné situaci pokusit přesídlit a pokračovat ve své činnosti v EU.

Komise a francouzské předsednictví Rady vzájemně spolupracovaly, mimo jiné i s agenturami EU působícími v oblasti spravedlnosti a vnitřních věcí, a zejména pak s Europolem, na mobilizaci evropské multidisciplinární platformy pro boj proti hrozbám vyplývajícím z trestné činnosti (**EMPACT**), aby vyhodnotily stávající nebo nově se objevující hrozby závažné a organizované trestné činnosti, mohly je předjímat a také jim předcházet a čelit. Dne 7. dubna 2022 uspořádala agentura Europol setkání platformy EMPACT, na němž se sešli zástupci a odborníci z členských států EU a bezpečnostního společenství EU, aby se zaměřili na hrozby závažné a organizované trestné činnosti, které se objevily v důsledku války na Ukrajině. Konkrétní kroky, o nichž se diskutovalo, zahrnovaly shromažďování dalších zpravodajských informací, provádění nouzových operativních opatření a přesměrovávání zaměření stávajících opatření, jakož i dny společných akcí ad hoc.

**CELBET** (celní odborná skupina pro východní a jihovýchodní pozemní hranice) – projekt spolupráce financovaný Evropskou komisí – sleduje vývoj na hranicích v rámci své mise cílené na poskytování provozní podpory a poradenství celníkům a monitoruje případy zabavení celními orgány na hraničních přechodech na hranicích EU (Polsko, Slovensko, Maďarsko a Rumunsko) s Ukrajinou.

## *Trestná a teroristická činnost*

---

<sup>27</sup> Skupina Google's Threat Analysis Group (skupina pro analýzu hrozeb společnosti Google) zaznamenala rostoucí počet aktérů, kteří využívají válku na Ukrajině jako prvek k nalákání pro účely phishingových a malwarových kampaní. Výzkumníci společnosti Cyren, která se zabývá internetovou bezpečností, hlásí nárůst kryptopodvodů, které využívají konfliktu prostřednictvím falešných dárcovských webových stránek.

Přestože v EU prozatím nevyvstala v souvislosti s ruskou invazí na Ukrajinu žádná bezprostřední teroristická hrozba, potřeba zachovávat ostražitost je očividná.

Zvýšení rizika v souvislosti s trestnou a teroristickou činností vyzdvihuje skutečnost, že je důležité, aby členské státy využívaly příslušné databáze EU, jako je Schengenský informační systém, a v případě potřeby do nich vkládaly údaje a nahlížely do nich při kontrolách osob vstupujících do EU. To pomůže zajistit, aby jednotlivci, kteří představují hrozbu pro vnitřní bezpečnost EU, byli identifikováni na vnějších hranicích. Agentura Evropské unie pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (eu-LISA) nadále zajišťuje plnou dostupnost a účinnost systémů EU pro správu hranic. Pokyny<sup>28</sup> členským státům objasnily, jakým způsobem vyvážit potřebu zajištění plynulého odbavení příchozích na vnější hranici a současného provedení nezbytných bezpečnostních kontrol.

### ***Přípravenost***

Kromě poradenství a koordinace byla připravenost EU posílena i nasazením zaměstnanců agentur EU.

**Europol** vyslal do členských států EU sousedících s Ukrajinou operační týmy. Tyto týmy se skládaly z hostujících příslušníků agentury Europol z členských států a odborníků Europolu v Maďarsku, Litvě, Polsku, Rumunsku, na Slovensku a v Moldavsku<sup>29</sup>. Hostující příslušníci agentury Europol pomáhají vnitrostátním orgánům s bezpečnostními kontrolami v druhé linii na vnějších hranicích EU. Odborníci Europolu shromažďují a vyhodnocují informace za účelem odhalování hrozeb vyplývajících z teroristické a trestné činnosti, aby byla podpořena vyšetřování a byly identifikovány osoby, jejichž pokusy o vstup do EU představují riziko. Tyto operační týmy shromažďují informace, které doplňují posouzení hrozeb vyplývajících z trestné činnosti, jež mají k dispozici členské státy. Takové shromažďování zpravodajských informací umožňuje Europolu předjímat vývoj a koordinovat operační činnosti s členskými státy EU tak, aby mohly reagovat na aktivity zločineckých skupin, které se snaží využít války na Ukrajině, a navázat na aktivní spolupráci Europolu s ukrajinskými donucovacími orgány prostřednictvím ukrajinského styčného důstojníka, který je přítomen v sídle Europolu v Nizozemsku.

**Evropská agentura pro pohraniční a pobřežní stráž (Frontex)** je v členských státech a sousedních zemích EU přítomna také, aby poskytovala podporu při provádění operací hraničních kontrol: v současné době je v celé EU, na západním Balkáně a v Moldavsku rozmístěno více než 2 100 příslušníků pohraniční stráže. **Evropský podpůrný úřad pro otázky azylu (EUAA)** rozmístil téměř 750 zaměstnanců v členských státech jižní části EU a Litvě, aby poskytovali podporu při operačních činnostech, posílili přijímací kapacity a pomáhali s azylovými řízeními.

---

<sup>28</sup> Sdělení Komise, kterým se stanoví operační pokyny pro správu vnějších hranic s cílem usnadnit překračování hranic mezi EU a Ukrajinou 2022/C 104 I/01.

<sup>29</sup> Od 3. května nasadila agentura Europol jednoho svého zaměstnance a tři hostující příslušníky na Slovensku, jednoho příslušníka Europolu v Polsku, jednoho příslušníka Europolu a čtyři hostující příslušníky v Rumunsku a dva hostující příslušníky v Maďarsku. Jeden zaměstnanec Europolu a dva hostující příslušníci jsou nasazeni v Moldavsku.

V návaznosti na stávající **průmské rozhodnutí**<sup>30</sup>, které poskytuje členským státům rámec pro nasazení příslušníků donucovacích orgánů pro účely provádění společných operací, například společných hlídek, zaslaly Komise a francouzské předsednictví Rady Evropské unie všem členským státům společný dopis s cílem identifikovat potřeby, ve kterém současně žádají o nasazení policistů za účelem zahájení provádění společných hlídek v členských státech EU nacházejících se v přední linii, jež jsou nejvíce postiženy hromadným překračováním hranic v důsledku války. Komise bude tato nasazení financovat z Fondu pro vnitřní bezpečnost – policie.

### **Boj proti obchodování s lidmi**

EU byla od prvních dnů války ve střehu, pokud jde o rizika jedné konkrétní oblasti trestné činnosti, která by mohla těžit z obrovského pohybu lidí hledajících bezpečí v EU. Bylo nezbytné zabránit obchodníkům s lidmi zaměřovat se na cestující zranitelné osoby, kterými jsou většinou **ženy a děti**, například prostřednictvím falešných nabídek dopravy nebo ubytování.

V březnu vydaly Europol a Eurojust příslušným vnitrostátním orgánům oznámení včasného varování o možném obchodování s lidmi a vykořisťování obětí přicházejících z Ukrajiny. Agentura Eurojust pomáhá zlepšovat výměnu informací a urychlovat justiční spolupráci, včetně spolupráce s Ukrajinou. Vyšetřování případů obchodování s lidmi bylo předáno agentuře ke koordinaci.

Koordinátor EU pro boj proti obchodování s lidmi pořádal setkání se zástupci sítě EU sdružující vnitrostátní zpravodaje nebo rovnocenné mechanismy, s agenturami pro spravedlnost a vnitřní věci a platformami občanské společnosti EU pro boj proti obchodování s lidmi za účelem výměny informací o opatřeních potřebných k předcházení a potírání zneužívání a k ochraně obětí. V několika členských státech bylo zahájeno vyšetřování potenciálních případů.

EU rychle a aktivně zajistila koordinovanou reakci na tuto skutečnou hrozbu, které jsou vystaveni lidé, jež potřebují pomoc EU. Členským státům provádějícím směrnici o poskytování dočasné ochrany na podporu osob prchajících před válkou na Ukrajině byly rychle nabídnuty operační pokyny<sup>31</sup>, včetně pokynů týkajících se problematiky obchodování s lidmi. V rámci desetibodového plánu na posílení evropské koordinace přijímání osob prchajících před válkou z Ukrajiny<sup>32</sup>, který byl představen na zasedání Rady pro spravedlnost a vnitřní věci dne 28. března 2022, vypracoval koordinátor EU pro boj proti obchodování s lidmi ve spolupráci s agenturami EU a členskými státy společný plán boje proti obchodování s lidmi<sup>33</sup> zaměřený na předcházení tomuto obchodu a pomoc obětem. Zvláštní pozornost je věnována registraci subjektů a jednotlivců (včetně dobrovolníků), kteří hodlají poskytnout ubytování, dopravu a další druhy pomoci, a také provádění ověřování spolehlivosti. Komise rovněž spolupracuje s agenturou EUAA, které poskytuje podporu při odhalování obětí obchodování s lidmi v rámci posuzování zdravotního stavu v přijímacích střediscích. Děti bez

<sup>30</sup> 2008/615/SVV, 2008/616/SVV.

<sup>31</sup> C/2022/1806, EUR-Lex – 52022XC0321(03) – CS – EUR-Lex (europa.eu).

<sup>32</sup> [https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine\\_en](https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en)

<sup>33</sup> [https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11\\_en](https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en)

doprovodu nebo děti odloučené od rodin jsou obzvláště ohroženy zneužíváním, pohlavním vykořisťováním nebo nucenou trestnou činností. Výše uvedené operační pokyny slouží také jako vodítko, které má členským státům pomoci při řešení příchodu, přijímání a poskytování podpory dětem, zejména nezletilým osobám bez doprovodu. Za účelem zvýšení informovanosti ohrožených osob spustila Komise také speciální internetové stránky, které obsahují sekci s praktickými radami, jak se vyhnout obchodníkům s lidmi.

Zatímco některá opatření na zvýšení připravenosti byla přijata konkrétně v reakci na nové podmínky, které nastaly v důsledku války, další klíčová opatření vyplývají z **legislativních iniciativ**, které byly připravovány již před ruskou agresivní válkou proti Ukrajině.

Komise vítá dohodu z února 2022 o revidovaném mandátu<sup>34</sup> **Europolu**, která po svém provedení umožní Europolu lépe podporovat členské státy v boji proti organizované trestné činnosti a terorismu. Agentura pak bude mít k dispozici ty správné nástroje a záruky na podporu policejních složek při provádění analýzy velkého objemu údajů pro vyšetřování trestné činnosti a při vývoji průkopnických metod zaměřených na boj proti kyberkriminalitě. Tyto změny přicházejí s posíleným rámcem ochrany údajů, jakož i se silnějším parlamentním dohledem a odpovědností.

Balíček týkající se **policejní spolupráce**, který Komise předložila dne 8. prosince 2021<sup>35</sup> a který je v současné době projednáván, posílí spolupráci mezi úředníky donucovacích orgánů v členských státech tím, že zrychlí, zjednoduší a více zabezpečí výměnu údajů a dále posílí a zefektivní operativní policejní spolupráci na místě. Komise vyzývá Evropský parlament a Radu, aby tento balíček urychleně přijaly.

Jakmile budou tyto legislativní návrhy přijaty a provedeny, podpoří prosazování práva v rámci boje proti přeshraniční organizované trestné činnosti. To bude důležité zejména v situaci, kdy se zločinná společenství z Ukrajiny mohou pokusit z důvodu současné situace přesídlit a pokračovat ve svých aktivitách v EU.

**Poradní mise EU na Ukrajině** podporuje v zemi reformu donucovacích orgánů a orgánů právního státu od roku 2014. V březnu 2022 byl revidován mandát mise, který umožňuje poskytovat podporu na ukrajinských hraničních přechodech s Polskem, Rumunskem a Slovenskem, zvyšovat informovanost o přeshraniční trestné činnosti, včetně problematiky obchodování s lidmi, a o pohybu humanitárního zboží na Ukrajinu.

#### **IV. ZBRANĚ, NEBEZPEČNÉ MATERIÁLY A KRITICKÉ INCIDENTY**

Válka masivně zvýšila pohyb palných a jiných zbraní na samotné Ukrajině, což představuje nové riziko pro EU a další státy s Ukrajinou sousedící.

##### ***Ostražitost a koordinace***

<sup>34</sup> COM(2020) 796.

<sup>35</sup> COM(2021) 780, COM(2021) 782, COM(2021) 784.

Operační pokyny vydané v březnu poskytly členským státům doporučení, jak řešit problém zvýšeného pohybu palných zbraní v období hromadných příjezdů na vnější hranici EU<sup>36</sup>. Tyto pokyny zdůrazňují, že přítomnost palných zbraní by měla být nepřetržitě kontrolována a že nikomu bez povolení by neměl být povolen vstup do EU s palnou zbraní. Pokud ukrajinské orgány nahlásí, že některé z těchto palných zbraní chybí, měly by je členské státy nahlásit do Schengenského informačního systému.

Je velmi důležité, aby všechny zásilky palných zbraní na Ukrajinu byly řádně zaevidovány a obsahovaly všechny příslušné informace (včetně typu, země a roku výroby, značky, ráže, sériového čísla), aby bylo možné tyto palné zbraně na Ukrajině i v EU zpětně vysledovat.

EU veřejně odsoudila bezohledné vojenské útoky Ruska na civilní jaderná, biotechnologická a chemická zařízení na Ukrajině a v jejich bezprostřední blízkosti a také veškeré činy ohrožující bezpečnost těchto zařízení. Komise situaci na Ukrajině sleduje a věnuje zvláštní pozornost radiologické hrozbě, která je z hlediska vnitřní bezpečnosti EU nejzávažnější<sup>37</sup>. Komise rovněž sleduje potenciální chemické hrozby a zřídila vnitřní koordinační mechanismus pro případ potřeby rychlého posouzení rizik.

### ***Připravenost***

Ukrajina je již jednou ze zemí, které jsou v Akčním plánu EU proti nedovolenému obchodování s palnými zbraněmi na období 2020–2025 označeny za klíčové pro provedení konkrétních opatření na vnější úrovni. V souvislosti s palnými zbraněmi probíhá v oblasti, včetně Ukrajiny, v rámci platformy EMPACT také zvláštní operativní akce. Vzhledem k riziku zneužití palných zbraní však budou zapotřebí zvláštní projekty financované EU i operativní spolupráce s Europolem, agenturou Frontex a složkou EMPACT pro střelné zbraně. Komise brzy předloží návrh na revizi nařízení o palných zbraních<sup>38</sup> upravující vývoz, dovoz a tranzit střelných zbraní pro civilní použití jako součást celkového právního a operačního rámce pro předcházení, odhalování, vyšetřování a stíhání ve věci nedovoleného obchodování s palnými zbraněmi.

Za účelem zlepšení připravenosti EU a reakce na rizika pro veřejné zdraví, jako jsou chemické, biologické, radiologické a jaderné hrozby, vytváří Komise strategické rezervy v oblasti kapacit pro reakci prostřednictvím mechanismu civilní ochrany EU financovaného Úřadem pro připravenost a reakci na mimořádné situace v oblasti zdraví (HERA)<sup>39</sup>. Útvary Komise spolupracují na vytvoření strategických zásob v systému rescEU v hodnotě 540,5 milionu EUR. Tyto zásoby budou sestávat z vybavení a léků, vakcín a dalších léčivých přípravků k léčbě pacientů vystavených chemickým, biologickým, radiologickým a jaderným látkám jakož i z dekontaminačních rezerv rescEU za účelem poskytnutí dekontaminačního

---

<sup>36</sup> Sdělení Komise, kterým se stanoví operační pokyny pro správu vnějších hranic s cílem usnadnit překračování hranic mezi EU a Ukrajinou 2022/C 104 I/01.

<sup>37</sup> Komise ve spolupráci s americkými partnery uspořádá seminář zaměřený na rizika spojená s radiologickými materiály, které se nacházejí v nemocnicích a které se vymykají regulační kontrole.

<sup>38</sup> Nařízení Evropského parlamentu a Rady (EU) č. 258/2012 ze dne 14. března 2012, kterým se provádí článek 10 protokolu Organizace spojených národů proti nedovolené výrobě střelných zbraní a jejich součástí, dílů a střeliva a obchodování s nimi, který doplňuje Úmluvu Organizace spojených národů

proti nadnárodnímu organizovanému zločinu (Protokol OSN o střelných zbraních), a stanoví vývozní povolení a

opatření pro dovoz a tranzit střelných zbraní, jejich součástí, dílů a střeliva.

<sup>39</sup> [Pracovní plán HERA 2022 \(europa.eu\)](https://europa.eu/HERA2022)

vybavení a odborných zásahových týmů. V první řadě EU okamžitě uvolnila svou rezervu zdravotnických prostředků rescEU, aby zajistila tablety jodidu draselného, které lze použít k ochraně lidí před škodlivými účinky radiace, a další prostředky, které Ukrajina naléhavě potřebuje. S pomocí Francie a Španělska byly na Ukrajinu prostřednictvím mechanismu civilní ochrany Unie dodány již téměř 3 miliony jodových tablet.

## **V. KOORDINOVANÁ OPATŘENÍ S CÍLEM POHNAT RUSKO ZA JEHO AGRESI K ODPOVĚDNOSTI**

EU hraje rozhodující roli při uskutečňování aktivit mezinárodního společenství, jejichž cílem je vyvíjet tlak na Rusko, aby ukončilo svou agresi proti ukrajinskému státu a civilistům postiženým konfliktem, který je nepřijatelný a v rozporu s mezinárodním právem. Tento nátlak zahrnuje opatření, která naznačují důsledky pro pachatele, včetně přísných sankcí, a opatření k identifikaci a usnadnění stíhání válečných zločinů.

### *Omezující opatření a konfiskace*

Od ruského uznání vládou nekontrolovaných území Doněcké a Luhanské oblasti na Ukrajině dne 21. února 2022 a od invaze na Ukrajinu dne 24. února 2022 zavedla EU vůči Rusku dosud největší sérii omezujících opatření. Dosud bylo přijato pět balíčků sankcí. Tato opatření se zaměřují na klíčová odvětví, včetně finančnictví, obchodu, dopravy, obrany a médií, a jsou zaměřena na politické a vojenské elity a významné ruské a běloruské oligarchy. Na seznamu je již více než 1 000 fyzických osob a 80 subjektů. Rada projednává šestý balíček sankcí.

Dopad těchto a předchozích omezujících opatření vůči ruským a běloruským osobám a společnostem bude tak silný, jak důrazné bude jejich vynucování. Koordinace na úrovni EU může významně přispět k odstranění potenciálních mezer a Komise zúčastněným stranám poskytuje rozsáhlou podporu formou písemných pokynů, pořádání setkání zúčastněných stran a příslušných skupin odborníků a řady zdrojů pro usnadnění dodržování předpisů.

Kromě toho Komise zřídila pracovní skupinu „Freeze and Seize“ ke zmrazování a konfiskaci majetku, která sdružuje útvary Komise, členské státy a agentury Eurojust a Europol. Členské státy dosud oznámily zmrazení aktiv v hodnotě 9,89 miliardy EUR<sup>40</sup>. Dne 11. dubna zahájil Europol společně s členskými státy, Eurojustem a agenturou Frontex operaci s názvem Oscar na podporu vyšetřování v oblasti financí a trestné činnosti, které se zaměřuje na majetek pocházející z trestné činnosti vlastněný fyzickými a právníckými osobami, na něž se vztahují sankce EU v souvislosti s válkou Ruska proti Ukrajině. Pracovní skupina EU „Freeze and Seize“ úzce spolupracuje s pracovní skupinou zaměřenou na ruské elity, prostředníky a oligarchy (REPO), kterou vytvořily země G7 (Kanada, Francie, Německo, Itálie, Japonsko, Spojené království a Spojené státy) a podobně smýšlející partneři, jako je Austrálie, a také americká pracovní skupina KleptoCapture a ukrajinská pracovní skupina.

Pracovní skupina „Freeze and Seize“ slouží jako platforma pro koordinaci a usnadňování výměny informací a zkušeností mezi členskými státy a jejím úkolem je poskytovat pokyny k uplatňování sankcí a usnadňovat výměnu osvědčených postupů v oblasti vyšetřování trestných činů a konfiskace. Důležité je zejména to, aby donucovací orgány byly ve vztahu k potenciálním trestným činům sankcionovaných osob a subjektů ostražitě a aktivní. Cílem

---

<sup>40</sup> Je zde také částka zablokovaných aktiv Ruské centrální banky ve výši přibližně 23 miliard EUR.

pracovní skupiny je rovněž zahájit diskusi na téma možného využití zabavených finančních prostředků, například jako příspěvek na obnovu Ukrajiny.

Komise dnes přijímá balíček týkající se **vyhledávání a konfiskace majetku**<sup>41</sup>, který zohledňuje zkušenosti získané při provádění omezujících opatření Unie vůči ruským a běloruským osobám a subjektům. Usnadní účinné provádění omezujících opatření Unie v celé Unii tím, že umožní rychlé dohledání a identifikaci majetku, který vlastní nebo ovládají osoby nebo subjekty, na něž se tato opatření vztahují. Posílený rámec pro vyhledávání a konfiskaci majetku se bude vztahovat i na porušení omezujících opatření, a zajistí tak účinné vysledování, zmrazení, správu a konfiskaci výnosů plynoucích z porušení omezujících opatření. Aby bylo zajištěno, že majetek fyzických a právnických osob, které porušují omezující opatření, může být skutečně zabaven, přijímá dnes Komise rovněž návrhy rozhodnutí Rady o doplnění položky porušení sankcí na seznam trestných činů EU v čl. 83 odst. 1 SFEU<sup>42</sup>, k nimž je připojeno sdělení<sup>43</sup>, s cílem navrhnout směrnici, která by sblížila definici trestných činů a sankcí za porušení omezujících opatření.

V obecnější rovině představuje tento balíček zásadní krok v boji proti organizované trestné činnosti. Navazuje na závazky Komise obsažené ve strategii bezpečnostní unie a ve strategii EU pro boj proti organizované trestné činnosti (2020–2025)<sup>44</sup>. Reviduje směrnici o konfiskacích z roku 2014, rozhodnutí Rady o úřadech pro vyhledávání majetku z trestné činnosti z roku 2007 a rámcové rozhodnutí Rady o konfiskaci výnosů a majetku z trestné činnosti a nástrojů trestné činnosti z roku 2005 s cílem posílit kapacity v oblasti vysledování a identifikace a v neposlední řadě i konfiskace nezákonných příjmů a řešit tak velmi nízkou míru konfiskací v EU<sup>45</sup>. Balíček rozšiřuje okruh trestných činů, na které se vztahuje, a dále pravidla pro konfiskaci v případech, kdy nelze vynést odsuzující rozsudek za konkrétní trestný čin, ale kdy majetek jednoznačně pochází z trestné činnosti. Revize rovněž posiluje účinnou správu zmrazeného a zkonfiskovaného majetku a schopnosti úřadů pro vyhledávání majetku z trestné činnosti vysledovat a identifikovat nezákonný majetek. Nový rámec EU pro vymáhání majetku je navržen tak, aby řešil složitý způsob fungování zločinných společen, která často působí přeshraničně a používají různé metody k ukrytí svého majetku, včetně kryptoaktiv.

### *Koordinovaná reakce soudů*

Na úrovni EU se rovněž pracuje na zajištění koordinované soudní reakce na **mezinárodní zločiny**, údajně spáchané na Ukrajině, aby jejich pachatelé mohli být dohnáni k odpovědnosti.

Dva členské státy a Ukrajina zřídily společný vyšetřovací tým (SVT), který má vyšetřovat válečné zločiny, zločiny proti lidskosti a další mezinárodní zločiny, které měly být údajně spáchány na ukrajinském území. Agentura Eurojust poskytuje tomuto SVT právní,

---

<sup>41</sup> COM(2022) 245.

<sup>42</sup> COM(2022) 247.

<sup>43</sup> COM(2022) 249.

<sup>44</sup> COM(2021) 170.

<sup>45</sup> Europol odhaduje, že pouze 2 % majetku pocházejícího z trestné činnosti jsou zmrazena (2,4 miliardy EUR) a 1 % zkonfiskováno (1,2 miliardy EUR), zatímco příjmy z trestné činnosti na hlavních kriminálních trzích v EU v roce 2019 činily 139 miliard EUR (1 % z celkového objemu HDP EU).

analytickou, finanční a logistickou podporu. Dne 25. dubna 2022 se k SVT jako účastník<sup>46</sup> připojil Úřad žalobce Mezinárodního trestního soudu a očekává se, že se brzy připojí ještě další účastníci.

Dne 25. dubna 2022 předložila Komise návrh na změnu nařízení o Eurojustu<sup>47</sup>, aby mohl Eurojust uchovávat, analyzovat a ukládat důkazy o hlavních mezinárodních zločinech. Eurojust a Europol budou během tohoto procesu i nadále úzce spolupracovat. Klíčovou roli při koordinaci reakce soudů hraje také Síť pro vyšetřování genocidy, jejíž sekretariát je zřízen při Eurojustu, která připravila atlas nevládních organizací působících v současné době na Ukrajině a která podporuje vnitrostátní odborníky z členských států a Ukrajiny, kteří řeší aktivní případy související s válkou.

V dubnu 2022 Rada dále revidovala mandát **poradní mise EU na Ukrajině**, čímž připravila půdu pro podporu mise ukrajinským orgánům při vyšetřování a stíhání všech mezinárodních zločinů spáchaných v souvislosti s ruskou vojenskou agresí. Mise bude ukrajinským orgánům poskytovat strategické poradenství v oblasti vyšetřování a stíhání mezinárodních zločinů, nezbytných změn ukrajinských právních předpisů a také komunikační strategii a školení v souvisejících otázkách. Mise se v této souvislosti podílí na řadě iniciativ týkajících se koordinace a společně s delegací EU je součástí poradní skupiny USA–EU pro kruté zločiny páchané na Ukrajině.

## VI. ZAHRANIČNÍ MANIPULACE S INFORMACEMI A VMĚŠOVÁNÍ

Současný geopolitický vývoj zdůraznil rizika zahraničního vměšování. Vojenskou agresí Ruska proti Ukrajině doprovází aktivity spojené s **manipulací s informacemi a vměšováním**. K ospravedlnění brutálních útoků na Ukrajinu byla použita nepodložená obvinění ukrajinské vlády z „nacismu“ a „genocidy“ a z operací pod falešnou vlajkou a dále neopodstatněná obvinění vznesená proti NATO a Západu, zatímco svoboda slova a nezávislé zpravodajství v Rusku byly potlačeny. Nadále hrozí riziko v podobě zmanipulovaných audiovizuálních materiálů a dezinformací, kterých se Rusko může pokusit využít jako záminku pro další vojenské útoky, aby oslabilo odhodlání ukrajinského odboje, rozdělilo mezinárodní společenství v jeho odporu proti válce, nebo zaseló pochybnosti o porušování mezinárodního práva ze strany Ruska. EU se ve Strategickém kompasu zavázala, že bude důrazně reagovat na zahraniční manipulaci s informacemi a vměšováním a posílí svou odolnost a schopnost těmto hrozbám čelit<sup>48</sup>. Manipulace s demokratickou diskusí v EU je předmětem Akčního plánu pro evropskou demokracii, koordinovaného plánu Komise na řešení dezinformací a posílení odolnosti demokracie<sup>49</sup>.

### *Ostražitost a koordinace*

Evropská unie zareagovala na dezinformační kampaň Ruska v souvislosti s vojenskou agresí proti Ukrajině rozhodnými a koordinovanými kroky. EU úzce spolupracuje se svými členskými státy prostřednictvím systému včasného varování a dále s mezinárodními partnery, jako je NATO, USA, Kanada, a mechanismem rychlé reakce G7, aby si vyměňovala postřehy ohledně trendů manipulativních technik a taktik používaných Kremlem. Práce na rozkrytí

<sup>46</sup> <https://www.eurojust.europa.eu/eurojust-and-the-war-in-ukraine>

<sup>47</sup> COM(2022) 187 final.

<sup>48</sup> <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/cs/pdf>

<sup>49</sup> COM(2020) 790.

kremelských manipulací se zintenzivnila, zejména prostřednictvím webových stránek EUvsDisinfo, které vysílají v angličtině, ruštině, ukrajinštině a dalších jazycích a jejichž cílem je poskytovat faktické informace v rámci EU, na Ukrajině a v regionu a stejně tak v Rusku. Od 2. března byly v důsledku omezujících opatření přijatých EU pozastaveny přenos a vysílání kanálů spjatých s ruskými státními médii RT a Sputnik v EU a kanálů zaměřených proti EU. Signatáři kodexu zásad boje proti dezinformacím<sup>50</sup> z řad online platforem, předních sociálních sítí, inzerentů a reklamního průmyslu přijímají naléhavá opatření k omezení dezinformací souvisejících s ruskou agresí na Ukrajině. Komise a ESVČ toto úsilí sledují. Z poskytnutých informací vyplývá, že platformy posílily své monitorovací a intervenční nástroje vztahující se k válce.

Kromě toho se rychle zavádějí opatření na podporu zemí ve střední Asii a na západním Balkáně s cílem posílit odolnost informací a čelit zahraniční manipulaci s informacemi a dezinformacím.

### ***Přípravenost***

Zjevné používání technik zahraničního vměšování a manipulace s informacemi včetně šíření dezinformací, jako jednoho z nástrojů hybridních hrozeb, činí návazná opatření v rámci Evropského akčního plánu pro demokracii mimořádně naléhavými. V posledních měsících orgány EU podporovaly členské státy v boji proti zahraničnímu vměšování a manipulaci s informacemi, zejména v rámci systému rychlého varování, a to sdílením poznatků ohledně taktik používaných aktéry podílejícími se na zahraničním vměšování a manipulaci s informacemi a strategií reakce na ně. Na základě koncepční poznámky předložené ESVČ o vytvoření specializovaného **souboru nástrojů** pro řešení této hrozby probíhají diskuse o dalším posílení celkové reakce EU na činnosti týkající se zahraničního vměšování a manipulace s informacemi. Tím se propojují stávající vnitřní opatření a nové nástroje EU v rámci společné zahraniční a bezpečnostní politiky. Bude se těžit také z intenzivnější činnosti Evropské služby pro vnější činnost Stratcom<sup>51</sup> a rovněž z činnosti Komise.

Evropské středisko pro sledování digitálních médií (EDMO) zřídilo po vypuknutí války na Ukrajině pracovní skupinu pro dezinformace a koordinuje činnost ověřovatelů faktů a výzkumných pracovníků ve své síti. Provedlo analýzu toho, jak se zastánci konspiračních teorií COVID-19 rychle přeorientovali na šíření falešných zpráv na podporu ruské strany, přičemž tato změna kurzu byla zaznamenána v řadě členských států<sup>52</sup>.

Návrh aktu o digitálních službách se snaží přizpůsobit rychle se rozvíjejícím digitálním technologiím a jevům, které tento rozvoj přináší v rámci technologických a demokratických výzev, jako jsou například nenávistné projevy, dezinformace na internetu a destabilizační strategie. Významný pokrok v jednáních Evropského parlamentu a Rady by měl umožnit rychlé přijetí balíčku.

---

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

<sup>51</sup> Oddělení strategické komunikace, pracovních skupin a informační analýzy Evropské služby pro vnější činnost poskytuje strategickou komunikační podporu při provádění zahraniční a bezpečnostní politiky EU v příslušných prioritních oblastech (země jižního a východního sousedství, západního Balkánu) tím, že vyvíjí a provádí konkrétní strategické činnosti v oblasti komunikace zaměřené na prosazování politik, hodnot, cílů a zájmů EU.

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

## VII. ŠIRŠÍ PŘIPRAVENOST

V době, kdy se do Evropy vrátila válka a kdy dochází k významným geopolitickým změnám, se koordinace bezpečnosti v EU posunula na vyšší úroveň a navázala na iniciativy, které byly připravovány již před ruskou útočnou válkou proti Ukrajině. Iniciativy zaměřené především na vnější bezpečnost EU mají silný dopad na vnitřní agendu bezpečnostní unie.

Dne 15. února 2022 předložila Komise **obrný balíček**<sup>53</sup>, který obsahuje řadu iniciativ v oblastech, jež jsou pro obranu a bezpečnost v EU zásadní. Tento příspěvek Komise k evropské obraně a bezpečnosti pokrývá celou škálu výzev. Navrhuje konkrétní kroky k vytvoření integrovanějšího a konkurenceschopnějšího evropského obranného trhu, zejména prostřednictvím posílení spolupráce v rámci EU a vytváření úspor z rozsahu. Obsahuje také plán pro kritické technologie v oblasti bezpečnosti a obrany, který má podpořit výzkum, technologický rozvoj a inovace v těchto odvětvích a snížit závislost na kritických technologiích a hodnotových řetězcích. Cílem balíčku je na úrovni EU rovněž posílit aspekt obrany týkající se vesmíru. Dále se zabývá tím, jak by Komise mohla zintenzivnit svá opatření proti hybridním hrozbám, včetně oblasti kybernetiky, posílit vojenskou mobilitu v rámci Evropy i mimo ni a dále řešit výzvy související se změnou klimatu v oblasti obrany. Jako doplnění k této práci bylo vydáno společné sdělení „**Analýza nedostatečné míry investic do obrany a další postup**“<sup>54</sup> ze dne 18. května, které se zabývá nedostatky týkající se schopností a průmyslu, jež je třeba řešit s cílem podpořit nejvíce ohrožené členské státy EU a určit opatření ke zmírnění zjištěných nedostatků.

Odolnost EU vůči těmto hrozbám zahrnuje rovněž přístupy založené na schopnostech napříč bezpečnostními odvětvími, jak je doporučeno v akčním plánu Komise pro synergie mezi civilním, obranným a kosmickým průmyslem<sup>55</sup>. V oblasti vnitřní bezpečnosti a prosazování práva se pracuje na podpoře přístupů založených na schopnostech.

Dne 21. března 2022 přijala Rada **Strategický kompas pro bezpečnost a obranu**<sup>56</sup>, který krátce nato schválila Evropská rada. Kompas nastiňuje ambiciózní akční plán na posílení bezpečnostní a obranné politiky EU do roku 2030. Cílem je učinit z EU silnějšího a schopnějšího zajišťovatele bezpečnosti, který chrání své občany a přispívá k mezinárodnímu míru a bezpečnosti. Obsahuje konkrétní návrhy s velmi přesným harmonogramem provádění, které mají zlepšit schopnost EU jednat v krizových situacích rázně.

Jedním z výsledků Strategického kompasu je vytvoření **souboru hybridních nástrojů EU**, který by měl poskytnout rámec pro koordinovanou reakci na hybridní kampaně, které se dotýkají EU a jejích členských států, včetně opatření na vnitřní i vnější úrovni. V návaznosti na identifikaci základních hodnot odvětvové odolnosti provedenou na začátku roku 2022<sup>57</sup> bude dokončena analýza nedostatků a potřeb. V tomto rámci bude EU i nadále budovat připravenost, odolnost a schopnost reagovat na hrozby plynoucí z ruské agrese a dalších pokusů o destabilizaci demokracií a mnohostranného uspořádání založeného na pravidlech.

<sup>53</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence\\_cs](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_cs)

<sup>54</sup> JOIN(2022) 24.

<sup>55</sup> COM(2021) 70.

<sup>56</sup> Strategický kompas pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/cs/pdf>

<sup>57</sup> SWD(2022) 21 final.

## VIII. VÝHLED DO BUDOUCNA

Do budoucna bude EU muset zůstat mimořádně ostražitá vůči vyvíjejícím se hrozbám a budovat **přípravenost a odolnost vůči všem možným situacím**. Následky války mohou mít různé podoby, z nichž ne všechny lze zatím posoudit.

Rozsah přesunu ukrajinských zločineckých sítí ještě není znám. Případy, které Eurojust řešil v minulosti, ukazují na trend pašování heroinu z Afghánistánu do EU přes Ukrajinu, což potvrdilo i Evropské monitorovací centrum pro drogy a drogovou závislost (EMCDDA)<sup>58</sup>. Vlivem nestability se boj proti obchodu s heroinem na této trase může stát obtížnějším, což s sebou přináší riziko možného zvýšení toku drog do EU.

Některá rizika pro EU se pravděpodobněji zvýší na konci nebo během případných přestávek v bojích. Zvláštní pozornost bude věnována oběhu palných zbraní, přičemž riziko v této souvislosti stoupne, jakmile boje na Ukrajině ustanou. Zkušenosti z minulosti rovněž poukazují na riziko, že návrat zahraničních bojovníků, kteří získali bojové zkušenosti a kteří mohli přijít do kontaktu s extremistickými skupinami, může později nasměrovat teroristické akce do EU. Tento možný jev by měl být pečlivě sledován, přičemž Komise již zprostředkovává diskuse mezi členskými státy o výzvách, které přináší návrat zahraničních dobrovolníků s násilnou extremistickou minulostí.

Vzhledem k těmto možným hrozbám je důležité, aby se pokračovalo v provádění strategie bezpečnostní unie, včetně provádění klíčových strategií, jako je strategie kybernetické bezpečnosti, strategie EU pro boj proti organizované trestné činnosti (2020–2025), protiteroristická agenda pro EU (2020–2025), akční plán EU proti nedovolenému obchodování s palnými zbraněmi (2020–2025), strategie EU pro boj proti obchodování s lidmi (2021–2025) a protidrogová strategie EU (2021–2025).

Úsilí o vytvoření potřebného legislativního rámce EU bude pokračovat. Komise připravuje například posouzení dopadu návrhu upravujícího uvádění na trh a používání vysoce rizikových chemických látek.

## IX. ZÁVĚR

Bezpečnostní unie nadále plní svou úlohu při přípravě EU a jejích členských států na řešení stávajících a potenciálních hrozeb. Vojenská agrese Ruska vůči Ukrajině ukázala, jak rychle se teoretické hrozby mohou proměnit ve skutečnost, a zdůrazňuje význam ostražitosti, koordinace a připravenosti.

Tato čtvrtá zpráva o pokroku v oblasti strategie bezpečnostní unie ukazuje, že EU je schopna se přizpůsobit, a to i tváří v tvář výjimečným a neočekávaným hrozbám, jako je ruská útočná válka proti Ukrajině. Rozhodné provádění strategie bezpečnostní unie je nyní důležitější než kdykoli předtím.

<sup>58</sup> Zpráva o situaci související s drogami a alkoholem na Ukrajině za rok 2020 (podle údajů za rok 2019), OEDT, Zastavení obchodování s náhražkou heroinu ve Francii, Polsku a na Ukrajině, včetně plánování a provádění sledování zásilek, 2021/00446, Eurojust, květen 2020.