Monika Hullová

Iniciatíva a opatrenia prijaté zo strany EÚ na účely zabránenia šíreniu a negatívnym dôsledkom hybridných hrozieb

Anotácia: Autorka v prehľadovej vedeckej štúdii analyzuje kroky, ktoré boli podniknuté zo strany EÚ na úseku zabránenia šíreniu a negatívnym dôsledkom hybridných hrozieb od roku 2010 po súčasnosť, resp. aj v kontexte budúcich trendov a vízií. Hybridné hrozby ako nový spôsob pôsobenia určitých subjektov sa stali problémom, ktorému musia čeliť všetky štáty sveta. Aj z toho dôvodu boli podniknuté viaceré kroky na medzinárodnej a národnej úrovni, ktorých cieľom je vytvoriť optimálny legislatívno-inštitucionálny rámec na elimináciu tohto nežiadúceho bezpečnostného javu. Cieľom autorky bolo na základe širokého spektra analytických metód posúdiť postupnosť a koherenciu týchto krokov v kontexte identifikovaných potrieb spoločenskej praxe.

Kľúčové slová: hybridná hrozba, stratégia, bezpečnostná stratégia, obranná stratégia, akčný plán, kybernetická bezpečnosť, bezpečnostné prostredie, bezpečnostný systém, riadenie rizík, krízová situácia, dezinformácia, EUROPOL, FRONTEX, EUROJUST, CEPOL, East StratCom, Európska služba pre vonkajšiu činnosť, Spravodajské a situačné centrum EÚ, Spravodajské analytické centrum EÚ, Európske centrum výnimočnosti na boj proti hybridným hrozbám

Úvod

Z prieskumu Eurobarometra realizovaného v marci 2023 na tému *„Digitálna dekáda“ (Špeciálny Eurobarometer 532)* vyplýva, že medzi tri základné priority, ktorým by sa členské štáty mali do roku 2030 venovať, patrí okrem zlepšenia dostupnosti rýchleho internetového pripojenia *(27 % respondentov)* predovšetkým *„úloha chrániť používateľov digitálnych technológií pred kybernetickými útokmi (30 % respondentov) a chrániť ich pred dezinformáciami a ilegálnym obsahom na internete (26 % respondentov)“*, pričom až takmer 80 % opýtaných Európanov zdôrazňuje, že digitálne technológie zohrávajú a aj v najbližšej dekáde budú, v ich každodennom živote zohrávať dôležitú úlohu.[1]

Na základe poslednej publikovanej *(šiestej)* správy Európskej komisie *(ďalej len „Komisia“)* zo septembra 2022 o pokroku pri vykonávaní spoločného rámca pre boj proti hybridným hrozbám *(2016)* a spoločného oznámenia o zvyšovaní odolnosti a posilňovaní spôsobilosti riešiť hybridné hrozby *(2018)* možno konštatovať, že *„sledované obdobie bolo poznačené bezprecedentnými zmenami a výzvami v oblasti hybridných hrozieb, predovšetkým v kontexte globálnych dopadov ruskej agresie namierenej voči Ukrajine. Zároveň pokračovala pandémia COVID-19 a s ňou boli spojené aj dezinformácie, ktoré mali veľký vplyv na verejnú mienku. Okrem toho EÚ čelila novým pokusom o podkopanie svojej jednoty inštrumentalizáciou migračných tokov. Vzhľadom na zložitosť a mnohotvárnosť týchto výziev, rámec na boj proti hybridným hrozbám, ale aj nadnárodné a celospoločenské prístupy, ktoré sú súčasťou politík, sa stali ešte dôležitejšími.“*[2]

Aj tieto skutočnosti opodstatnene vyvolávajú potrebu ich hlbšieho vedeckého skúmania a stali sa aj pre nás v určitom zmysle výzvou, ktorá plne inhibuje náš záujem a stala sa reálnym objektom a predmetom našej výskumnej činnosti.[3]

Na túto realitu sme sa rozhodli reagovať tak, že realizujeme účelové vedecké skúmanie založené na objektivizujúcich postupoch. Naším cieľom v predkladanej prehľadovej

---

[1] Prieskumu sa zúčastnilo 26 376 respondentov z 27 krajín EÚ. In: *EURÓPSKA KOMISIA, 2023. Special Eurobarometer 532: The Digital Decade*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://webgate.ec.europa.eu/ebsm/api/public/deliverable/download?doc=true&deliverableId=87743.

[2] Ú. v. EÚ SWD(2022) 308 final, 16. 9. 2022.

[3] *Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy* [online] : Projekt podporený z Európskeho sociálneho fondu. Operačný program Efektívna verejná správa. Prijímateľ MV SR. Kód projektu ITMS2014+: 314011CDW7.

vedeckej štúdii je komplexná analýza vynaloženej iniciatívy a opatrení prijatých zo strany EÚ na účely zabránenia vzniku a šírenia hybridných hrozieb. Zjednodušene povedané, touto analytickou činnosťou sme sa rozhodli poskytnúť deskripciu fakticky realizovaných činností a výsledky dosiahnuté ich realizáciou. Pri napĺňaní tejto ambície sme dominantne využili metódy obsahovej analýzy, historickej *(retrospektívnej)* analýzy, kauzálnej analýzy a tzv. problémovej analýzy.

1 Analýza dokumentov reglementujúcich problematiku boja proti hybridným hrozbám v podmienkach EÚ

V novembri 2010 Komisia prijala **Stratégiu vnútornej bezpečnosti EÚ: päť krokov k bezpečnejšej Európe**, ktorá určuje päť strategických cieľov vnútornej bezpečnosti EÚ. Prioritným cieľom je rozloženie medzinárodných zločineckých sietí, a to prostredníctvom vytvorenia legislatívneho rámca EÚ týkajúceho sa zhromažďovania osobných údajov o cestujúcich v leteckej doprave, ktorí vstupujú na územie EÚ alebo ho opúšťajú, a právnych predpisov EÚ v oblasti boja proti praniu špinavých peňazí. Okrem toho Komisia zdôrazňuje potrebu častejšieho využívania spoločných vyšetrovacích tímov, zriaďovaných *ad hoc* a zložených zo zástupcov polície, colných orgánov, pohraničnej stráže a justičných orgánov v rôznych členských štátoch v spolupráci s EUROJUSTOM *(angl. EU Agency for Criminal Justice Cooperation – Agentúra EÚ pre justičnú spoluprácu v trestných veciach)*, EUROPOLOM *(angl. EU Agency for Law Enforcement Cooperation – agentúra EÚ na presadzovanie práva, tzv. Európsky policajný úrad)* a úradom OLAF *(angl. The European anti-fraud office – Európsky úrad pre boj proti podvodom)*. Ďalším potrebným krokom je vytvorenie legislatívneho rámca EÚ týkajúceho sa ochrany hospodárstva pred prenikaním zločineckých sietí *(boj proti korupcii; regulácia udeľovania licencií, povolení, zákaziek a dotácií; účinné presadzovanie práva duševného vlastníctva)* a konfiškácie majetku pochádzajúceho z trestnej činnosti. Druhým cieľom je zabraňovanie terorizmu, radikalizácii a náboru iných členov, a to prostredníctvom špecifických opatrení *(vytvorenie siete EÚ zameranej na zvyšovanie povedomia o radikalizácii; vytvorenie európskej siete špeciálnych jednotiek presadzovania práva v oblasti výbušnín a chemického, biologického, rádiologického a jadrového materiálu – označovaného aj ako materiálu CBRN; spracovanie stratégie EÚ v oblasti získavania a analýzy údajov zo správ o finančných transakciách zaregistrovaných na jej území; zaistenie bezpečnosti dopravy)*. Tretím cieľom je zvýšiť úroveň bezpečnosti občanov a podnikateľskej verejnosti v kybernetickom priestore. V tejto súvislosti sa EÚ zaviazala v rámci existujúcich štruktúr vytvoriť stredisko EÚ pre počítačovú kriminalitu,[4] ktoré v spolupráci s Európskou agentúrou pre bezpečnosť sietí a informácií resp. Agentúrou EÚ pre kybernetickú bezpečnosť *(angl. The European Network and Information Security Agency – ENISA)*, ako aj so sieťou národných/vládnych tímov reakcie na núdzové počítačové situácie *(angl. The Computer Emergency Response Team – CERT)*, budú ústredným článkom boja proti počítačovej kriminalite v Európe. Okrem toho sa Komisia zaviazala do roku 2013 vytvoriť Európsky systém zdieľania informácií a varovania *(angl. The European Information Sharing and Alerting System – EISAS)*, ako aj sieť kontaktných bodov medzi príslušnými orgánmi a členskými štátmi. Štvrtý cieľ sleduje zvýšenie bezpečnosti prostredníctvom

[4] Európske centrum boja proti počítačovej kriminalite *(angl. European Cybercrime Centre – EC3)* vzniklo v roku 2013 pod hlavičkou úradu EUROPOL a sídli v Holandsku, kde zohráva zásadnú úlohu pri zneškodňovaní operácií zločineckých skupín, ktoré sa dopúšťajú počítačovej kriminality. Právny rámec vzniku predstavuje oznámenie Komisie Rade a Európskemu parlamentu (Ú. v. EÚ COM(2012) 140 final, 28. 3. 2012).
In: *EUROPA.EU, 2014*. *Európske centrum boja proti počítačovej kriminalite na úrade EUROPOL*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://publications.europa.eu/resource/cellar/6d16d2d0-7561-4492-beef-048e64bed66a.0022.02/DOC_1.

riadenia hraníc. Dosiahnutie tohto cieľa je podľa Komisie možné na základe revízie colného kódexu spoločenstva, ako aj na základe spolupráce s Európskou agentúrou pre pohraničnú a pobrežnú stráž *(angl. The European Border and Coast Guard Agency – FRONTEX)* a s EUROPOLOM, a to tak na taktickej, ako aj na operačnej a strategickej úrovni *(vypracovaním spoločnej analýzy rizika trestnej činnosti na vonkajších hraniciach)*. Ďalším dôležitým krokom je zriadenie systému EUROSUR *(angl. The European Border Surveillance System – európsky systém kontroly hraníc, tzv. mechanizmus na výmenu operačných informácií v oblasti hraničného dozoru)*. Posledným cieľom, ktorý si EÚ vytýčila, je zvýšenie odolnosti Európy voči krízam a katastrofám, ktorý zahŕňal viacero opatrení. V prvom rade bolo potrebné zaviesť doložku o solidarite ustanovenú Lisabonskou zmluvou do praxe *(článok 222 zmluvy o fungovaní EÚ)*. Okrem toho sa Komisia zaviazala vypracovať usmernenia EÚ pre posudzovanie a mapovanie rizík, ktoré sa budú využívať pre potreby zvládania katastrof. Pokiaľ ide o posudzovanie hrozieb, členské štáty boli vyzvané, aby do roku 2012 vypracovali vlastné metódy posudzovania hrozieb terorizmu a iných zákerných hrozieb a od roku 2013 spoločne s Komisiou a koordinátorom EÚ pre boj proti terorizmu[5] pripravovali pravidelný prehľad aktuálnych hrozieb. Počas krízových situácií by sa mal aj naďalej využívať a rozvíjať systém rýchleho varovania ARGUS, ktorý bol vytvorený v roku 2005 a spája všetky špecializované systémy pre mimoriadne situácie. Súčasťou existujúceho systému krízového riadenia je zriadenie tzv. ústredného krízového centra, ktoré počas mimoriadnej situácie spája zástupcov všetkých relevantných útvarov Komisie.[6][7]

Z prezentovaného poznania je zrejmé, že hrozby, ktorým EÚ čelila na začiatku 21. storočia, mali jasne vymedzené kontúry, hoci s explicitným formulovaním potreby reagovať na hrozby s prívlastkom *„hybridné“* sme sa v euro priestore na oficiálnej úrovni prvýkrát stretli až v roku 2014 *(išlo napr. o politické usmernenia predsedu Komisie Jean-Claude Junckera z roku 2014, Závery Rady o spoločnej bezpečnostnej a obrannej politike z mája 2015, Závery Európskej rady z júna 2015)*.[8]

V nadväznosti na túto skutočnosť Komisia v apríli 2015 prijala **Európsky program v oblasti bezpečnosti**, ktorý predstavoval inovovanú stratégiu vnútornej bezpečnosti EÚ na obdobie najbližších piatich rokov reflektujúc pritom fakt, že hrozby, s ktorými bola moderná Európa konfrontovaná, *„... sú čoraz rozmanitejšie, dostávajú stále viac medzinárodný rozmer a zároveň majú čoraz viac cezhraničný a medziodvetvový charakter“*. Práve z tohto dôvodu sa Komisia rozhodla poukázať na potrebu lepšej spolupráce v oblasti bezpečnosti, ktorú je možné podporiť zriadením tzv. poradného fóra EÚ pre bezpečnosť *(2015)*, ktoré bude spájať členské štáty, Európsky parlament, agentúry EÚ v oblasti spravodlivosti a vnútorných vecí, napr. EUROPOL, FRONTEX, EUROJUST, CEPOL *(angl. EU Agency for Law Enforcement Training – Agentúra EÚ pre odbornú prípravu v oblasti presadzovania práva resp. agentúru Európskej policajnej akadémie)*, eu-LISA *(angl. EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice – Európska agentúra na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti)*, EMCDDA *(angl. European Monitoring Centre for Drugs and Drug Addiction – Európske monitorovacie centrum pre drogy a drogovú závislosť)*, ako aj zástupcov občianskej spoločnosti, akademickej obce a súkromného sektora. Súčasťou tejto stratégie je aj posilnenie spolupráce s medzinárodnými organizáciami, ako sú

[5] Po teroristických útokoch v Madride 11. marca 2004 lídri EÚ prijali **vyhlásenie o boji proti terorizmu**. Okrem iných opatrení sa dohodli na zriadení postu koordinátora EÚ pre boj proti terorizmu.
In: *EURÓPSKA RADA, 2021. Koordinátor pre boj proti terorizmu*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/fight-against-terrorism/counter-terrorism-coordinator/.
[6] Ú. v. EÚ KOM(2005) 662 v konečnom znení, 23. 12. 2005.
[7] Ú. v. EÚ KOM(2010) 673 v konečnom znení, 22. 11. 2010.
[8] Ú. v. EÚ Consilium 8971/15, 18. 5. 2015) a (Ú. v. EÚ EUCO 22/15, 26. 6. 20115.

OSN, Rada Európy, INTERPOL *(The International Criminal Police Organization – Medzinárodná organizácia kriminálnej polície)* a v neposlednom rade aktívnejšie využívanie mnohostranného fóra, akým je napr. Globálne fórum pre boj proti terorizmu *(angl. Global Counterterrorism forum – GCTF).*[9] Na účel posilnenia pilierov EÚ je potrebné vytvorenie nových alebo rozvinutejších nástrojov, ktoré umožnia efektívnejšiu výmenu informácií, operačnú spoluprácu a inú podporu.

Na tomto úseku pri zaisťovaní bezpečnosti na vonkajších hraniciach EÚ zohráva dôležitú úlohu hlavne Schengenský informačný systém *(angl. The Schengen Information System – SIS)* spolu s databázou INTERPOL-u s informáciami o odcudzených a stratených cestovných dokladoch *(angl. Stolen and Lost Travel Documents – SLTD).* K ďalším nástrojom efektívnej výmeny informácií medzi vnútroštátnymi orgánmi presadzovania práva možno zaradiť:

- ✓ vytvorenie súboru spoločných ukazovateľov rizika, pokiaľ ide o zahraničných teroristických bojovníkov;
- ✓ informačný systém pre boj proti podvodom *(angl. The EU anti-fraud information system – AFIS)*;
- ✓ nástroje Prümského rámca;[10]
- ✓ sieťovú aplikáciu EUROPOL-u na zabezpečenú výmenu informácií *(angl. The Secure Information Exchange Network Application – SIENA)*;
- ✓ zriadenie systému EÚ pre osobné záznamy o cestujúcich *(angl. Passenger Name Record – PNR),* v ktorom sa zaznamenajú údaje o cestujúcich v leteckej doprave;
- ✓ Európsky informačný systém registrov trestov *(angl. The European Criminal Records Information System – ECRIS)*, ktorý umožňuje výmenu informácií o predchádzajúcich odsúdeniach občanov EÚ;
- ✓ Európsky systém policajných záznamov *(angl. The European Police Records Index System – EPRIS)* pre uľahčenie cezhraničného prístupu k informáciám uchovávaným vo vnútroštátnych policajných záznamoch;
- ✓ vytvorenie spoločného prostredia na zdieľanie informácií pre námornú oblasť *(angl. the common information sharing environment – CISE).*[11]

---

[9] EÚ bola jedným z 30-tich jeho zakladajúcich členov. Globálne fórum pre boj proti terorizmu (2011) slúži ako mnohostranné fórum na posilnenie medzinárodnej spolupráce pri boji proti terorizmu, v ktorom zúčastnení členovia diskutujú o potrebe mobilizácie odborných znalostí, zdrojov a iniciatív pre účinnejší boj proti terorizmu. V tomto rámci členovia fóra zriadili špecializované medzinárodné orgány na riešenie otázok predchádzania násilnému extrémizmu a boja proti nemu: centrum excelentnosti pre boj proti násilnému extrémizmu Hedayah, Medzinárodný inštitút pre spravodlivosť a právny štát a Globálny fond na podporu komunitnej angažovanosti a odolnosti (Ú. v. EÚ JOIN(2015) 32 final, 27. 8. 2015) In: *GCTF, 2023. Who we are*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.thegctf.org/Who-we-are/Background-and-Mission.

[10] V máji 2005 sedem štátov *(Rakúsko, Belgicko, Francúzsko, Nemecko, Luxembursko, Holandsko, Španielsko)* podpísalo tzv. Prümskú zmluvu o zintenzívnení cezhraničnej spolupráce, najmä v boji proti terorizmu, cezhraničnej trestnej činnosti a nelegálnej migrácii, ktorá bola potom neskôr (v roku 2008) plne zavedená na úrovni EÚ, a to na základe Rozhodnutia Rady (Ú. v. EÚ L 210/1, 6. 8. 2008). V tejto dohode boli vymedzené základné oblasti policajnej spolupráce, a to predovšetkým oblasť poskytovania resp. výmeny informácií *(napr. údaje o DNA profiloch, daktyloskopické údaje, údaje o evidencii vozidiel, údaje týkajúce sa významných udalostí s cezhraničným rozmerom, napr. pri športových podujatiach alebo zasadnutiach Európskej rady)* a oblasť tzv. spoločných hliadkovaní a iných spoločných operácií.

[11] CISE je iniciatívou EÚ, ktorá zahŕňa viac než 300 európskych a národných autorít v oblasti námornej bezpečnosti. Bola spustená v roku 2009, pričom od roku 2019 pracuje na rozvoji tzv. operačného statusu pod záštitou Európskej agentúry pre námornú bezpečnosť *(The European Maritime Safety Agency – EMSA)*. Súčasťou tejto iniciatívy je aj výmena informácií o pirátstve, rizikách terorizmu, pašovaní zbraní a drog, obchodovaní s ľuďmi, znečistení životného prostredia, civilnej ochrane a prírodných katastrofách. In EURÓPSKA KOMISIA, 2023. Common information sharing environment (CISE). [online]. [cit. 2023-7-3].

V rovine operačnej spolupráce má podľa Európskeho programu v oblasti bezpečnosti kľúčovú pozíciu Stály výbor pre operačnú spoluprácu v oblasti vnútornej bezpečnosti *(angl. The Standing Committee on Operational Cooperation on Internal Security – COSI)*, ktorý tvoria zástupcovia členských štátov *(ministri vnútra/ministri spravodlivosti)*, zástupcovia Komisie, EEAS *(angl. European External Action Service – Európska služba pre vonkajšiu činnosť – ESVČ)*, EUROPOL, EUROJUST, FRONTEX, CEPOL a ďalší. V tejto súvislosti nemožno opomenúť ani úlohu spoločných vyšetrovacích tímov *(angl. joint investigation teams – JITs)*, centier policajnej a colnej spolupráce *(angl. police customs cooperation centres – PCCC)* v regiónoch na vnútorných hraniciach EÚ alebo cezhraničnú spoluprácu medzi vnútroštátnymi finančnými spravodajskými jednotkami *(angl. Financial Intelligence Units – FIUs*) a vnútroštátnymi úradmi pre vyhľadávanie majetku pochádzajúceho z trestnej činnosti *(angl. Asset Recovery Offices – AROs)*.

Európsky program zastrešuje aj podpornú oblasť, ktorá zahŕňa opatrenia na úseku odbornej prípravy, financovania, výskumu a inovácie, kde zohráva dôležitú úlohu CEPOL, ale aj Európska sieť odbornej justičnej prípravy *(angl. The European Judicial Training Network – EJTN)*, Európsky portál elektronickej justície a elektronického vzdelávania a Európske stredisko odbornej prípravy v oblasti bezpečnostnej ochrany.

Uvedený strategický dokument určuje tri hlavné priority pre európsku bezpečnosť, a to boj proti terorizmu a predchádzanie radikalizácii, boj proti organizovanej trestnej činnosti a boj proti počítačovej kriminalite. Na úseku boja proti terorizmu sa EÚ v časovom horizonte piatich rokov okrem iného zaviazala spustiť fórum EÚ s IT spoločnosťami,[12] spracovať návrh na revíziu rámcového rozhodnutia o terorizme,[13] vytvoriť centrum excelentnosti RAN.[14]

Vo vzťahu k potieraniu organizovanej trestnej činnosti boli revidované právne predpisy týkajúce sa strelných zbraní, ako aj existujúce politiky a právne predpisy o trestnej činnosti proti životnému prostrediu a prijatá stratégia pre boj proti obchodovaniu s ľuďmi na obdobie po roku 2016.

Prioritným cieľom v oblasti boja proti kybernetickej kriminalite je dosiahnuť vykonávanie legislatívnych aktov *(napr. stratégie kybernetickej bezpečnosti EÚ z roku 2013,[15] smernice o útokoch na informačné systémy z roku 2013,[16] smernice o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii z roku 2011,[17] Dohovoru Rady Európy o počítačovej kriminalite[18])*, ale aj revidovať existujúci či kodifikovať nový právny rámec *(napr. rámcového rozhodnutia z roku 2001 o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov[19] a prijatie návrhu*

Dostupné na internete: https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en.

[12] V roku 2017 vzniklo Globálne internetové fórum na boj proti terorizmu *(angl. The Global Internet Forum to Counter Terrorism – GIFCT)*. Iniciatívu založili spoločnosti Facebook *(neskôr Meta)*, Google/YouTube, Microsoft a Twitter. Cieľom GIFCT je zabrániť teroristom a násilným extrémistom zneužívať digitálne platformy. V júli 2020 zriadilo fórum viaceré pracovné skupiny. V tejto súvislosti možno spomenúť napr. pracovnú skupinu pre reakcie na incidenty *(angl. Incident Response Working Group – IRWG)*, ktorej súčasťou je od jesene 2022 aj Rada pre mediálne služby. In RADA PRE MEDIÁLNE SLUŽBY, 2023. Globálne internetové fórum na boj proti terorizmu (GIFCT). [online]. [cit. 2023-7-3]. Dostupné na internete: https://rpms.sk/globalne-internetove-forum-na-boj-proti-terorizmu-gifct.

[13] Ú. v. EÚ L 330, 9. 12. 2008 a Ú. v. EÚ L 88/6, 31. 3. 2017.

[14] Centrum excelentnosti RAN CoE *(angl. Radicalisation Awareness Network)* vzniklo v roku 2011. Združuje viac ako 6000 odborníkov z členských štátov EÚ v oblasti boja proti radikalizácii a násilného extrémizmu. In: *RADAR EUROPE, 2023. Radicalisation Awareness Network (RAN).* [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.radareurope.nl/themes/ran-coe/.

[15] Ú. v. EÚ JOIN/2013/01 final.

[16] Ú. v. EÚ L 218/8, 14. 8. 2013.

[17] Ú. v. EÚ L 335, 17. 12. 2011.

[18] *Oznámenie M ZV SR č. 137/2008 Z. z. Dohovor o počítačovej kriminalite.*

[19] Ú. v. EÚ L 123/18, 10. 5. 2019.

smernice o bezpečnosti sietí a informácií[20]*)*. Okrem toho stratégia poukazuje na význam inštitucionálneho rámca, ktorý prioritne zastrešuje Európske centrum boja proti počítačovej kriminalite pôsobiace v rámci EUROPOL-u, ako aj tímy reakcie na núdzové počítačové situácie v členských štátoch. [21]

V roku 2015 bola po výzve Európskej rady v rámci Oddelenia strategickej komunikácie a analýzy informácií ESVČ zriadená osobitná pracovná skupina pre strategickú komunikáciu **East StratCom** *(angl. The East StratCom* Task Force – *ESTF)* spolu s ďalšími dvoma skupinami – pre západný Balkán a juh – pre arabský svet *(Blízky východ, severná Afrika, Perzský záliv)*.[22] Samotná ESVČ vznikla v roku 2011, pričom jej poslaním, ako to už vyplýva z názvu, je riadiť diplomatické vzťahy EÚ s inými krajinami a vykonávať zahraničnú a bezpečnostnú politiku EÚ.[23]

Hlavnou náplňou práce skupiny East StratCom je identifikovať a vysvetľovať dezinformačné naratívy a analyzovať dezinformačné trendy, ktoré sú šírené v informačnom priestore orientujúc svoju pozornosť prioritne na našich východných susedov *(Arménsko, Azerbajdžan, Bielorusko, Gruzínsko, Moldavsko a Ukrajina)*. Jej vlajkovým projektom je webová stránka, na ktorej je umiestnená databáza článkov a médií, ktoré prezentujú nepravdivé, skreslené alebo neúplné informácie *(EUvsDisinfo)*, ako aj tematický týždenník *Desinformation Review*, ktorého poslaním je zvyšovanie povedomia o dezinformáciách. Možno konštatovať, že výstupným produktom činnosti tohto tímu expertov sú predovšetkým odborné analýzy, informácie, správy a podklady určené pre strategickú komunikáciu vládnych a politických špičiek, tlačové služby, ale aj pre širokú verejnosť. Aj z tohto dôvodu sa pracovná skupina vo svojej činnosti riadi Akčným plánom v oblasti strategickej komunikácie *(2015),*[24] uznesením o strategickej komunikácii EÚ s cieľom bojovať s propagandou tretích strán zameranou proti Únii *(2016),*[25] Akčným plánom proti dezinformáciám *(2018)*[26] a Akčným plánom pre európsku demokraciu *(2020)*[27], ktoré regulujú postup EÚ na tomto úseku.[28]

Jedným z kľúčových dokumentov na úseku boja proti hybridným hrozbám na úrovni EÚ je nesporne **Spoločný rámec pre boj proti hybridným hrozbám** *(2016)*. Uvedený strategický dokument prezentuje 22 opatrení, ktoré sú tematicky rozčlenené do piatich základných oblastí:

1. identifikácia hybridnej hrozby *(potreba realizácie prieskumu v členských štátoch s cieľom identifikovať oblasti potenciálne zraniteľné hybridnými hrozbami)*;
2. zlepšovanie informovanosti *(zriadenie Strediska EÚ pre hybridné hrozby v rámci ESVČ; zriadenie národných kontaktných miest pre hybridné hrozby v členských štátoch s cieľom zaistiť spoluprácu a komunikáciu so strediskom EÚ pre hybridné hrozby; strategická komunikácia a monitorovanie sociálnych médií mimo EÚ realizované ESVČ v spolupráci s East StratCom a Arab StratCom; zriadenie Centra excelentnosti pre boj proti hybridným hrozbám)*,

[20] Ú. v. EÚ COM(2013) 48 final, 7. 2. 2013.
[21] Ú. v. EÚ COM(2015) 185 final, 28. 4. 2015.
[22] Ú. v. EÚ EUCO 11/15, 20. 3. 2015.
[23] EUROPA.EU, 2023. *Európska služba pre vonkajšiu činnosť (ESVČ)*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-external-action-service-eeas_sk.
[24] Ú. v. EÚ Ares(2015) 2608242, 22. 06. 2015.
[25] Ú. v. EÚ C 224/58, 27. 6. 2018.
[26] Ú. v. EÚ JOIN(2018) 36 final, 5. 12. 2018.
[27] Ú. v. EÚ COM(2020) 790 final, 3. 12. 2020.
[28] EEAS, 2021. *Questions and Answers about the East StratCom Task Force.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11235.

3. budovanie odolnosti v jednotlivých oblastiach *(ochrana kritickej infraštruktúry – transpozícia a vykonávanie smernice týkajúcej sa kritickej infraštruktúry;*[29] *energetické siete – transpozícia a vykonávanie smernice o jadrovej bezpečnosti*[30] *a smernice o základných bezpečnostných štandardoch týkajúcich sa medzinárodnej spolupráce v oblasti havarijnej pripravenosti a odozvy na havarijnú situáciu;*[31] *bezpečnosť dopravy a dodávateľských reťazcov – napĺňanie Stratégie EÚ pre námornú bezpečnosť a jej akčný plán;*[32] *vesmír – príprava budúcej generácie GovSatCom na európskej úrovni a použitie systému Galileo pri kritických infraštruktúrach, ktoré závisia od časovej synchronizácie; obranná spôsobilosť; ochrana verejného zdravia a potravinová bezpečnosť – Výbor pre zdravotnú bezpečnosť, systém rýchleho varovania pre potraviny a krmivá (angl. The Rapid Alert System for Food and Feed – RASFF) a spoločného colného systému na riadenie rizík (angl. The Common* Customs *Risk Management System – CRMS); kybernetická bezpečnosť – výkon a transpozícia smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii*[33] *a v tejto súvislosti zriadenie siete 28 vnútroštátnych tímov pre reakciu na incidenty v oblasti počítačovej bezpečnosti (angl. Computer Security Incident Response Team –CSIRT) a tímu pre reakciu na núdzové počítačové situácie pre inštitúcie EÚ, tzv. CERT-EU; priemysel; energetika – napĺňanie Európskej stratégie energetickej bezpečnosti*[34] *a stratégia pre energetickú úniu,*[35] *zriadenie Strediska EÚ pre zdieľanie informácií o hrozbách a incidentoch – ITIS a platformy expertov kybernetickej bezpečnosti v odvetví energetiky (angl. Energy Expert Cyber Security Platform – EECSP); zabezpečenie zdravých finančných systémov v spolupráci s ENISA; doprava – spracovanie plánu pre kybernetickú bezpečnosť v letectve v spolupráci s Európskou agentúrou pre bezpečnosť letectva (angl. The European Union Aviation Safety Agency – EASA), v oblasti námornej bezpečnosti vychádzať zo stratégie námornej bezpečnosti EÚ a jej akčného plánu; boj proti financovaniu hybridných hrozieb – vykonávanie akčného plánu pre boj proti financovaniu terorizmu;*[36] *budovanie odolnosti proti radikalizácii a násilnému extrémizmu – vykonávanie opatrení proti radikalizácii stanovené v Európskom programe v oblasti bezpečnosti;*[37] *posilnenie spolupráce s tretími krajinami – budovanie fungujúcich a zodpovedných inštitúcií v tretích krajinách)*;

---

[29] Ú. v. EÚ L 345, 23. 12. 2008. V roku 2016 bola prijatá smernica Európskeho parlamentu a Rady (Ú. v. EÚ L 194/1, 19. 7. 2016).

[30] *Smernica Rady 2009/71/Euratom z 25. júna 2009, ktorou sa zriaďuje rámec Spoločenstva pre jadrovú bezpečnosť jadrových zariadení, zmenená smernicou Rady 2014/87/Euratom z 8. júla 2014*. Na tomto úseku bol prijatý Akčný plán na zlepšenie pripravenosti na chemické, biologické, rádiologické a jadrové bezpečnostné riziká (Ú. v. EÚ COM(2017) 610 final, 18. 10. 2017).

[31] Ú. v. EÚ L 13/1, 17. 1. 2014.

[32] *Akčný plán EÚ pre námornú bezpečnosť* (EUMSS) (Ú. v. EÚ ST/17002/14, 16. 12. 2014). Uvedená stratégia a akčný plán z roku 2014 boli v marci 2023 aktualizované v dokumente Spoločné oznámenie Európskemu parlamentu a Rade o aktualizácii stratégie námornej bezpečnosti EÚ a jej akčného plánu „Posilnená stratégia námornej bezpečnosti EÚ pre vyvíjajúce sa námorné hrozby" (Ú. v. EÚ JOIN (2023) 8 final, 10. 3. 2023).

[33] Ú. v. EÚ L 194/1, 19. 7. 2016. V roku 2017 boli na tomto úseku okrem iného prijaté: (Ú. v. EÚ JOIN(2017) 450 final, 13. 9. 2017), (Ú. v. EÚ COM(2017) 477 final, 13. 9. 2017) a (Ú. v. EÚ, COM(2018) 236 final, 26. 4. 2018).

[34] Ú. v. EÚ COM(2014) 0330 final.

[35] Ú. v. EÚ COM(2015) 080 final.

[36] Ú. v. EÚ COM(2016) 50 final, 2. 2. 2016.

[37] Stratégia vnútornej bezpečnosti na roky 2010 – 2014 bola revidovaná Európskym programom v oblasti bezpečnosti na roky 2015 – 2020 (Ú. v. EÚ COM(2015) 185 final, 28. 4. 2015) a neskôr Stratégiou EÚ pre bezpečnostnú úniu na roky 2020 – 2025 (Ú. v. EÚ COM/2020/605 final, 24. 7. 2020).

4. prevencia, reakcia na krízu a obnova *(činnosť Európskeho koordinačného centra pre reakcie na núdzové situácie (angl. The Emergency Response Coordination Centre – ERCC);*[38]
5. posilnenie spolupráce s NATO *(priama spolupráca medzi strediskom EÚ pre hybridné hrozby a strediskom NATO pre hybridné hrozby)*.[39] [40]

Ako sme už uviedli vyššie, v spoločnom rámci bola vymedzená potreba zriadenia **Strediska EÚ pre hybridné hrozby**. K jeho vzniku došlo ešte v priebehu roka 2016, pričom stredisko sa stalo organizačnou súčasťou **Spravodajského a situačného centra EÚ** *(angl. The EU Intelligence and Situation Centre – EU SITCEN, príp. SITCEN EÚ)*, ktoré už od roku 2011 operuje pod záštitou ESVČ. Právny základ pre zriadenie a fungovanie centra tvorí nariadenie Rady o organizácii a fungovaní Európskej služby pre vonkajšiu činnosť z roku 2010.[41] V tomto smere je potrebné uviesť, že stredisko vo svojej podstate reprezentuje tzv. **EU Hybrid Fusion Cell** *(EU HFC)* tak ako ho vymedzuje **Operačný protokol EÚ pre boj proti hybridným hrozbám** (2016). EU HFC je určeným kontaktným miestom pre spravodajské informácie týkajúce sa potenciálnych hybridných hrozieb. Úlohou tohto špecializovaného pracoviska je realizovať analýzy a zdieľať utajované informácie a informácie z otvorených zdrojov, ktoré sa týkajú najmä indikátorov hybridných hrozieb a rôznych varovaní smerujúcich k EÚ od rôznych zainteresovaných strán, napr. v rámci ESVČ *(vrátane delegácií EÚ)*, útvarov Komisie, agentúr EÚ a členských štátov. Pokiaľ ide o informácie o kybernetických hrozbách, EU HFC úzko spolupracuje s už spomínaným CERT-EU.[42]

CERT-EU *(angl. The Computer Emergency Response Team for the EU institutions, bodies and agencies)* vznikol v roku 2011. Napriek tomu, že administratívne spadá pod Generálne riaditeľstvo pre informatiku Komisie, t. j. orgán zodpovedný za digitálne služby, v zásade ide medziinštitucionálny útvar, ktorý prispieva k bezpečnosti infraštruktúry informačno-komunikačných technológií tým, že pomáha predchádzať kybernetickým útokom, odhaľovať ich, zmierňovať ich následky a reagovať na ne. *De facto* funguje ako centrum výmeny informácií o kybernetickej bezpečnosti a koordinácie reakcie na kybernetické incidenty pre všetkých adresátov *(inštitúcie, orgány a agentúry EÚ)*. Je členom CSIRTs Network *(CNW)*,[43] skupiny EGC *(angl. European Government CERTs Group)*,[44] FIRST,[45]

---

[38] Centrum existuje od roku 2001. Operuje v režime 24/7 a plní úlohu koordinátora, podpory, civilnej ochrany a humanitárnej pomoci v krízových situáciách medzi členskými štátmi EÚ a ďalšími 9 krajinami.
In: *EURÓPSKA KOMISIA, 2023. Emergency Response Coordination Centre (ERCC).* [online]. [cit. 2023-7-3]. Dostupné na internete: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/emergency-response-coordination-centre-ercc_en.

[39] Boj proti hybridným hrozbám je jednou zo siedmich oblastí spolupráce s NATO uvedenej v spoločnom vyhlásení podpísanom vo Varšave v júli 2016 predsedom Európskej rady, predsedom Komisie a generálnym tajomníkom NATO.

[40] Ú. v. EÚ JOIN/2016/018 final, 6. 4. 2016.

[41] Ú. v. EÚ L 201/30, 3. 8. 2010.

[42] Ú. v. EÚ SWD(2016) 227 final, 7. 7. 2016.

[43] CSIRTs Network je sieť zložená zo skupín CSIRT a CERT-EU určených členskými štátmi. Za SR je to SK-CERT a CSIRT.SK. CSIRTs Network poskytuje fórum pre členov, kde môžu spolupracovať a vymieňať si informácie o incidentoch ohrozujúcich kybernetickú bezpečnosť. In: *CSIRTs NETWORK.EU, 2023. About The Csirts Network.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://csirtsnetwork.eu/.

[44] Skupina EGC je neformálnym združením vládnych CERT v Európe. Vo svojej podstate ide o operačnú technickú skupinu, ktorej úlohou je spolupracovať pri reakcii na bezpečnostné incidenty v oblasti informačných technológií. In: *EGC GROUP, 2022. European Government CERTs (EGC) group*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://egc-group.org/.

[45] FIRST je globálnym lídrom v reakcii na bezpečnostné incidenty v oblasti informačných technológií. V súčasnosti má táto organizácia viac ako 600 členov v Európe, Amerike, Afrike, Ázii a Oceánii. In: *FIRST, 2023. FIRST is the global Forum of Incident Response and Security Teams*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.first.org/.

Trusted Introducer[46] a ďalších fór. Spolupracuje s agentúrou ENISA.[47] A v roku 2016 podpísal dohodu s NATO Computer Incident Response Capability *(NCIRC)* na výmenu informácií o kybernetickej bezpečnosti.[48]

Všeobecná potreba vytvorenia špecializovaného spravodajského pracoviska na pôde EÚ vo svojej podstate vyplynula zo spádu nešťastných udalostí súvisiacich s teroristickými útokmi v New Yorku dňa 11. 9. 2001. Práve na podklade týchto skutočností bolo v roku 2002 formálne vytvorené SITCEN EÚ, ktoré po personálnej stránke zastrešujú národní experti a zamestnanci spravodajských služieb členských štátov. Týmito krokmi sa podarilo nastaviť optimálne podmienky pre spravodajskú činnosť a v konečnom dôsledku aj na získavanie strategických informácií o rôznych druhoch bezpečnostných hrozieb vrátane terorizmu. Aj to boli dôvody, prečo centrum od roku 2007 začalo úzko spolupracovať so spravodajským riaditeľstvom Vojenského štábu EÚ *(angl. The European Union Military Staff – EUMS)* v tzv. jednotnej spravodajskej analytickej kapacite *(angl. Single Intelligence Analysis Capacity – SIAC)*. SITCEN EÚ od svojho vzniku prešlo viacerými reštrukturalizáciami, ktoré v roku 2012 viedli k tomu, že sa premenovalo na **Spravodajské analytické centrum EÚ** *(angl. Intelligence Analysis Centre – EU INTCEN)*. K hlavným úlohám nového centra patrí poskytovanie spravodajských a analytických produktov určeným adresátom, napr. ESVČ, rozhodovacím orgánom EÚ a členským štátom. Je preto logické, že aj jeho štrukturálna stránka koreluje s napĺňaním týchto funkcií *(centrum má dve organizačné súčasti – analytickú divíziu a divíziu pre všeobecné a vonkajšie vzťahy)*. Centrum zároveň vystupuje ako jednotné kontaktné miesto v EÚ pre utajované informácie pochádzajúce z civilných spravodajských a bezpečnostných služieb členských štátov, čo vnímame ako veľmi podstatný fakt na úseku koordinácie spravodajskej činnosti.[49]

K ďalším subjektom operujúcim na úseku boja proti hybridným hrozbám zriadeným práve na základe predmetného spoločného rámca možno zaradiť **Európske centrum výnimočnosti na boj proti hybridným hrozbám** *(angl. The European Centre of Excellence for Countering Hybrid Threats – ďalej len „Hybrid CoE")*. Centrum výnimočnosti zriadilo Fínsko v Helsinkách v apríli 2017 na základe výzvy EÚ adresovanej jej členským štátom. V súčasnosti na tomto projekte spolupracuje 33 členských štátov, EÚ a NATO vrátane Slovenska, ktoré je jeho členom od augusta 2020. Centrum má 3 základné siete záujmových komunít (tzv. *„The Community of Interest"*), a to: 1. Hybridný vplyv, 2. Zraniteľnosť a odolnosť, 3. Stratégia a obrana. Tieto komunity reprezentujú odborníci z členských krajín, EÚ a NATO. Ich úlohou je multinacionálna a multidisciplinárna výmena osvedčených

---

[46] Trusted Introducer *(TF-CSIRT)* vznikol v roku 2000 ako nástroj podpory pre všetky tímy na úseku informačnej bezpečnosti a reakcie na incidenty v oblasti informačných technológií. Trusted Introducer spravuje európsku databázu jednotiek CSIRT *(známych aj ako CERT)* a iných akreditovaných bezpečnostných tímov. Za SR tam vystupuje 13 tímov, napr. SK-CERT, CSIRT.SK, GOV CERT SK. In: *TF-CSIRT, 2019. Services for Security and Incident Response Teams*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.trusted-introducer.org/.

[47] ENISA vznikla v roku 2004. Právnym rámcom jej vzniku bolo Naradenie ES č. 460/2004 Európskeho parlamentu a Rady z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií EÚ (Ú. v. ES L 077, 13. 3. 2004). Toto nariadenie bolo zrušené Nariadením Európskeho parlamentu a Rady (EÚ) č. 526/2013 z 21. mája 2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) – (Ú. v. EÚ L 165/41, 18. 6. 2013). Agentúra sídli v Irekleio v Grécku. Prispieva k vytváraniu kybernetickej politiky EÚ a pomocou systémov certifikácie kybernetickej bezpečnosti zvyšuje dôveryhodnosť produktov, služieb a procesov informačno-komunikačných technológií, spolupracuje s členskými štátmi a orgánmi. In: *ENISA, 2023. ENISA Mandate and Regulatory Framework.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.enisa.europa.eu/about-enisa/regulatory-framework.

[48] CERT-EU, 2023. *About us.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://cert.europa.eu/about-us.

[49]STATEWATCH, 2015. *The EU Intelligence Analysis Centre*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf.

postupov, skúseností a odborných poznatkov, ako aj vytváranie priestoru pre koordinačné aktivity. Centrum zriadilo aj ďalšie organizačno-štrukturálne jednotky, ktoré plnia parciálne ciele na úseku boja proti hybridným hrozbám. Samotný akademický výskum a odbornú diskusiu na relevantné témy zabezpečuje špecifický výskumný a analytický tím *(angl. The Research and Analysis Team*). Okrem toho, úsek vzdelávania a prípravy na prácu s rôznymi scenármi hybridných hrozieb zastrešuje špecializovaný tím *(angl. The Training and Exercises Team*).[50]

Na Spoločný rámec pre boj proti hybridným hrozbám – reakcia EÚ nadviazal ďalší dôležitý nástroj, ktorým bolo Spoločné oznámenie Európskeho parlamentu, Európskej Rade a Rade pod názvom **Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby** (2018). Cieľom tohto materiálu bolo zhodnotiť doterajšiu reakciu EÚ na hybridné hrozby a zintenzívniť toto úsilie v najbližšom období. Súčasťou načrtnutej stratégie bol sled krokov tematicky rozdelených do piatich základných oblastí:

1. Situačné povedomie – lepšia schopnosť odhaľovať hybridné hrozby *(zefektívnenie činnosti Strediska pre hybridné hrozby ESVČ a Spravodajského analytického centra EÚ (INTCEN) na operačnej – spravodajskej úrovni),*
2. Posilnené opatrenia proti chemickým, biologickým, rádiologickým a jadrovým hrozbám *(plnenie Akčného plánu z októbra 2017 proti chemickým, biologickým, rádiologickým a jadrovým bezpečnostným rizikám, [51] prijatie nových operatívnych opatrení v súlade s odporúčaním o okamžitých krokoch na zabránenie zneužívania prekurzorov z roku 2017 a nariadením o uvádzaní prekurzorov výbušnín na trh a ich používaní z roku 2019),* [52]
3. Strategická komunikácia – šírenie zrozumiteľných informácií *(osobitne v období volieb, ktoré je mimoriadne strategickým a citlivým cieľom pre kybernetické útoky a online obchádzanie platných („off-line") záruk a pravidiel),*
4. Budovanie odolnosti a odstrašujúceho účinku v sektore kybernetickej bezpečnosti *(realizácia opatrení vyjadrených v smernici o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii z roku 2016*[53] *a odporúčaní komisie o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu z roku 2017*[54]*),*
5. Budovanie odolnosti proti nepriateľskej spravodajskej činnosti *(preverovanie investícií a finančných transakcií v EÚ na základe návrhu nariadenia, ktorým sa stanovuje rámec na preverovanie priamych zahraničných investícií do EÚ*[55]*).*[56]

Implementácia opatrení stanovených v spoločnom rámci a spoločnom oznámení sa pravidelne monitoruje, pričom Európska komisia prostredníctvom svojho útvaru – Generálneho riaditeľstva pre obranný priemysel a vesmír *(angl. Directorate-General for Defence Industry and Space – DEFIS)* - v spolupráci s ESVČ každoročne *(od roku 2017 do roku 2022)* predkladá správu o úrovni pokroku v tejto oblasti.[57]

---

[50] Hybrid CoE, 2023. *What is Hybrid CoE?* [online]. [2023-2-1]. Dostupné na internete: https://www.hybridcoe.fi/.

[51] Ú. v. EÚ COM(2017) 610 final, 18. 10. 2017.

[52] Ú. v. EÚ L 273/12, 24.10.2017 a Ú. v. EÚ L 186/1, 11. 7. 2019.

[53] Ú. v. EÚ L 194/1, 19. 7. 2016.

[54] Ú. v. EÚ L 239/36, 19. 9. 2017.

[55] Ú. v. EÚ COM(2017) 487, 13. 9. 2017. Medzičasom v roku 2019 bolo v tomto smere prijaté Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/452 z 19. marca 2019, ktorým sa ustanovuje rámec na preverovanie priamych zahraničných investícií do Únie (Ú. v. EÚ LI 79/1, 21. 3. 2019).

[56] Ú. v. EÚ JOIN/2018/16 final, 13. 6. 2018.

[57] *Annual progress reports on countering hybrid threats*: Ú. v. EÚ JOIN(2017) 30 final, 19. 7. 2017; Ú. v. EÚ JOIN(2018) 14 final, 13. 6. 2018; Ú. v. EÚ SWD(2019) 200 final, 29. 5. 2019; Ú. v. EÚ SWD(2020) 153 final, 24.7.2020; Ú. v. EÚ SWD (2021) 729, 22. 7. 2021; Ú. v. EÚ SWD(2022) 308, 16. 9. 2022.

V súvislosti s činnosťou osobitnej skupiny pre strategickú komunikáciu East StratCom v rámci ESVČ k významným dokumentom na úseku boja proti dezinformáciám v euro priestore možno zaradiť **Akčný plán proti dezinformáciám** *(2018)*, ktorý nadviazal na **Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov: Boj proti dezinformáciám na internete: európsky prístup** *(2018)*. Pre doplnenie uvádzame, že súčasťou akčného plánu je aj správa o pokroku v súvislosti s predmetným oznámením *(2018)*.[58] Vzniku akčného plánu predchádzalo zriadenie expertnej skupiny na vysokej úrovni, ktorá má v tejto záležitosti poskytovať poradenstvo *(2017)*, proces konzultácií so širokou verejnosťou založený na online dotazníkoch, štruktúrovaných dialógoch s príslušnými zainteresovanými stranami a prieskume verejnej mienky Eurobarometra, ktorý sa konal vo všetkých 27 členských štátoch *(2019 – 2020)*. Akčný plán proti dezinformáciám je prínosný vo viacerých ohľadoch. Nielenže vo všeobecnej rovine vymedzuje pojem dezinformácie, ale zároveň špecifikuje koordinovaný postup na úseku boja proti dezinformáciám prostredníctvom spektra opatrení globálneho významu. [59]

Za dezinformáciu sa považuje overiteľne nepravdivá alebo zavádzajúca informácia, ktoré je vytvorená, prezentovaná a šírená na účely hospodárskeho zisku alebo zámerného zavádzania verejnosti a môže poškodiť verejný záujem. Poškodenie verejného záujmu zahŕňa hrozby pre demokratické procesy, ako aj pre verejné statky, napríklad pre zdravie občanov Únie, životné prostredie alebo bezpečnosť. Medzi dezinformácie nepatria neúmyselné chyby v spravodajstve, satira a paródie ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené. Opatrenia uvedené v tomto akčnom pláne sú zamerané len na dezinformácie, ktoré sú zákonné podľa právnych predpisov Únie alebo vnútroštátnych právnych predpisov. Nie sú nimi dotknuté potenciálne uplatniteľné právne predpisy Únie ani ktoréhokoľvek členského štátu vrátane pravidiel týkajúcich sa nezákonného obsahu.[60]

Koordinovaná reakcia na dezinformácie prezentovaná v tomto akčnom pláne je založená na štyroch pilieroch:

1. zlepšovanie schopností inštitúcií Únie, pokiaľ ide o detekciu, analýzu a odhaľovanie dezinformácií;
2. posilňovanie koordinovaných a spoločných reakcií na dezinformácie;
3. mobilizácia súkromného sektora pri boji proti dezinformáciám;
4. zvyšovanie informovanosti a zlepšovanie odolnosti spoločnosti.

V rámci prvého piliera sa Únia zaviazala kapacitne posilniť osobitné strategicko-komunikačné jednotky ESVČ, ktoré budú spolupracovať s Komisiou, konkrétne s internou sieťou Komisie proti dezinformáciám, ktorá bola zriadená po oznámení o boju proti dezinformáciám na internete z roku 2018. V praktickom význame to značí, že je potrebné navýšiť rozpočet a personálne kapacity týchto expertných zoskupení, pričom s vyčlenením finančných prostriedkov už počítajú program Horizont Európa *(2021 – 2027)*[61] a program Kreatívna Európa *(2021 – 2027)*.[62]

V kontexte úloh vymedzených v druhom pilieri je potrebné zaviesť systém včasného varovania na boj proti dezinformačným kampaniam, ktorý by mal fungovať na obdobnej

[58] Ú. v. EÚ COM(2018) 794 final, 5. 12. 2018.
[59] Ú. v. EÚ COM(2018) 236 final, 26. 4. 2018.
[60] Napr. Ú. v. EÚ L 63/50, 6. 3. 2018 a Ú. v. EÚ L 172/79, 17. 5. 2021.
[61] ERAPORTAL, 2023. *Horizont Európa*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://eraportal.sk/horizont-europa-2/.
[62] EURÓPSKA RADA, 2023. *Program Kreatívna Európa na roky 2021 – 2027*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/creative-europe-2021-2027/.

báze, ako je tomu pri Koordinačnom centre pre reakcie na núdzové situácie *(v režime 24/7)*.[63] Funkcie systému včasného varovania budú po inštitucionálnej stránke zastrešovať Situačné stredisko ESVČ, ďalej stredisko EÚ pre hybridné hrozby Spravodajského a situačného centra, prípadne príslušné pracovné skupiny Rady, pričom budú úzko spolupracovať s Európskym parlamentom, ako aj Organizáciou Severoatlantickej zmluvy a mechanizmom rýchlej reakcie skupiny G7.

V súlade s tretím pilierom bol v septembri 2018 uverejnený **Kódex postupov proti šíreniu dezinformácií**.[64] Pôvodnými signatármi kódexu sú najväčšie online platformy *(Facebook, Google, Youtube, Twitter)*, poskytovatelia softvéru *(Mozilla)*, inzerenti, ako aj viaceré obchodné združenia, ktoré zastupujú online platformy a reklamný priemysel. Cieľom kódexu postupov je vytvoriť transparentnejší, dôveryhodnejší a spoľahlivejší online ekosystém, ktorý bude chrániť používateľov pred dezinformáciami. Dodržiavanie kódexu bude pravidelne monitorované za pomoci Skupiny európskych regulačných orgánov pre audiovizuálne mediálne služby *(angl. The European Regulators Group for Audiovisual Media Services – ERGA)* a Európskeho audiovizuálneho observatória *(angl. The European Audiovisual Observatory – EAO)* v súlade so **smernicou o audiovizuálnych mediálnych službách** *(2010)*.[65] V tejto súvislosti považujeme za potrebné uviesť, že kódex postupov bol v roku 2022 revidovaný. Obsahuje 44 záväzkov a 128 konkrétnych opatrení, pričom záväzok posilniť proces boja proti dezinformáciám podpísalo 34 signatárov a zaviazalo sa, že tieto záväzky splnia do konca roka 2022. Za zmienenie určite stojí zriadenie Centra pre transparentnosť *(angl. The Transparency Centre)* a analogickej pracovnej skupiny, ku ktorému formálne došlo vo februári 2023. Praktickým prínosom tohto centra je dispozícia jednotného úložiska dát, kde budú mať občania EÚ, výskumní pracovníci a mimovládne organizácie prístup k informáciám a budú si ich môcť stiahnuť online. Práve vďaka tomuto môžu získať také údaje, ako napr. *koľko príjmov z reklamy, ktoré prúdili k šíriteľom dezinformácií, sa podarilo obmedziť; množstvo prijatých alebo zamietnutých politických reklám; zistené prípady manipulatívneho správania (t. j. vytváranie a používanie falošných účtov); informácie o stave na úseku overovania faktov.*[66] Nový kódex zohľadňoval požiadavky formulované v hodnotení efektívnosti prvotného kódexu postupov, ktoré bolo pod záštitou Komisie realizované v roku 2020 a návrh Komisie o tzv. Akte o digitálnych službách. **Akt o digitálnych službách,** ktorý novelizoval smernicu o elektronickom obchode *(2000)*,[67] bol nakoniec prijatý v októbri 2022.[68]

V rámci štvrtého piliera je potrebné zorganizovať cielené kampane pre verejnosť a kurzy pre médiá a tvorcov verejnej mienky v Únii a jej susedstve s cieľom zvýšiť informovanosť o negatívnych dosahoch dezinformácií. Okrem toho sa javí žiadúce vytvárať multidisciplinárne tímy nezávislých overovateľov informácií a výskumníkov so špecifickými znalosťami miestnych informačných prostredí s cieľom detegovať a odhaľovať dezinformačné kampane na rôznych sociálnych sieťach a v digitálnych médiách. Nezávislí overovatelia faktov musia v tejto súvislosti rešpektovať dokument z roku 2015 pod názvom

---

[63] Koordinačné centrum pre reakcie na núdzové situácie *(angl. The Emergency Response Coordination Centre – ERCC)* bolo zriadené v roku 2013. Právnym rámcom jeho vzniku bolo rozhodnutie Európskeho parlamentu a Rady (Ú. v. EÚ L 347/924, 20. 12. 2013).

[64] EURÓPSKA KOMISIA, 2018. *EU Code of Practice on Disinformation*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://digital-strategy.ec.europa.eu/sk/library/2018-code-practice-disinformation.

[65] Ú. v. EÚ L 95/1, 15. 4. 2010.

[66] EURÓPSKA KOMISIA, 2023. *Kódex nakladania s dezinformáciami: Nové centrum transparentnosti poskytuje po prvýkrát poznatky a údaje o dezinformáciách na internete*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation-new-transparency-centre-provides-insights-and-data-online.

[67] Ú. v. EÚ L 178, 17. 7. 2000.

[68] Ú. v. EÚ L 277/1, 27. 10. 2022.

Kódex zásad Medzinárodnej siete pre overovanie faktov *(angl. International Fact-Checking Network – IFCN Codes and Principles)*, ktorý je primárne určený pre organizácie, ktoré pravidelne uverejňujú nestranné správy o presnosti vyhlásení verejných činiteľov a významných inštitúcií a iných rozšírených tvrdení, ktoré sú pre spoločnosť dôležité. Na to, aby určitému subjektu bol udelený štatút signatára IFCN, musí spĺňať viacero podmienok *(31 kritérií)*, pričom splnenie týchto kritérií v konečnom dôsledku posudzuje poradný výbor IFCN.[69]V tejto súvislosti bolo navrhnuté zriadiť európsku online platformu na prepojenie overovateľov faktov a výskumníkov, ako aj online platformu o dezinformáciách. Pilotné financovanie týchto nástrojov bolo realizované v rámci tzv. Nástroja na prepájanie Európy v súlade s naradením Európskeho parlamentu a Rady. [7071]

V **Záveroch Rady o komplementárnom úsilí zameranom na zvyšovanie odolnosti a boj proti hybridným hrozbám** *(2019)* Rada oceňuje dosiahnutý pokrok a stanovuje priority týkajúce sa ochrany EÚ pred hybridnými hrozbami, medzi ktoré radí koherentné úsilie zamerané na posilnenie odolnosti a boj proti hybridným hrozbám; prepojenie vnútornej a vonkajšej bezpečnosti; situačné povedomie a analýzu spravodajských informácií; ochranu kritickej infraštruktúry; boj proti dezinformáciám a zabezpečenie slobodných a spravodlivých volieb a v neposlednom rade aj bezpečnosť inštitúcií, orgánov a agentúr EÚ.[72]

Boj proti dezinformáciám bol zahrnutý aj v už vyššie spomínanom **Akčnom pláne pre európsku demokraciu** *(2020)* spolu s ďalšími dvoma základnými sférami, na ktoré sa musí EÚ v najbližšom období zamerať *(ochrana integrity volieb a podpory demokratickej účasti; posilňovanie slobody a plurality médií)*. V tejto súvislosti je potrebné pracovať na zlepšovaní kapacít EÚ a členských štátov v boji proti dezinformáciám a zlepšovaní spolupráce s agentúrou ENISA, Európskym strediskom pre monitorovanie digitálnych médií *(angl. The*

[69] INFCN, 2023. *Code of principles*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://ifcncodeofprinciples.poynter.org/know-more/the-commitments-of-the-code-of-principles.
[70] Ú. v. EÚ L 348/129, 20. 12. 2013.
[71] Ú. v. EÚ JOIN(2018) 36 final, 5. 12. 2018.
[72] Ú. v. EÚ 14972/19, 10. 12. 2019.

European Digital Media Observatory – EDMO)[73] a EUROPOLOM,[74] ale aj s medzinárodnými partnermi, ako sú NATO alebo G7, osobitne na úseku budovania systému včasného varovania a reakcie na hybridné hrozby. Skutočnosť, že sú to práve online platformy, ktoré môžu využívať úmyselne škodiaci prevádzkovatelia na šírenie nepravdivého a zavádzajúceho obsahu, a ktoré majú signifikantný mienkotvorný vplyv na ich používateľov, viedol k potrebe vytvorenia regulačného rámca, ktorý bol načrtnutý v už spomínanom Akte o digitálnych službách *(2022)* a v Kódexe postupov proti šíreniu dezinformácií *(2018; revidovaný v roku 2022)*.

V júli 2019 vznikla **horizontálna pracovná skupina pre zvyšovanie odolnosti a boj proti hybridným hrozbám** *(angl. The Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats)* v rámci prípravných orgánov Rady. Pracovná skupina uľahčuje koordináciu činností Rady v oblasti boja proti hybridným hrozbám a podľa potreby spolupracuje s inými prípravnými orgánmi *(napr. horizontálnou pracovnou skupinou pre kybernetické otázky – angl. The Horizontal Working Party on Cyber Issues – CYBER, Koordinačným výborom pre komunikačné a informačné systémy – angl. Coordination Committee for Communication and Information Systems – CCCIS, Politickým a bezpečnostným výborom – PBV – angl. Political and Security Committee – PSC)*, inými inštitúciami, útvarmi a agentúrami EÚ.[75]

V júli 2020 Komisia zhodnotila úroveň boja proti hybridným hrozbám[76] a zároveň bola schválená **Stratégia pre bezpečnú EÚ**. Táto stratégia sa týka obdobia 2020 – 2025 a zameriava sa na budovanie spôsobilostí a kapacít na zabezpečenie nadčasového bezpečnostného prostredia. Dôvodom pre vytvorenie tejto stratégie je skutočnosť, že európska panoráma bezpečnostných hrozieb má premenlivý charakter, a práve preto je dôležité

[73] EDMO je projektom, ktorý podporuje nezávislú komunitu pracujúcu na boji proti dezinformáciám. Je centrom pre overovateľov faktov, akademikov a ďalšie príslušné zainteresované strany, ktoré môžu navzájom spolupracovať. Podporuje ich v aktívnom prepojení s mediálnymi organizáciami, odborníkmi na mediálnu gramotnosť a poskytuje podporu tvorcom politík. Formálne vzniklo na základe Akčného plánu boja proti dezinformáciám z roku 2018. In: *EURÓPSKA KOMISIA, 2023. European Digital Media Observatory (EDMO)*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory.

[74] EUROPOL je agentúrou EÚ od roku 2010. Prostredníctvom svojho operačného centra zabezpečuje nepretržitý tok informácií *(24/7)* medzi ním, členskými štátmi a tretími stranami o trestnej činnosti. V rámci tohto centra pracujú aj analytici, ktorí poskytujú relevantné analýzy žiadateľom. Na úseku výmeny informácií má zriadené viaceré nástroje, napr. sieťovú aplikáciu bezpečnej výmeny informácií *(SIENA)*, informačný systém EUROPOL-u *(angl. The Europol Information System – EIS)*, ktorý bol spustený v roku 2005 a je v 22 jazykoch, pričom predstavuje databázu kriminálnych a spravodajských informácií týkajúcich sa trestnej činnosti podľa mandátu EUROPOL-u; platformu EUROPOL-u pre expertov v oblasti presadzovania práva *(angl. The Europol Platform for Experts – EPE)*. Spracúva spravodajské a strategické analýzy za využitia analytického systému *(angl. The Europol Analysis System – EAS)*. K najvýznamnejším produktom strategickej analýzy zameranej na najzávažnejšie bezpečnostné hrozby, možno zaradiť *(angl.) Serious and Organised Crime Threat Assessment (SOCTA)*, Internet Organised Crime Threat Assessment *(IOCTA)*, *EU Terrorism Situation & Trend Report (TE-SAT)*, varovnú notifikáciu nových hrozieb organizovanej kriminality *(angl. from Europol's Scanning, Analysis and Notification (SCAN) team)*. Okrem toho poskytuje forenznú podporu v oblasti boja proti falšovaniu eura, nezákonnej výrobe drog, podvodom s platobnými kartami a kyberkriminalite. Práve v poslednej spomenutej oblasti EUROPOL figuruje v súvislosti s činnosťou EUCTF *(angl. EU Cybercrime Task Force)*, EC3 *(angl. European Cybercrime Centre)*, J-CAT *(angl. Joint Cybercrime Action Taskforce)*, SPACE *(angl. Secure Platform for Accredited Cybercrime Experts)*. In: *EUROPOL, 2021. Operations, Services & Innovation: Fighting crime with a full arsenal of tools.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.europol.europa.eu/operations-services-and-innovation.

[75] Ú. v. EÚ 10027/19, 8. 7. 2019.

[76] Ú. v. EÚ SWD(2020) 152 final, 24.7.2020.

sústrediť pozornosť na hľadanie optimálnych reakcií na tieto hrozby. EÚ si vytýčila štyri navzájom prepojené strategické priority, na ktorých sa bude v najbližšom období pracovať:

1. nadčasové bezpečnostné prostredie *(ochrana kritickej infraštruktúry – doprava, vesmírne systémy, energetika, financie a zdravotníctvo; preverovanie priamych zahraničných investícií; kybernetická bezpečnosť – napr. zriadenie spoločnej kybernetickej jednotky; ochrana verejných priestorov vrátane miest na bohoslužby; riešenie zneužívania bezpilotných vzdušných prostriedkov)*;
2. riešenie vyvíjajúcich sa hrozieb *(počítačová kriminalita – účinnejší boj proti sexuálnemu zneužívaniu detí a detskej pornografii, posilnenie kapacít v oblasti presadzovania práva pri digitálnych vyšetrovaniach, preskúmanie operačného protokolu EÚ na boj proti hybridným hrozbám z roku 2016*[77] *a posilnenie systému EÚ v oblasti reakcie na krízy, určenie odvetvových základných scenárov odolnosti voči hybridným hrozbám pre členské štáty aj inštitúcie a orgány EÚ)*;
3. ochrana Európanov pred terorizmom a organizovanou trestnou činnosťou *(posúdenie účinnosti a efektívnosti protiteroristickej agendy pre EÚ vrátane obnovených opatrení proti radikalizácii v EÚ, agendy boja proti organizovanej trestnej činnosti vrátane obchodovania s ľuďmi, vytvorenie novej agendy v oblasti drog,*[78] *nového akčného plánu EÚ proti prevádzačstvu migrantov na roky 2021 – 2025;*[79] *posúdenie účinnosti a efektívnosti smernice o ochrane životného prostredia prostredníctvom trestného práva,*[80] *vytvorenie akčného plánu EÚ na boj proti nedovolenému obchodovaniu so strelnými zbraňami na roky 2020 – 2025,*[81] *preskúmanie právnych predpisov o zaistení a konfiškácii majetku,* [82] *ako aj o úradoch pre vyhľadávanie majetku*[83]*)*;
4. pevný európsky bezpečnostný ekosystém *(posilnenie mandátu EUROPOLU, preskúmanie kódexu policajnej spolupráce EÚ a policajnej koordinácie v čase krízy, posilnenie EUROJUSTU s cieľom prepojiť justičné orgány a orgány presadzovania práva, revízia smernice o vopred poskytovaných informáciách o cestujúcich, oznámenie o vonkajšom rozmere záznamov o cestujúcich, posilnenie spolupráce medzi EÚ a INTERPOLOM, rámec na rokovanie o výmene informácií s kľúčovými tretími krajinami, lepšie bezpečnostné normy týkajúce sa cestovných dokladov, preskúmanie možnosti vytvorenia európskeho inovačného centra pre vnútornú bezpečnosť)*.[84]

Stratégia poukázala na potrebu posilnenia medzinárodnej policajnej a justičnej spolupráce, ktorá sa javí aj v kontexte existujúcich bezpečnostných hrozieb ako neuspokojivá, aj vzhľadom na to, že jej právny rámec bol koncipovaný už pred viac ako 30 rokmi. V tejto súvislosti je žiadúce zamerať sa na vzájomnú koordináciu činností medzi OLAF, EUROPOLOM, EUROJUSTOM a Európskou prokuratúrou *(angl. The European Public Prosecutor's Office – EPPO)*, napr. aj v rámci už existujúcej platformy EMPACT *(angl. European Multidisciplinary Platform Against Criminal Threats – Európska multidisciplinárna platforma proti hrozbám trestnej činnosti)*.[85]

---

[77] Ú. v. EÚ SWD(2016) 227, 7. 7. 2016.
[78] Ú. v. EÚ COM(2020) 606, 24. 7. 2020.
[79] Ú. v. EÚ COM(2020) 606 final, 29. 9. 2021.
[80] Ú. v. EÚ L 328/28, 6. 12. 2008.
[81] Ú. v. EÚ COM(2020) 608 final, 24. 7. 2020.
[82] Ú. v. EÚ L 127/39, 29. 4. 2014.
[83] Ú. v. EÚ L 332/103, 18. 12. 2007.
[84] Ú. v. EÚ COM/2020/605 final, 24. 7. 2020.
[85] EMPACT je bezpečnostná iniciatíva členských štátov EÚ zameraná na identifikáciu, stanovenie priorít a riešenie hrozieb, ktoré predstavuje organizovaný a závažný medzinárodný zločin. V roku 2021 sa EMPACT stala stálym nástrojom EÚ (závery Rady o trvalom pokračovaní cyklu politík EÚ v oblasti organizovanej a závažnej medzinárodnej trestnej činnosti). EMPACT prebieha v štvorročných cykloch. Ide o multidisciplinárnu platformu spolupráce členských štátov, ktorú podporujú všetky inštitúcie, orgány a agentúry EÚ *(napríklad*

Imanentnou podmienkou efektívnej policajnej spolupráce je výmena informácií. Napriek tomu, že v máji 2019 bol prijatý rámec interoperability medzi informačnými systémami EÚ v oblasti spravodlivosti a vnútorných vecí, napr. medzi systémom vstup/výstup *(angl. The Entry/Exit System – EES)*, európskym systémom pre cestovné informácie a povolenia *(angl. The European Travel Information and Authorization System – ETIAS)*, rozšíreným európskym informačným systémom registrov trestov *(ECRIS-TCN)*,[86] Schengenským informačným systémom, vízovým informačným systémom a aktualizovaným systémom EURODAC,[87] prax poukazuje na možné rezervy *(napr. je potrebné zvážiť potrebu automatizovanej výmeny údajov, ktorá by značne zjednodušila a zrýchlila celý proces výmeny dát)*.[88]V decembri 2021 Komisia navrhla **Kódex policajnej spolupráce** *(EU Police Cooperation Code)*, ktorý zahŕňal legislatívny balík troch oblastí: operačnú policajnú spoluprácu,[89] výmenu informácií medzi orgánmi presadzovania práva členských štátov[90] a automatizovanú výmenu údajov na účely policajnej spolupráce *(„Prümský rámec II“)*.[91]

V samotnej rovine operačnej policajnej spolupráce je v nadchádzajúcom období potrebné osobitne sa venovať cezhraničnému prenasledovaniu, cezhraničnému sledovaniu, spoločným hliadkam a spoločným operáciám. Donedávna sme tu registrovali množstvo problémov, napr. pri cezhraničných operáciách museli príslušníci polície rešpektovať rozdielne a v mnohých prípadoch aj zložité vnútroštátne pravidlá pre vstup do iného členského štátu a aj samotná komunikácia *(výmena správ)* nebola po technickej stránke na vyhovujúcej bezpečnej úrovni. Napriek tomu je potrebné povedať, že niektoré európske nástroje cezhraničnej operačnej policajnej spolupráce sa jednoznačne osvedčili, napr. tzv. vnútroštátne jednotné kontaktné body na výmenu informácií v oblasti presadzovania práva *(angl. single point of contact – SPOC)*, príp. už spomínané centrá policajnej a colnej

---

EUROPOL, FRONTEX, EUROJUST, CEPOL, OLAF, EU-LISA, EFCA, t. j. Európska agentúra na kontrolu rybárstva, angl. The European Fisheries Control Agency a ďalšie). Zapojené sú aj tretie krajiny, medzinárodné organizácie a ďalší verejní a súkromní partneri. Rada v máji 2021 prijala závery, v ktorých stanovila priority pre cyklus EMPACT *(január 2022 – december 2025)*: vysoko rizikové zločinecké siete, kybernetické útoky, obchodovanie s ľuďmi, sexuálne vykorisťovanie detí, prevádzačstvo migrantov, obchodovanie s drogami, podvody, hospodárske a finančné trestné činy, organizovaná majetková trestná činnosť, environmentálna trestná činnosť, obchodovanie so strelnými zbraňami. Okrem týchto priorít sa ako spoločný horizontálny strategický cieľ budú riešiť aj podvody s dokumentmi, pretože sú kľúčovým faktorom pre mnohé trestné činy. In: *EURÓPSKA KOMISIA, 2023. EMPACT fighting crime together*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/operational-cooperation/empact-fighting-crime-together_en.

[86] Európsky informačný systém registrov trestov *(ECRIS)*, ktorý funguje od apríla 2012, zabezpečuje elektronickú výmenu informácií z registrov trestov na decentralizovanom základe medzi členskými štátmi. ECRIS-TCN bude po zriadení centralizovaný systém, ktorý umožní orgánom členských štátov určiť, ktoré iné členské štáty majú záznamy v registri trestov o štátnych príslušníkoch tretích krajín alebo osobách bez štátnej príslušnosti, ktoré sa kontrolujú, aby potom mohli použiť existujúci systém ECRIS na adresovanie žiadostí o informácie o odsúdeniach len identifikovaným členským štátom. ECRIS-TCN bude spravovať agentúra eu-LISA. *In: EU-LISA, 2023. ECRIS-TCN*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn.

[87] EURODAC je informačný systém, ktorý od roku 2003 pomáha pri vybavovaní žiadostí o azyl tým, že uchováva a spracúva odtlačky prstov žiadateľov o azyl a nelegálnych migrantov, ktorí vstúpili do niektorej z európskych krajín. Týmto spôsobom systém pomáha identifikovať nové žiadosti o azyl na základe žiadostí už zaregistrovaných v databáze. Využíva ho 31 krajín: 27 členských štátov EÚ a 4 pridružené krajiny *(Island, Nórsko, Švajčiarsko a Lichtenštajnsko)*. In: *EU-LISA, 2023. EURODAC*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac.

[88] Ú. v. EÚ L 135/85, 22. 5. 2019.

[89] Ú. v. EÚ COM(2021) 780 final, 8. 12. 2021. K schváleniu odporúčania došlo v júni 2022 (Ú. v. EÚ ST/8720/22, 24. 5. 2022).

[90] Ú. v. EÚ COM(2021) 782 final, 8. 12. 2021.

[91] Ú. v. EÚ COM(2021) 784 final, 8. 12. 2021.

spolupráce v regiónoch na vnútorných hraniciach EÚ alebo spoločné vyšetrovacie tímy. Operačnú spoluprácu medzi orgánmi presadzovania práva krajín EÚ výrazne podporujú aj špecializované agentúry EÚ, medzi ktoré patrí napr. EUROPOL, CEPOL, FRONTEX, eu-LISA, EMCDDA, Agentúra EÚ pre azyl *(angl. The European Union Agency for Asylum – EUAA)* a EUROJUST. V neposlednom rade odporúčanie Rady vo sfére operačnej policajnej spolupráce poukazuje aj na význam spoločnej odbornej prípravy, vrátane jazykových kurzov a výmenných programov so zameraním na osobný profesionálny rozvoj a vytvorenie tzv. európskej policajnej kultúry *(angl. European police culture)*.

Na účely predchádzania, odhaľovania a vyšetrovania trestných činov je aj na úseku výmeny informácií medzi orgánmi presadzovania práva členských štátov potrebné stanoviť nové pravidlá, ktoré by platili pre všetky členské štáty rovnako. Práve preto by členské štáty mali zriadiť jednotné kontaktné miesto na výmenu informácií s ostatnými krajinami EÚ, ktoré by fungovalo nepretržite, zároveň by malo primerané personálne obsadenie a poskytovalo by požadované informácie v stanovených lehotách *(v naliehavých prípadoch do 8 hodín, v ostatných prípadoch max. do 7 dní)*. Štandardným komunikačným kanálom by sa podľa návrhu mala stať už vyššie spomínaná, dôveryhodná sieťová aplikácia na zabezpečenú výmenu informácií *(SIENA)*, ktorej gestorom je EUROPOL.[92]

Vo vzťahu k revidovaným pravidlám automatizovanej výmeny údajov na účely policajnej spolupráce definovanej v tzv. *„Prümskom rámci“* je súčasťou návrhu doplnenie podôb tváre podozrivých a odsúdených páchateľov a policajných záznamov do systému automatizovanej výmeny údajov a zavedenie centrálneho smerovača, ku ktorému sa môžu pripojiť vnútroštátne databázy, čím sa nahradí množstvo prepojení medzi jednotlivými národnými databázami. EUROPOL bude môcť takisto účinnejšie podporovať členské štáty tým, že údaje z krajín mimo EÚ bude porovnávať s údajmi v databázach členských štátov, čo pomôže identifikovať páchateľov známych v krajinách mimo EÚ.[93]V tejto súvislosti možno uviesť, že v súčasnosti agentúra eu-LISA pracuje na projekte e-CODEX *(angl. e-Justice Communication via Online Data Exchange)*, ktorý poskytuje interoperabilné riešenie na cezhraničnú výmenu justičných údajov a umožňuje tak všetkým členským štátom komunikovať medzi sebou prostredníctvom ich existujúcich vnútroštátnych systémov.[94]

V kontexte medzinárodných kooperatívnych tendencií vymedzených v kódexe policajnej spolupráce nemožno opomenúť ani spravodajskú činnosť realizovanú spravodajskými a bezpečnostnými službami členských štátov a na nadnárodnej úrovni – centrom EU INTCEN, ktoré na základe spravodajských informácií poskytuje situačnú informovanosť exkluzívne inštitúciám EÚ. Zároveň sa javí ako žiadúce posilnenie spolupráce

---

[92] V posledných rokoch sa SIENA stala aj štandardným kanálom na výmenu informácií pre špecializované útvary a orgány presadzovania práva a rôzne iniciatívy, ako sú AROs, PCCC, útvary informácií pre cestujúcich *(angl. passenger-information units – PIUs)*, FIUs, Európska sieť pracovísk cieľového pátrania *(angl. The European Network of Fugitive Active Search Teams – ENFAST)*, špeciálne taktické jednotky *(angl. special tactics units – ATLAS)*, spoločná akčná skupina pre počítačovú kriminalitu *(angl. Joint Cybercrime Action Taskforce – J-CAT)*, atď. Bol vytvorený osobitný rámec SIENA, ktorý umožňuje manipuláciu s vyhradeným obsahom týkajúcim sa boja proti terorizmu. Začiatkom roka 2022 bolo na špecializované protiteroristické prostredie SIENA pripojených 49 protiteroristických orgánov. Stratégia Europolu 2020+ vyzýva na ďalšie zavádzanie a rozvoj tohto systému. In: *EUROPOL, 2022. Secure Information Exchange Network Application (SIENA)*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena.

[93] EURÓPSKE NOVINY, 2021. *Kódex policajnej spolupráce: V záujme zvýšenia bezpečnosti posilňuje EK cezhraničnú policajnú spoluprácu.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://europske.noviny.sk/2021/12/13/kodex-policajnej-spoluprace-v-zaujme-zvysenia-bezpecnosti-posilnuje-ek-cezhranicnu-policajnu-spolupracu/.

[94] EU-LISA, 2023. e-CODEX. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/e-CODEX.

s INTERPOL-om *(napr. sprístupnenie databáz INTERPOL-u)*. Dôležitú úlohu tu zohráva predovšetkým zefektívnenie výmeny informácií. [95]

Vo februári 2021 Komisia v spolupráci s Hybrid CoE vydala publikáciu **Krajina hybridných hrozieb – koncepčný model**, ktorá opisuje zložky hybridných hrozieb z hľadiska aktérov, ich cieľov, nástrojov, oblastí, ktoré môžu byť ohrozené, ako aj rôznych fáz činnosti. Cieľmi modelu sú uľahčenie včasného odhalenia hybridných hrozieb, identifikácia nedostatkov v pripravenosti, reakcia na takéto hrozby a vypracovanie účinných opatrení na boj proti tomuto komplexnému javu. Analytický rámec navrhovaného koncepčného modelu sa ďalej overuje na základe viacerých reálnych prípadových štúdií s cieľom posúdiť jeho platnosť a analytickú hodnotu.[96]

V marci 2021 Rada schválila ďalší rozhodujúci dokument pre smerovanie EÚ – **Strategický kompas EÚ**, ktorý je vo svojej podstate ambicióznym akčným plánom EÚ na posilnenie bezpečnostnej a obrannej politiky EÚ do roku 2030. Členské štáty sa v tejto stratégii zaviazali realizovať aktivity v štyroch základných oblastiach, a to aktivita, bezpečnosť, investície a partneri. Čo sa týka oblasti aktivít, tam sa opatrenia EÚ zamerajú na spoločnú obrannú a bezpečnostnú politiku, v rámci ktorej je potrebné vytvoriť silnú kapacitu rýchleho nasadenia EÚ pre rôzne druhy kríz pozostávajúcu až z 5 000 vojakov; civilnú misiu s 200 plne vybavenými odborníkmi, a to aj v zložitých prostrediach; budú sa vykonávať pravidelné taktické cvičenia na súši a na mori; posilní sa vojenská mobilita, t. j. civilné a vojenské misie a operácie, a v neposlednom rade bude EÚ v plnej miere využívať tzv. Európsky mierový nástroj[97] na podporu partnerov.

Vo sfére bezpečnosti, EÚ zvýši svoje kapacity na analýzu spravodajských informácií; vytvorí súbor hybridných nástrojov a tímy rýchlej reakcie na hybridné hrozby; bude ďalej rozvíjať súbor nástrojov kybernetickej diplomacie a vytvorí politický rámec EÚ pre kybernetickú obranu s cieľom lepšie sa pripraviť a reagovať na kybernetické útoky; vytvorí súbor nástrojov proti manipulácii s informáciami a zasahovaniu zo zahraničia; vypracuje Stratégiu EÚ v oblasti kozmického priestoru pre bezpečnosť a obranu a v neposlednom rade posilní úlohu EÚ ako aktéra námornej bezpečnosti.

Na úseku investícií EÚ plánuje viac a lepšie investovať do spôsobilostí a inovatívnych technológií, ktorými sa bude snažiť vyplniť strategické medzery a znížiť technologickú a priemyselnú závislosť. V tejto súvislosti plánuje vytvoriť nové centrum pre inovácie v oblasti obrany v rámci Európskej obrannej agentúry.

Vo sfére partnerstva je žiadúce posilniť strategické partnerstvá s NATO a OSN, spoluprácu s regionálnymi partnermi vrátane OBSE *(Organizácia pre bezpečnosť a spoluprácu v Európe, angl. Organization for Security and Cooperation in Europe),* AÚ *(Africkou úniou)* a ASEAN-u *(Združenie národov juhovýchodnej Ázie, angl. The Association of Southeast Asian Nations)*, spoluprácu s bilaterálnymi partnermi, napr. s USA, Nórskom, Kanadou, Spojeným kráľovstvom a Japonskom; individualizované partnerstvá na západnom Balkáne, v našom východnom a južnom susedstve, v Afrike, Ázii a Latinskej Amerike a za týmto účelom vytvoriť fórum EÚ pre partnerstvo v oblasti bezpečnosti a obrany.[98]

Rok po schválení Strategického kompasu EÚ, zhodnotili ministri zahraničných vecí a ministri obrany členských štátov EÚ na spoločnom zasadnutí v marci 2023 pokrok, ktorý sa

---

[95] Ú. v. EÚ COM/2020/605 final, 24. 7. 2020.

[96] Hybrid CoE, 2021. *The landscape of Hybrid Threats: A conceptual model.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

[97] Európsky mierový nástroj je mimorozpočtový mierový fond, ktorého cieľom je predchádzať konfliktom, budovať mier a posilňovať medzinárodnú bezpečnosť. Bol vytvorený v roku 2021 na základe rozhodnutia Rady. In: *EURÓPSKA RADA, 2023. Európsky mierový nástroj.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/european-peace-facility/.

[98] Ú. v. EÚ ST/7371/22, 21. 3. 2022.

dosiahol pri jeho vykonávaní.[99] Dospeli k záveru, že vo všetkých štyroch pilieroch bol zaznamenaný progres a zároveň určili oblasti, ktoré si vyžadujú ďalšie úsilie. Vo vzťahu k hybridným hrozbám sa pracuje na vytvorení tzv. súboru nástrojov boja proti hybridným hrozbám EÚ *(angl. EU Hybrid Toolbox – EUHT),* súčasťou ktorého je aj vytvorenie tímov rýchlej reakcie EÚ na hybridné útoky *(angl. EU Hybrid Rapid Response Teams).* Okrem toho poukázali na potrebu vytvorenia tzv. súboru nástrojov FIMI *(angl. Toolbox Foreign Information Manipulation and Interference)*, ktorý predstavuje nový centrálny dátový priestor na zhromažďovanie informácií o hrozbách vyplývajúcich z dezinformácií a zahraničnej manipulácie s informáciami. V súčasnosti sa pracuje na jeho vytvorení spolu s medzinárodnými partnermi vrátane krajín G7 a NATO, ako aj so zainteresovanými stranami z občianskej spoločnosti a súkromného sektora. Okrem toho sa vykonáva revízia Protokolu EÚ v boji proti hybridným hrozbám *(angl. EU Protocol on countering hybrid threats)* a zároveň sa priebežne testujú a precvičujú aj naše možnosti reakcie na základe rôznych scenárov, aby sme mohli pokračovať vo vývoji nášho koncepčného prístupu k odolnosti a hybridným hrozbám. Aj vzhľadom na registrované bezpečnostné riziká v najbližšom období je potrebné zamerať sa na posilnenie odolnosti kritickej infraštruktúry. Na tomto úseku bola koncom roka 2022 prijatá smernica Európskeho parlamentu a Rady o odolnosti kritických subjektov, t. j. subjektov, ktoré sú kritické alebo životne dôležité pre spoločnosť a hospodárstvo, v súlade s ktorou bola vytvorená skupina pre odolnosť kritických subjektov *(angl. The Critical Entities Resilience Group – CERG).* [100] Okrem toho bolo prijaté odporúčanie Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry,[101]ktoré kontinuitne nadväzuje na Európsky program ochrany kritickej infraštruktúry *(2006),*[102] a Oznámenie Komisie Rade a Európskemu Parlamentu: Ochrana najdôležitejšej infraštruktúry v boji proti terorizmu *(2004).*[103]V nadväznosti na tieto kroky bola zriadená sieť ERNCIP *(angl. The European Reference Network for Critical Infrastructure Protection)* s cieľom zlepšiť ochranu kritických infraštruktúr v EÚ, ktorá úzko spolupracuje so všetkými typmi zainteresovaných strán v tejto oblasti, pričom sa zameriava najmä na technické riešenia ochrannej bezpečnosti.[104]

Platformou s analogickými cieľmi a úlohami je tzv. **spoločné výskumné centrum** *(angl. Joint Research Centre – JRC – resp. EU Science Hub)*, ktoré vzniklo paralelne s Európskym spoločenstvom pre atómovú energiu *(Euratom)* v roku 1957 s tým, že prvotne sa zameriavalo na výskum v nukleárnej oblasti. Až neskôr, v roku 1972, rozšírilo svoj mandát aj na výskum iných oblastí, najmä súvisiacich s bezpečnosťou a životným prostredím. Vzhľadom na to, že JRC je vo svojej podstate organizačnou súčasťou Komisie, zohráva kľúčovú úlohu vo viacerých fázach politického cyklu EÚ. Jeho cieľom je napĺňanie šiestich priorít Komisie *(stanovených na obdobie rokov 2019 – 2024),* a to 1. Európska zelená dohoda, 2. Európa pripravená na digitálny vek, 3. Hospodárstvo, ktoré pracuje v prospech ľudí, 4. Silnejšia Európa vo svete, 5. Podpora európskeho spôsobu života, 6. Nový impulz pre európsku demokraciu *(rozdelených do 33 portfólií).* [105] JRC poskytuje nezávislé, na faktoch založené poznanie a výskum, s pozitívnym dosahom na tvorbu európskej politiky

[99]EEAS, 2023. *Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eeas.europa.eu/sites/default/files/documents/2023/StrategicCompass_1stYear_Report.pdf.

[100] Ú. v. EÚ L 333/164, 27. 12. 2022.

[101] Ú. v. EÚ C 20/1, 20. 1. 2023.

[102] Ú. v. EÚ KOM/2006/0786 v konečnom znení, 12. 12. 2006.

[103] Ú. v. EÚ KOM/2004/0702 v konečnom znení, 20. 10. 2004.

[104] JRC, 2018. *ERNCIP Handbook 2018 editio*n. [online]. [cit. 2023-7-3]. Dostupné na internete: https://erncip-project.jrc.ec.europa.eu/documents/erncip-handbook-2018-edition.

[105] EURÓPSKA KOMISIA, 2023. *Priority Európskej komisie.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024_sk.

a spoločnosť. Prispieva k naplneniu celkového cieľa programu Horizont Európa *(je financované týmto rámcovým programom pre výskum a inováciu)* a úzko spolupracuje s výskumnými a politickými organizáciami v členských štátoch, európskymi inštitúciami a agentúrami a vedeckými partnermi v Európe a na medzinárodnej úrovni *(napr. aj s OSN).*[106] V roku 2016 JRC prijalo Stratégiu do roku 2030, pričom v decembri 2022 bola táto stratégia inovovaná *(Revitalizing the JRC Strategy 2030)*. V súlade s ňou si centrum vytýčilo 20 priorít, medzi ktoré v kontexte boja proti hybridným hrozbám okrem iného patrí napr. riešenie geopolitických hrozieb a zvyšovanie technologickej suverenity, predpovedanie a manažovanie krízy, riadenie digitálnej transformácie, podpora komplexného prístupu k bezpečnosti.[107]

Špecifickým projektom Komisie zameraným na boj proti hybridným hrozbám je aj tzv. **EU-HYBNET** *(Paneurópska sieť na boj proti hybridným hrozbám, angl. Empowering a Pan-European Network to Counter Hybrid Threats).* Tento projekt bol spustený v máji 2020 s plánovaným ukončením v apríli 2025. Sieť spája celoeurópskych odborníkov z praxe a zainteresované strany s cieľom identifikovať a analyzovať spoločné výzvy a požiadavky na boj proti hybridným hrozbám. Vykonáva výskum, upozorňuje na inovačné iniciatívy, organizuje vzdelávacie podujatia na testovanie inovácií a vydáva odporúčania na prijatie, industrializáciu a štandardizáciu týchto inovácií. O tieto výsledky sa delí s odborníkmi z praxe a tvorcami politík EÚ. V spolupráci s Komisiou/JRC boli vymedzené štyri kľúčové témy boja proti hybridným hrozbám *(trendy v oblasti hybridných hrozieb, kybernetické technológie a budúce technológie, odolnosť obyvateľstva, miestnej a národnej úrovne štátnej správy, informačná a strategická komunikácia)*.[108]

Záver

Z prezentovaného poznania, ktoré sme nadobudli účelovým vedeckým prístupom, vyplýva niekoľko čiastkových záverov.

V prvom rade, problematika hybridných hrozieb získava na dôležitosti minimálne posledných dvadsať rokov, dôkazom čoho je celý rad dokumentov a aktivít realizovaných zo strany EÚ. V tejto súvislosti považujeme za potrebné zdôrazniť, že boj proti hybridným hrozbám je už od roku 2010 kontinuitne subsumovaný do strategických cieľov EÚ v rámci bezpečnostnej politiky tohto spoločenstva štátov s výhľadom do roku 2030.

Boj proti hybridným hrozbám si vyžaduje, aj vzhľadom na ich multidisplinárny charakter, systematický, procesuálny a komplexný prístup, tzn. že sa neustále mení, adaptuje a inovuje v korelácii so stupňom poznania vývoja bezpečnostného prostredia. Napriek tomu, že kľúčoví hráči majú v tomto systéme nezameniteľné postavenie *(napr. Komisia, ESVČ, East StratCom, Hybrid CoE, EU-INTCEN, EU Hybrid Fusion Cell)*, bez spolupráce s inými subjektmi *(napr. členskými štátmi, Európskym parlamentom, agentúrami EÚ, zástupcami občianskej spoločnosti, akademickej obce a súkromného sektora, ale aj s medzinárodnými organizáciami, ako sú OSN, Rada Európy, INTERPOL a NATO)* by očakávaný výsledok celého snaženia bol značne poznamenaný dávkou skepsy.

---

[106] EURÓPSKA KOMISIA, 2023. *Joint Research Centre.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC133084/JRC133084_01.pdf.

[107] EURÓPSKA KOMISIA, 2023. *Revitalising the JRC Strategy 2030*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131698/JRC131698_01.pdf.

[108] EU-HYBNET, 2023. *A Pan-European Network to Counter Hybrid Threats.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://euhybnet.eu/.

Literatúra

Akčný plán EÚ pre námornú bezpečnosť (EUMSS) (Ú. v. EÚ ST/17002/14, 16. 12. 2014).

Akčný plán na zlepšenie pripravenosti na chemické, biologické, rádiologické a jadrové bezpečnostné riziká (Ú. v. EÚ COM(2017) 610 final, 18. 10. 2017).

Akčný plán v oblasti strategickej komunikácie (Ú. v. EÚ Ares(2015) 2608242, 22. 06. 2015).

Annual progress reports on countering hybrid threats: Ú. v. EÚ JOIN(2017) 30 final, 19. 7. 2017; Ú. v. EÚ JOIN(2018) 14 final, 13. 6. 2018; Ú. v. EÚ SWD(2019) 200 final, 29. 5. 2019; Ú. v. EÚ SWD(2020) 153 final, 24.7.2020; Ú. v. EÚ SWD (2021) 729, 22. 7. 2021; Ú. v. EÚ SWD(2022) 308, 16. 9. 2022.

CERT-EU, 2023. *About us.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://cert.europa.eu/about-us.

Council conclusions on CSDP (Ú. v. EÚ Consilium 8971/15, 18. 5. 2015), European Council meeting (25 and 26 June 2015) – Conclusions (Ú. v. EÚ EUCO 22/15, 26. 6. 20115).

Council recommendation on operational law enforcement cooperation (Ú. v. EÚ ST/8720/22, 24. 5. 2022).

CSIRTs NETWORK.EU, 2023. *About The Csirts Network*. [online]. [cit. 2023-07-03]. Dostupné na internete: https://csirtsnetwork.eu/.

EEAS, 2021. *Questions and Answers about the East StratCom Task Force*. [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11235.

EGC GROUP, 2022. *European Government CERTs (EGC) group.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://egc-group.org/.

ENISA, 2023. *ENISA Mandate and Regulatory Framework.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.enisa.europa.eu/about-enisa/regulatory-framework.

ERAPORTAL, 2023. *Horizont Európa.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://eraportal.sk/horizont-europa-2/.

EEAS, 2023. *Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence.* [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eeas.europa.eu/sites/default/files/documents/2023/StrategicCompass_1stYear_Report.pdf.

EU-HYBNET, 2023. *A Pan-European Network to Counter Hybrid Threats*. [online]. [cit. 2023-07-03]. Dostupné na internete: https://euhybnet.eu/.

EU-LISA, 2023. *e-CODEX*. [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/e-CODEX.

EU-LISA, 2023. *ECRIS-TCN*. [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn.

EU-LISA, 2023. *EURODAC*. [online]. [cit. 2023-7-3]. Dostupné na internete: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac.

EUROPA.EU, 2014. *Európske centrum boja proti počítačovej kriminalite na úrade Europol*. [online]. [cit. 2023-07-03]. Dostupné na internete:

https://publications.europa.eu/resource/cellar/6d16d2d0-7561-4492-beef-048e64bed66a.0022.02/DOC_1.

EUROPA.EU, 2023. *Európska služba pre vonkajšiu činnosť (ESVČ).* [online]. [cit. 2023-07-03]. Dostupné na internete: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-external-action-service-eeas_sk.

European Council meeting (19 and 20 March 2015) – Conclusions (Ú. v. EÚ EUCO 11/15, 20. 3. 2015).

EUROPOL, 2021. *Operations, Services & Innovation: Fighting crime with a full arsenal of tools.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.europol.europa.eu/operations-services-and-innovation.

EUROPOL, 2022. *Secure Information Exchange Network Application (SIENA).* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena.

EURÓPSKA KOMISIA, 2018. *EU Code of Practice on Disinformation.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://digital-strategy.ec.europa.eu/sk/library/2018-code-practice-disinformation.

EURÓPSKA KOMISIA, 2023. *Common information sharing environment (CISE).* [online]. [cit. 2023-07-03]. Dostupné na internete: https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en.

EURÓPSKA KOMISIA, 2023. *Emergency Response Coordination Centre (ERCC).* [online]. [cit. 2023-07-03]. Dostupné na internete: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/emergency-response-coordination-centre-ercc_en.

EURÓPSKA KOMISIA, 2023. *EMPACT fighting crime together.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/operational-cooperation/empact-fighting-crime-together_en.

EURÓPSKA KOMISIA, 2023. *European Digital Media Observatory (EDMO).* [online]. [cit. 2023-07-03]. Dostupné na internete: https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory.

EURÓPSKA KOMISIA, 2023. *Joint Research Centre.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC133084/JRC133084_01.pdf.

EURÓPSKA KOMISIA, 2023. *Kódex nakladania s dezinformáciami: Nové centrum transparentnosti poskytuje po prvýkrát poznatky a údaje o dezinformáciách na internete.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation-new-transparency-centre-provides-insights-and-data-online.

EURÓPSKA KOMISIA, 2023. *Priority Európskej komisie*. [online]. [cit. 2023-07-03]. Dostupné na internete: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024_sk.

EURÓPSKA KOMISIA, 2023. *Revitalising the JRC Strategy 2030.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131698/JRC131698_01.pdf.

EURÓPSKA KOMISIA, 2023. *Special Eurobarometer 532: The Digital Decade*. [online]. [cit. 2023-07-3]. Dostupné na internete: https://webgate.ec.europa.eu/ebsm/api/public/deliverable/download?doc=true&deliverableId=87743.

EURÓPSKA RADA, 2021. *Koordinátor pre boj proti terorizmu.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/fight-against-terrorism/counter-terrorism-coordinator/.

EURÓPSKA RADA, 2023. *Európsky mierový nástroj.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/european-peace-facility/.

EURÓPSKA RADA, 2023. *Program Kreatívna Európa na roky 2021 – 2027.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.consilium.europa.eu/sk/policies/creative-europe-2021-2027/.

EURÓPSKE NOVINY, 2021. *Kódex policajnej spolupráce: V záujme zvýšenia bezpečnosti posilňuje EK cezhraničnú policajnú spoluprácu.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://europske.noviny.sk/2021/12/13/kodex-policajnej-spoluprace-v-zaujme-zvysenia-bezpecnosti-posilnuje-ek-cezhranicnu-policajnu-spolupracu/.

FIRST, 2023. *FIRST is the global Forum of Incident Response and Security Teams.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.first.org/.

GCTF, 2023. *Who we are.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.thegctf.org/Who-we-are/Background-and-Mission.

Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats: Establishment and adoption of its Terms of Reference (Ú. v. EÚ 10027/19, 8. 7. 2019).

Hybrid CoE, 2021. *The landscape of Hybrid Threats: A conceptual model.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

Hybrid CoE, 2023. *What is Hybrid CoE?* [online]. [2023-02-01]. Dostupné online: https://www.hybridcoe.fi/.

INFCN, 2023. *Code of principles.* [online]. [cit. 2023-07-03]. Dostupné na internete: https://ifcncodeofprinciples.poynter.org/know-more/the-commitments-of-the-code-of-principles.

Joint staff working document: EU operational protocol for countering hybrid threats 'EU Playbook' (Ú. v. EÚ SWD(2016) 227 final, 7. 7. 2016).

Joint staff working document: Mapping of measures related to enhancing resilience and countering hybrid threats (Ú. v. EÚ SWD(2020) 152 final, 24.7.2020).

JRC, 2018. *ERNCIP Handbook 2018 edition*. [online]. [cit. 2023-07-03]. Dostupné na internete: https://erncip-project.jrc.ec.europa.eu/documents/erncip-handbook-2018-edition.

Komplementárne úsilie zamerané na zvyšovanie odolnosti a boj proti hybridným hrozbám – závery Rady, ktoré Rada prijala na svojom 3739. zasadnutí 10. decembra 2019. (Ú. v. EÚ 14972/19, 10. 12. 2019).

Nariadenie ES č. 460/2004 Európskeho parlamentu a Rady z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií EÚ (Ú. v. ES L 077, 13. 3. 2004).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/818 z 20. mája 2019 o stanovení rámca pre interoperabilitu medzi informačnými systémami EÚ v oblasti policajnej a justičnej

spolupráce, azylu a migrácie a o zmene nariadení (EÚ) 2018/1726, (EÚ) 2018/1862 a (EÚ) 2019/816 (Ú. v. EÚ L 135/85, 22. 5. 2019).

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1316/2013 z 11. decembra 2013 o zriadení Nástroja na prepájanie Európy, ktorým sa mení nariadenie (EÚ) č. 913/2010 a zrušujú sa nariadenia (ES) č. 680/2007 a (ES) č. 67/2010. (Ú. v. EÚ L 348/129, 20. 12. 2013).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/452 z 19. marca 2019, ktorým sa ustanovuje rámec na preverovanie priamych zahraničných investícií do Únie (Ú. v. EÚ LI 79/1, 21. 3. 2019).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/784 z 29. apríla 2021 o riešení šírenia teroristického obsahu online (Ú. v. EÚ L 172/79, 17. 5. 2021).

Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách). (Ú. v. EÚ L 277/1, 27. 10. 2022).

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 526/2013 z 21. mája 2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) (Ú. v. EÚ L 165/41, 18. 6. 2013).

Návrh nariadenia Európskeho parlamentu a Rady o automatizovanej výmene údajov na účely policajnej spolupráce („prümský rámec II“), ktorým sa menia rozhodnutia Rady 2008/615/SVV a 2008/616/SVV a nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1726, (EÚ) 2019/817 a (EÚ) 2019/818 (Ú. v. EÚ COM(2021) 784 final, 8. 12. 2021).

Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje rámec na preverovanie priamych zahraničných investícií do EÚ (Ú. v. EÚ COM(2017) 487, 13. 9. 2017).

Návrh odporúčania Rady týkajúce sa operačnej policajnej spolupráce (Ú. v. EÚ COM(2021) 780 final, 8. 12. 2021).

Návrh smernice Európskeho parlamentu a Rady o výmene informácií medzi orgánmi presadzovania práva členských štátov, ktorou sa zrušuje rámcové rozhodnutie Rady 2006/960/SVV (Ú. v. EÚ COM(2021) 782 final, 8. 12. 2021).

Návrh zákona o kybernetickej bezpečnosti (Ú. v. EÚ COM(2017) 477 final, 13. 9. 2017).

Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu C(2017)6100 (Ú. v. EÚ L 239/36, 19. 9. 2017).

Odporúčanie Komisie (EÚ) 2018/334 z 1. 3. 2018 o opatreniach na účinný boj proti nezákonnému obsahu na internete (Ú. v. EÚ L 63/50, 6. 3. 2018).

Odporúčanie Komisie z 18. októbra 2017 o okamžitých krokoch na zabránenie zneužívania prekurzorov (Ú. v. EÚ L 273/12, 24.10.2017) a Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1148 z 20. júna 2019 o uvádzaní prekurzorov výbušnín na trh a ich používaní, ktorým sa mení nariadenie (ES) č. 1907/2006 a ktorým sa zrušuje nariadenie (EÚ) č. 98/2013 (Ú. v. EÚ L 186/1, 11. 7. 2019).

Odporúčanie Rady z 8. decembra 2022 o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry 2023/C 20/01 (Ú. v. EÚ C 20/1, 20. 1. 2023).

Oznámenie Komisie Európskemu parlamentu a Rade o akčnom pláne na posilnenie boja proti financovaniu terorizmu (Ú. v. EÚ COM(2016) 50 final, 2. 2. 2016).

Oznámenie Komisie Európskemu parlamentu a Rade: Európska stratégia energetickej bezpečnosti (Ú. v. EÚ COM(2014) 0330 final).

Oznámenie Komisie Európskemu parlamentu a Rade: Stratégia vnútornej bezpečnosti EÚ: päť krokov k bezpečnejšej Európe (Ú. v. EÚ KOM(2010) 673 v konečnom znení, 22. 11. 2010).

Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov o stratégii EÚ pre bezpečnostnú úniu (Ú. v. EÚ COM/2020/605 final, 24. 7. 2020).

Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Ustanovenia Komisie o spoločnom systéme rýchleho varovania „ARGUS“ (Ú. v. EÚ KOM(2005) 662 v konečnom znení, 23. 12. 2005).

Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Európsky program v oblasti bezpečnosti (Ú. v. EÚ COM(2015) 185 final, 28. 4. 2015).

Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: o akčnom pláne pre európsku demokraciu (Ú. v. EÚ COM(2020) 790 final, 3. 12. 2020).

Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Boj proti dezinformáciám na internete: európsky prístup (Ú. v. EÚ, COM(2018) 236 final, 26. 4. 2018).

Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru, Výboru regiónov a Európskej investičnej banke: „Rámcová stratégia odolnej energetickej únie s výhľadovou politikou v oblasti zmeny klímy“ (Ú. v. EÚ COM(2015) 080 final).

Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Protidrogový program a akčný plán EÚ na boj proti drogám na roky 2021 – 2025 (Ú. v. EÚ COM(2020) 606, 24. 7. 2020).

Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Obnovený akčný plán EÚ proti prevádzačstvu migrantov (2021 – 2025) (Ú. v. EÚ COM(2020) 606 final, 29. 9. 2021).

Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Akčný plán EÚ na boj proti nedovolenému obchodovaniu so strelnými zbraňami na roky 2020 – 2025 (Ú. v. EÚ COM(2020) 608 final, 24. 7. 2020).

Oznámenie Komisie o Európskom programe na ochranu kritickej infraštruktúry (Ú. v. EÚ KOM/2006/0786 v konečnom znení, 12. 12. 2006).

Oznámenie Komisie Rade a Európskemu Parlamentu: Ochrana najdôležitejšej infraštruktúry v boji proti terorizmu (Ú. v. EÚ KOM/2004/0702 v konečnom znení, 20.10. 2004).

Oznámenie Komisie Rade a Európskemu parlamentu: Riešenie otázok trestnej činnosti v digitálnom veku: zriadenie európskeho centra boja proti počítačovej kriminalite (Ú. v. EÚ COM(2012) 140 final, 28. 3. 2012).

Oznámenie M ZV SR č. 137/2008 Z. z. Dohovor o počítačovej kriminalite.

RADA PRE MEDIÁLNE SLUŽBY, 2023. *Globálne internetové fórum na boj proti terorizmu (GIFCT).* [online]. [cit. 2023-07-03]. Dostupné na internete: https://rpms.sk/globalne-internetove-forum-na-boj-proti-terorizmu-gifct.

RADAR EUROPE, 2023. *Radicalisation Awareness Network (RAN).* [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.radareurope.nl/themes/ran-coe/.

Rámcové rozhodnutie Rady z 13. júna 2002 o boji proti terorizmu 2002/475/SVV (Ú. v. EÚ L 164, 22. 6. 2002), pozmenené rámcovým rozhodnutím Rady 2008/919/SVV z 28. novembra 2008, ktorým sa mení a dopĺňa rámcové rozhodnutie 2002/475/SVV o boji proti terorizmu (Ú. v. EÚ L 330, 9. 12. 2008).

Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Ú. v. EÚ L 347/924, 20. 12. 2013).

Rozhodnutie Rady 2007/845/SVV o spolupráci medzi úradmi pre vyhľadávanie majetku v členských štátoch pri vypátraní a identifikácii príjmov z trestnej činnosti alebo iného majetku súvisiaceho s trestnou činnosťou (Ú. v. EÚ L 332/103, 18. 12. 2007).

Rozhodnutie Rady 2008/615/SVV z 23. júna 2008 o zintenzívnení cezhraničnej spolupráce, najmä v boji proti terorizmu a cezhraničnej trestnej činnosti (Ú. v. EÚ L 210/1, 6. 8. 2008).

Rozhodnutie Rady z 26. júla 2010 o organizácii a fungovaní Európskej služby pre vonkajšiu činnosť (2010/427/EÚ) (Ú. v. EÚ L 201/30, 3. 8. 2010).

Sixth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (Ú. v. EÚ SWD(2022) 308 final, 16. 9. 2022).

Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode). (Ú. v. EÚ L 178, 17. 7. 2000).

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 (Ú. v. EÚ L 194/1, 19. 7. 2016).

Smernica Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV (Ú. v. EÚ L 88/6, 31. 3. 2017).

Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV (Ú. v. EÚ L 123/18, 10. 5. 2019).

Smernica Európskeho parlamentu a Rady 2008/99/ES z 19. novembra 2008 o ochrane životného prostredia prostredníctvom trestného práva (Ú. v. EÚ L 328/28, 6. 12. 2008).

Smernica Európskeho parlamentu a Rady 2014/42/EÚ z 3. apríla 2014 o zaistení a konfiškácii prostriedkov a príjmov z trestnej činnosti v Európskej únii (Ú. v. EÚ L 127/39, 29. 4. 2014).

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 (Ú. v. EÚ L 194/1, 19. 7. 2016).

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (Ú. v. EÚ L 333/164, 27. 12. 2022).

Smernica Európskeho parlamentu a Rady 2010/13/EÚ z 10. marca 2010 o koordinácii niektorých ustanovení upravených zákonom, iným právnym predpisom alebo správnym opatrením v členských štátoch týkajúcich sa poskytovania audiovizuálnych mediálnych služieb (smernica o audiovizuálnych mediálnych službách) (kodifikované znenie). (Ú. v. EÚ L 95/1, 15. 4. 2010).

Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17. 12. 2011).

Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218/8, 14. 8. 2013).

Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23. 12. 2008).

Smernica Rady 2009/71/Euratom z 25. júna 2009, ktorou sa zriaďuje rámec Spoločenstva pre jadrovú bezpečnosť jadrových zariadení, zmenená smernicou Rady 2014/87/Euratom z 8. júla 2014. Na tomto úseku bol prijatý Akčný plán na zlepšenie pripravenosti na chemické, biologické, rádiologické a jadrové bezpečnostné riziká (Ú. v. EÚ COM(2017) 610 final, 18. 10. 2017).

Smernica Rady 2013/59/Euratom z 5. decembra 2013, ktorou sa stanovujú základné bezpečnostné normy ochrany pred nebezpečenstvami vznikajúcimi v dôsledku ionizujúceho žiarenia, a ktorou sa zrušujú smernice 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom a 2003/122/Euratom (Ú. v. EÚ L 13/1, 17. 1. 2014).

Spoločné oznámenie Európskemu parlamentu a Rade o aktualizácii stratégie námornej bezpečnosti EÚ a jej akčného plánu „Posilnená stratégia námornej bezpečnosti EÚ pre vyvíjajúce sa námorné hrozby" (Ú. v. EÚ JOIN (2023) 8 final, 10. 3. 2023).

Spoločné oznámenie Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ, ktorým bola vymedzená širšia stratégia EÚ (Ú. v. EÚ JOIN(2017) 450 final, 13. 9. 2017).

Spoločné oznámenie Európskemu parlamentu a Rade: Spoločný rámec pre boj proti hybridným hrozbám reakcia Európskej únie (Ú. v. EÚ JOIN/2016/018 final, 6. 4. 2016).

Spoločné oznámenie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a výboru regiónov: Akčný plán proti dezinformáciám (Ú. v. EÚ JOIN(2018) 36 final, 5. 12. 2018).

Spoločné oznámenie Európskemu parlamentu, Európskej rade a Rade: Zvyšovanie odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby (Ú. v. EÚ JOIN/2018/16 final, 13. 6. 2018).

Spoločné oznámenie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor (Ú. v. EÚ JOIN/2013/01 final).

Spoločné rozhodnutie Európskej komisie a vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku o účasti EÚ v rôznych organizáciách pre spoluprácu pri predchádzaní terorizmu a boji proti nemu (Ú. v. EÚ JOIN(2015) 32 final, 27. 8. 2015).

Správa Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov o vykonávaní oznámenia „Boj proti dezinformáciám na internete: európsky prístup“ (Ú. v. EÚ COM(2018) 794 final, 5. 12. 2018).

STATEWATCH, 2015. *The EU Intelligence Analysis Centre*. [online]. [cit. 2023-07-03]. Dostupné na internete: https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf.

Stratégia vnútornej bezpečnosti na roky 2010 – 2014 bola revidovaná Európskym programom v oblasti bezpečnosti na roky 2015 – 2020 (Ú. v. EÚ COM(2015) 185 final, 28. 4. 2015).

Strategický kompas pre bezpečnosť a obranu – za Európsku úniu, ktorá chráni svojich občanov, hodnoty a záujmy a prispieva k medzinárodnému mieru a bezpečnosti. (Ú. v. EÚ ST/7371/22, 21. 3. 2022).

TF-CSIRT, 2019. *Services for Security and Incident Response Teams.* [online]. [cit. 2023-07-03]. Dostupné na *internete: https://www.trusted-introducer.org/.*

Uznesenie Európskeho parlamentu z 23. novembra 2016 o strategickej komunikácii EÚ s cieľom bojovať s propagandou tretích strán zameranou proti Únii (2016/2030(INI)) (Ú. v. EÚ C 224/58, 27. 6. 2018).

Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy [online]: Projekt podporený z Európskeho sociálneho fondu. Operačný program Efektívna verejná správa. Prijímateľ MV SR. Kód projektu ITMS2014+: 314011CDW7.

Keywords: hybrid threat, strategy, security strategy, defence strategy, action plan, cybersecurity, security environment, security system, risk management, crisis situation, disinformation, EUROPOL, FRONTEX, EUROJUST, CEPOL, East StratCom, European External Action Service, EU Intelligence and Situation Centre, EU Intelligence Analysis Centre, European Centre of Excellence for Countering Hybrid Threats

Summary

Countering hybrid threats has been at the forefront of the EU security policy for the past 20 years, as evidenced by the extensive legislative and institutional framework that is constantly evolving and responding to changing challenges in the global security environment. In terms of the direction of the security policy of the EU Member States, in the horizon until 2030, it is possible to expect an escalation of efforts, a higher extent of coordination of activities at the political, military, security, judicial, technical, and social level.

pplk. doc. JUDr. Monika Hullová, PhD.
Akadémia Policajného zboru v Bratislave
Katedra kriminálnej polície
e-mail: monika.hullova@akademiapz.sk

Recenzenti: doc. Ing. Stanislav Šišulák, PhD., MBA, JUDr. Juraj Drugda, PhD.