Evropská unie a hybridní hrozby: pozice Česka a výzvy, příležitosti či budoucnost evropské demokracie

Pavel Havlíček, Lukáš Horák

Shrnutí

→ ČR i EU v posledních letech čelí stále silnějšímu hybridnímu působení ze strany třetích stran, a to také v domácím prostředí v součinnosti s domácími proxy aktéry vystupujícími v zájmu cizí moci. Tento fakt souvisí především se stále více agresivním chování Ruské federace nejen vůči Ukrajině, ale také západnímu společenství jako celku.

→ Tyto výzvy, navíc umocněné proměnou informačního světa pod vlivem digitálních i AI technologií, mají přitom zásadní vliv na fungování západních demokracií i jejich vnitřní procesy, včetně voleb, referend a dalších procesů zapojování veřejnosti do veřejných politik státu, které se cizí moci snaží stále intenzivněji ovlivňovat.

→ V této souvislosti podkladový dokument analyzuje a popisuje hlavní výzvy pro ČR i EU a také navrhuje, co všechno by se mělo změnit, aby reakce evropského společenství na tato rizika a výzvy byla efektivnější a dokázala protivníky a soupeře Evropy od budoucího konání odradit. Proto publikace klade na přední místo tzv. asymetrickou reakci přinášející novou kvalitu odvetné reakce i nákladů za vedení hybridních operací.

→ Zvláštní pozornost autoři věnují ochraně demokratických procesů a integritě voleb, která je v poslední době stále častěji zpochybňována jak ze strany vnějších aktérů, tak hráčů na domácím politickém poli. Zároveň se zabývají rolí občanské společnosti a připraveností na krize, ale také silnějším zapojením občanů do řešení těchto krizí.

→ Podkladový dokument navazuje taktéž na trendy na evropské úrovni a snaží se propojit českou diskuzi s posledním vývojem v rámci EU rámovaným především politicky exponovanou zprávou bývalé ho finského prezidenta Sauli Niinistöho, která uvedla do pohybu řadu navazujících procesů, včetně v oblasti krizové připravenosti či užší spolupráce mezi evropskými členskými státy v oblasti vnitřní i vnější bezpečnosti.

Úvod

Hybridní hrozby představují jednu z nejdynamičtějších a nejzávažnějších bezpečnostních výzev současnosti pro Evropskou unii (EU) i její členské státy, včetně České republiky.[1] Moderní hybridní hrozby přesahují rámec tradičních vojenských konfliktů a zasahují širokou škálu oblastí – od kognitivních informačně-psychologických operací, dezinformací a propagandy, přes působení v kyberprostoru, ekonomickém sektoru a sektoru kritické infrastruktury a informačních systémů, až po kulturně-společenské vměšování, realizaci cílených sabotáží a ovlivňování demokratických procesů a voleb. V posledních letech došlo k výraznému nárůstu hybridních operací, které jsou realizovány především autoritářskými režimy, zejména Ruskou federací (RF) a Čínskou lidovou republikou (ČLR), které pro členské státy EU představují aktuálně nejvýznamnější hrozbu.

RF eskalovala své hybridní aktivity zejména v návaznosti na plnohodnotnou invazi na Ukrajinu v roce 2022 a systematicky usiluje o destabilizaci evropských společností.[2] Významnou hrozbou se stávají pokusy o ovlivňování demokratických voleb, přičemž nedávné případy vměšování do volebních kampaní v několika členských státech EU, včetně Německa, Polska nebo Rumunska, ukazují na narůstající koordinaci a intenzitu těchto vlivových aktivit, zejména ze strany RF. Hrozba ovlivnění demokratických procesů je v posledních letech aktuální i v ČR,[3] kde v říjnu 2025 proběhnou volby do Poslanecké sněmovny. Zde existuje riziko zvýšené vlny dezinformačních kampaní, kybernetických útoků na volební infrastrukturu a manipulace veřejného diskurzu.

Vedle zasahování do voleb ruské hybridní operace zahrnují také kybernetické útoky na státní instituce, zdravotnická zařízení, dopravní a energetickou infrastrukturu. Skryté sabotáže zaměřené na kritické uzly evropské infrastruktury, včetně plynovodů, telekomunikačních sítí a podmořských kabelů, představují novou formu asymetrického konfliktu, jehož původci často využívají obtížné přímé přiřazení útoku k odpovědnému aktérovi.[4] Paralelně s tím ruské dezinformační kampaně soustavně zintenzivňující existující štěpící linie, a tím rozkládají evropské společnosti zevnitř, podkopávají důvěru veřejnosti v demokratické instituce, šíří společenskou polarizaci a podporují extremistické narativy. Konkrétním případem z minulého roku je například aféra kolem serveru Voice of Europe, který za peníze z Ruska systematicky poskytoval prostor pro krajně pravicové a levicové evropské politiky před volbami do Evropského parlamentu v červnu 2024.[5]

Specifickým rysem hybridních hrozeb vycházejících z ČLR je sofistikované využívání ekonomických nástrojů, legislativních kliček a kulturní diplomacie. ČLR prostřednictvím investic do kritické infrastruktury, pokročilých technologií, datových center a ICT řešení upevňuje svůj vliv v Evropě, přičemž takové investice často nesou bezpečnostní rizika v podobě možnosti narušení klíčových systémů nebo neoprávněného přístupu k citlivým datům. Paralelně s tím ČLR rozšiřuje své kulturní působení skrze Konfuciovy instituty a další kulturní a vzdělávací organizace, které

[1] Lukáš Marek, „Sabotáže jsou krajním činem. Ani Sověti si na ně netroufli, říká expertka", *Seznam zprávy*, 12. 5. 2025, https://www.seznamzpravy.cz/clanek/zahranicni-sabotaze-jsou-krajnim-cinem-ani-soveti-si-na-ne-netroufli-rika-expertka-275856.

[2] Joe Stanley-Smith, „Russia burned down Warsaw's biggest mall, Tusk says", *Politico Europe*, 11. 5. 2025, https://www.politico.eu/article/russia-warsaw-poland-fire-donald-tusk/.

[3] Bezpečnostní informační služba, „Výroční zpráva 2023", 12. 9. 2024, https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2023-vz-cj.pdf.

[4] Benjamin L. Schmitt, Michal Kurtyka and Alan Riley, „Underwater Maybem", Vol. 1., *Penn – University of Pennsylvania*, https://upenn.app.box.com/s/wvrobfk9j1h34agng36chj73ibtkcxoh.

[5] Vojtěch Berger, „Měsíc s kauzou Voice of Europe. Co víme s jistotou a kdo stále vyrábí „mlhu", *Hlídací pes*, 7. 5. 2024, https://hlidacipes.org/mesic-s-kauzou-voice-of-europe-co-vime-s-jistotou-a-kdo-stale-vyrabi-mlhu/.

slouží nejen k propagaci čínské kultury, ale také k prosazování ideologických a politických zájmů čínského režimu.

EU v posledních letech výrazně zintenzivnila svou reakci na narůstající hybridní hrozby, které vnímá jako jednu z hlavních výzev pro svou bezpečnost a stabilitu. Přijetím Strategického kompasu pro bezpečnost a obranu v roce 2022 EU jasně definovala potřebu koordinovaného a proaktivního přístupu k hybridním útokům, [6] včetně dezinformací, kybernetických útoků, nátlaku na kritickou infrastrukturu a zahraničního vměšování. V návaznosti na něj vznikl komplexní rámec opatření známý jako „hybridní toolbox", který propojuje různé nástroje – od sdílení informací přes právní a ekonomické nástroje až po nasazení expertních týmů rychlé reakce.

V souladu s tímto přístupem EU rozšiřuje právní rámec pro obranu kritických oblastí – od kybernetické bezpečnosti (směrnice NIS2) přes ochranu infrastruktury (směrnice CER) až po omezení zahraničních vlivů na politický proces (Balíček na obranu demokracie). Posiluje také dohled nad digitálním prostředím skrze nová pravidla pro online platformy (nařízení DSA), rozvíjí schopnost strategické komunikace a zavádí cílené sankce proti pachatelům hybridních útoků. Tento vícevrstvý přístup odráží rostoucí potřebu chránit evropské demokratické instituce, ekonomiku i informační prostor před komplexními a koordinovanými hrozbami.

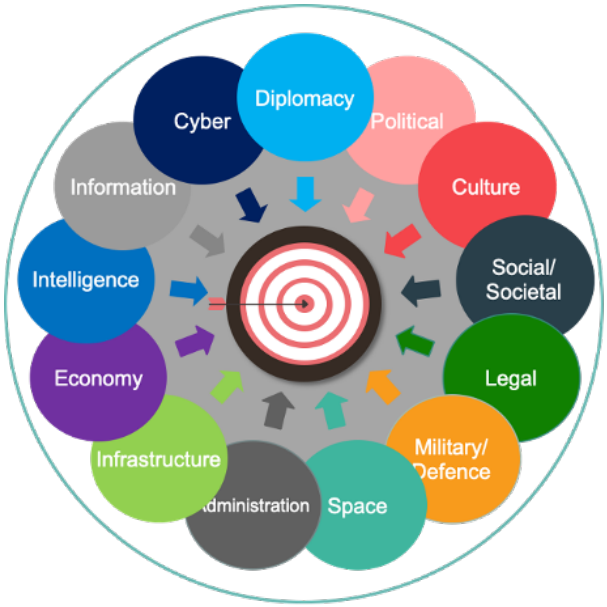
Pro Českou republiku znamená čelení hybridním hrozbám klíčovou výzvu nejen v ochraně vlastních demokratických procesů, ale i v aktivním podílu na evropské odpovědi. Sněmovní volby v roce 2025 budou testem schopnosti českého státu odolat pravděpodobným hybridním hrozbám a vlivovým aktivitám ze zahraničí. Proto je zásadní posílit ochranu volební infrastruktury, připravenost bezpečnostních složek a veřejných institucí, zvýšit mediální a digitální gramotnost občanů a systematicky pracovat na budování celospolečenské odolnosti. Česká republika by zároveň měla aktivně podporovat posilování evropských kapacit v boji proti hybridním hrozbám a prosazovat koordinovanou, efektivní a proaktivní bezpečnostní politiku v rámci celé Evropské unie.

[6] Evropská rada – Rada Evropské unie, „Strategický kompas pro bezpečnost a obranu" https://www.consilium.europa.eu/cs/policies/strategic-compass/.

1 Jaké konkrétní typy hybridních hrozeb představují největší riziko pro EU a ČR?

Hybridní hrozby jsou charakterizovány kombinací konvenčních i nekonvenčních nástrojů, jejichž cílem je celkové oslabení protivníka bez přímé vojenské konfrontace. Největší riziko pro Evropskou unii a Českou republiku představují v současnosti hybridní aktivity RF a ČLR, ale nelze opomenout ani rostoucí zapojení dalších států, jako je Írán nebo Severní Korea, stejně jako nestátních aktérů a proxy aktérů. Aktéři hybridních hrozeb pro realizaci těchto aktivit využívají veškeré dostupné strategické domény a spektra, které Evropské centrum excelence pro boj s hybridními hrozbami shrnuje v následujícím schématu:

Schéma č. 1: Konceptuální oblasti hybridních hrozeb



Zdroj: The Landscape of Hybrid Threats, European Hybrid CoE in Finland, 2021

Hybridní hrozby vedené proti členským státům EU a instituci jako takové lze rozdělit do několika klíčových kategorií, které se navzájem prolínají a jejichž účinky se synergicky zesilují.

Kybernetické útoky a sabotáže kritické infrastruktury

Kybernetické útoky patří k nejrychleji se rozvíjejícím formám hybridního působení. RF i ČLR investují značné prostředky do kybernetických kapacit, které jsou využívány jak pro masivní shromažďování informací a špionáž, tak pro narušení klíčových systémů cílových států a s tím související vyvolání chaosu a podkopání důvěry občanů v ochranu vlastního státu. Typické jsou útoky zaměřené na vládní instituce a veřejný sektor (veřejné služby), nemocnice, finanční sektor, média či energetickou a síťovou infrastrukturu.

V posledních dvou letech došlo k několika vážným incidentům, které ukázaly, jak snadno lze prostřednictvím kyberútoků paralyzovat důležité služby.[7] Kromě klasických kyberšpionážních aktivit, které již v minulosti českou národní bezpečnostní zásadním způsobem ohrozily,[8] se zvyšuje i riziko skrytých sabotáží,

[7] MZV, „Prohlášení MZV ke kyberútokům ruského aktéra APT28 na Česko“, 3. 5. 2024, https://mzv.gov.cz/jnp/cz/udalosti_a_media/tiskove_zpravy/prohlaseni_mzv_ke_kyberutokum_ruskeho.html.

[8] MZV, „Prohlášení vlády České republiky“, 28. 5. 2024, https://mzv.gov.cz/jnp/cz/udalosti_a_media/tiskove_zpravy/prohlaseni_vlady_ceske_republiky.html.

například útoky na energetické sítě, telekomunikační kabely či podmořské infrastruktury. Výbuchy plynovodů Nord Stream v roce 2022 či nedávné incidenty se zpřetrhanými podmořskými kabely mezi Finskem a Estonskem ukazují, jak závažné dopady mohou takové útoky mít na evropskou bezpečnost.

ČR jakožto otevřená a digitalizovaná společnost – avšak v této souvislosti bez dostatečné míry ochrany proti hrozbám – je v tomto ohledu zvláště zranitelná. Ochrana klíčové infrastruktury a posilování kyberbezpečnostní odolnosti představují proto absolutní prioritu v boji proti hybridním hrozbám.

Dezinformační a informačně-psychologické aktivity

Informační doména je klíčovým prostorem soudobé hybridní války. Dezinformační kampaně, kognitivní manipulace, šíření falešných zpráv a cílené ovlivňování veřejného mínění patří mezi hlavní nástroje hybridních aktérů.

Ruské dezinformační operace, vedené např. prostřednictvím státních médií jako RT a Sputnik, soukromých aktérů jako SDA (Social Design Agency),[9] proxy serverů a sociálních sítí, jsou zaměřeny na rozkládání společenské soudržnosti a oslabování důvěry v demokratické instituce a evropské hodnoty. Často využívají aktuální témata (migrace, energetická krize, ruská agresivní válka na Ukrajině) a snaží se je zneužívat a interpretovat způsobem, který podporuje cynismus, extremismus, nedůvěru a antisystémové nálady vzhledem k institucím státu.

Čínská strana naproti tomu v informačním prostoru postupuje sofistikovaněji a v dlouhodobějším časovém horizontu,[10] zaměřuje se zejména na formování dlouhodobě pozitivního obrazu Číny a minimalizaci kritiky její politiky, například v oblasti lidských práv. Tento přístup je patrný zejména na akademické půdě, v kulturní diplomacii a skrze mediální spolupráce.[11]

Pro ČR představují zahraniční dezinformační operace zásadní riziko, neboť mohou přímo ovlivnit volební výsledky, polarizovat společnost a oslabit odolnost státu vůči dalším hybridním útokům a malignímu vlivovému působení.

Ekonomické a technologické hybridní hrozby

Ekonomická oblast je dalším klíčovým prostorem pro hybridní operace. ČLR využívá investice do strategických sektorů, jako je energetika, telekomunikace nebo datová centra, k posilování svého geopolitického vlivu v Evropě. Tato strategie je založena na plíživém budování ekonomické závislosti, využívání ekonomické a technologické domény pro špionáž a využívání legislativních kliček k získávání kontroly nad klíčovými technologickými a infrastrukturními aktivy.[12]

Podobné riziko představují i ruské ekonomické operace, zejména v oblasti energetiky, kde Moskva tradičně využívá dodávky plynu a ropy jako nástroje politického nátlaku.

Pro Česko je v této oblasti klíčové důsledně aplikovat principy screening mechanismu zahraničních investic EU a provádět vlastní bezpečnostní hodnocení projektů v sektorech s vysokou citlivostí.

---

[9] Psychological Defence Research Institute, „Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency“, *Lund University*, 15 May 2025, https://www.psychologicaldefence.lu.se/article/beyond-operation-doppelganger-capability-assessment-social-design-agency.

[10] R. A. Khairunnisa, „Strengthening China's soft power through public diplomacy: NGOs as important players“, *Modern Diplomacy*, 2024 https://moderndiplomacy.eu/2024/02/04/strengthening-chinas-soft-power-through-public-diplomacy-ngos-as-important-players/.

[11] C. Zanardi, China's soft power with Chinese characteristics: The cases of Confucius Institutes and Chinese naval diplomacy, *Journal of Political Power*, 9(3), 431–447. 2016, https://doi.org/10.1080/2158379X.2016.1232289.

[12] David Tramba, „Spolupráce Rusů s Maďary vázne. První blok elektrárny Paks měl být letos hotový, ale teprve se začal stavět“, *Ekonomický deník*, 24. 8. 2023, https://ekonomickydenik.cz/spoluprace-rusu-s-madary-vazne-prvni-blok-elektrarny-paks-2-mel-byt-letos-hotovy-ale-jeste-se-nezacal-stavet/.

Kulturní a společenské vlivové operace

Kulturně-společenské hybridní působení je tradiční doména ČLR, která svoji sílu v této doméně projevuje v řadě států, jež jsou branami do EU, jako např. v Itálii či v kandidátských státech regionu západního Balkánu. ČLR velice umně využívá kulturní diplomacii jako nástroj vlivových operací. Zakládání Konfuciových institutů a jiných kulturních center je součástí širší strategie, která má za cíl ovlivňovat veřejné mínění, prosazovat čínskou agendu a eliminovat kritiku režimu. Tyto instituce mohou sloužit i jako platformy pro sběr informací a budování sítí vlivu.

Ruská federace po této linii působí méně výrazně, nicméně také pro své působení využívá ruské kulturní instituce či náboženské organizace jako např. infrastrukturu ortodoxní církve. Zatímco ČLR využívá své kulturní instituce jako přímý nástroj socio-kulturního ovlivňování a působení, RF tyto instituce využívá primárně jako prostředek realizace hybridních útoků či jako podpůrnou infrastrukturu pro realizaci zpravodajských operací, skrytých sabotáží a dalších asymetrických operací, ideálně pod vlajkou kulturně-náboženských a „nedotknutelných" institucí.[13]

V evropském prostoru byl v posledních letech zaznamenán rostoucí trend v počtech případů, kdy je kulturní nebo náboženská činnost zneužívána k prosazování cílů zahraničních mocností, včetně špionáže a podpory zpravodajských aktivit a operací, pokusů o rozklad komunitní soudržnosti a šíření ideologicky motivovaných narativů. ČR by měla věnovat zvýšenou pozornost monitorování těchto aktivit, zejména v oblasti akademické svobody, kultury a vzdělávání.

[13] Vinohradská 12, „Ruští agenti na faře v Karlových Varech: Domlouvali se na akcích v Evropě, tvrdí novinář Respektu", *Český rozhlas Plus*, 19. 12. 2024, https://plus.rozhlas.cz/rusti-agenti-na-fare-v-karlovych-varech-domlouvali-se-na-akcich-v-evrope-tvrdi-9376991.

2 Jak by se vůči hybridním hrozbám měla EU chránit a jaké priority by měla v této oblasti prosazovat Česká republika? Jaké překážky brání efektivnější spolupráci mezi členskými státy navzájem a mezi nimi a institucemi EU?

EU v uplynulých letech přijala řadu klíčových iniciativ, které tvoří základ její obranné architektury vůči hybridním hrozbám. Jejich účinnost však závisí na důsledné implementaci zejména ze strany členských států, posilování synergií mezi členskými státy a zvýšení flexibility a rychlosti rozhodovacích procesů.

Strategické rámce a budování kapacit

Zásadním krokem bylo přijetí **Strategického kompasu pro bezpečnost a obranu** v roce 2022 jako základního strategického dokumentu pro společnou bezpečnostní a obrannou politiku EU, podpořeného následně i Evropskou radou. Kompas hybridní hrozby jednoznačně zařadil mezi hlavní bezpečnostní priority EU a stanovil potřebu posílit schopnosti v oblasti odhalování, odolnosti a reakce na hybridní operace.

Na tomto základě následně vznikl tzv. **Hybridní toolbox** – sada nástrojů, které členským státům a institucím EU umožňují lépe detekovat hybridní aktivity, sdílet informace, koordinovat reakce a využívat politické, diplomatické, ekonomické a právní prostředky ke snižování hybridních hrozeb.[14] Toolbox se ukázal jako klíčový při rychlé podpoře států čelících hybridním hrozbám, například vysláním **Hybridního týmu rychlé reakce (HRRT)** do Moldavska. Krátkodobě vyslaný tým může stejně tak pomoct s (preventivním) budováním odborných kapacit v členském státě, jako i akutně řešit existující hybridní hrozbu. Dalším nástrojem v toolboxu je např. systém včasného varování, který pomáhá při rozsáhlých útocích napříč státy nebo sektory.

V oblasti kyberbezpečnosti EU aktualizovala právní rámec prostřednictvím **směrnic NIS2**[15] a vytvořila **CER**,[16] které zvyšují ochranu strategických sektorů, jako jsou energetika, doprava, zdravotnictví a digitální infrastruktura. Dále byl zaveden **screening zahraničních investic (FDI Screening)** pro ochranu kritických aktiv před nepřátelskými převzetími ze strany autoritářských režimů.

Budování vlastní technologické suverenity, například prostřednictvím projektů jako **Gaia-X** (evropský cloud) nebo standardizace bezpečných 5G sítí (EU 5G Toolbox), má rovněž zásadní význam pro snížení zranitelnosti vůči hybridním operacím.

Rychlá a efektivní reakce

Hybridní operace mají často charakter rychlých, obtížně atribuovatelných útoků,[17] které vyžadují promptní reakci. EU proto rozvíjí kapacity pro **rychlé nasazení**

[14] European Council – Council of the European Union, „Council conclusions on a Framework for a coordinated EU response to hybrid campaigns," https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/.

[15] European Union, „Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union", https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[16] European Union, „Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities", https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

[17] NÚKIB, „Národní strategie kybernetické bezpečnosti ČR", str. 14, https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf.

expertních týmů v případě hybridních incidentů, jako jsou např. zmíněné HRRT, a podporuje zlepšení krizového řízení na národní i unijní úrovni.

Fungující Systém rychlého varování (**Rapid Alert System, RAS)** umožňuje sdílení informací o hybridních incidentech v reálném čase mezi členskými státy a institucemi EU. V návaznosti na zkušenosti s hybridními hrozbami ze strany Ruska EU postupně začíná také využívat možnost sankcí jako nástroje rychlé reakce na hybridní útoky – například v případě sankcionování konkrétních osob, institucí či proxy aktérů odpovědných za hybridní operace.

Významným posunem je rostoucí akceptace principu „**naming and shaming**", tedy veřejného přiznání odpovědnosti konkrétních aktérů za hybridní útoky,[18] v kombinaci s uplatněním diplomatických a ekonomických nástrojů odstrašování.

Ochrana demokratických procesů a **budování společenské odolnosti** jsou jako významné prvky evropské reakce na hybridní hrozby rozpracovány do větší míry detailu níže.

2.1 České priority v boji proti hybridním hrozbám

Aby mohla ČR hybridním výzvám efektivně čelit, musí formulovat jasné priority zaměřené na budování odolnosti, ochranu demokratických procesů a aktivní přispívání k posilování společné evropské bezpečnosti.

V první řadě by ČR měla aktivně vstupovat do tvorby a implementace evropských politik v oblasti hybridních hrozeb. Neměla by se stát pouze pasivním příjemcem evropských opatření a návrhů, ale měla by pokračovat ve své aktivní roli spolutvůrce a hybatele dané problematiky. ČR by proto měla vykazovat aktivní účast na rozpracování a využívání hybridního toolboxu, zapojení do operativního nasazování HRRT a důsledné prosazování nástrojů Balíčku na obranu demokracie a Evropského štítu pro demokracii. Právě tam může ČR svými zkušenostmi významně přispět. V evropských strukturách by měla podporovat rozvoj schopností pro rychlou krizovou reakci, lepší sdílení informací o hybridních incidentech a zefektivnění koordinačních mechanismů mezi členskými státy a institucemi EU.

Na národní úrovni musí Česko věnovat maximální pozornost posilování vlastní odolnosti, zejména v oblasti kybernetické bezpečnosti a ochrany kritické infrastruktury. Implementace směrnice NIS2 a směrnice CER musí být prováděna důsledně a v co nejkratším čase. Zajištění kybernetické ochrany sítí a systémů v sektorech jako energetika, doprava, zdravotnictví či informační technologie je nezbytné pro udržení fungování společnosti v případě hybridního útoku. Klíčovou roli zde hraje také budování kapacit v oblasti detekce a reakce na kybernetické incidenty, včetně investic do technologií, školení odborníků a rozvoje krizového řízení.

Ochrana demokratických procesů, zejména voleb, by měla patřit mezi absolutní priority. V souvislosti s nadcházejícími parlamentními volbami v říjnu 2025 je nutné zajistit bezpečnost volební infrastruktury, včetně elektronických systémů správy voleb či prevenci další delegitimizace volebního procesu.[19] Je nezbytné zavést opatření zajišťující maximální transparentnost financování politických stran a kampaní, stejně jako posílit monitoring a nástroje omezující prosazování možného zahraničního vlivu. Česko by mělo rovněž připravit krizové scénáře pro případ hybridního zasahování do voleb a využívat nástroje jako Systém rychlého varování (RAS) pro rychlou identifikaci a reakci na pokusy o manipulaci.

[18] Viz například zde, U.S. Embassy Prague, „Jejich zbraní je klávesnice, jejich cílem je chaos", https://x.com/usembassyprague/status/1920743171690008952?s=46&t=EEGIz3KpcycxRozMGiKOpA.

[19] iRozhlas.cz, „Češi se obávají volebních podvodů, ukazuje průzkum. Dvě třetiny pochybují o korespondenčních hlasech", 15. 5. 2025, https://www.irozhlas.cz/volby/cesi-se-obavaji-volebnich-podvodu-ukazuje-pruzkum-dve-tretiny-pochybuji-o_2505151317_mst.

Současně je důležité zaměřit se na posilování společenské odolnosti vůči dezinformacím a polarizačním narativům a dalším technikám. Hybridní hrozby nesměřují pouze proti institucím, ale míří přímo na veřejnost a její důvěru v demokratický systém. ČR by měla finanční i jiné zdroje investovat do programů na posílení mediální a digitální gramotnosti napříč celou společností, a to primárně skrze nestátní subjekty, tj. podpořit nezávislé fact-checkingové iniciativy a spolupracovat s občanskou společností, akademickou sférou i samosprávami na budování celospolečenské odolnosti. Důležitým prvkem je také posilování nezávislých médií, která hrají zásadní roli v ochraně informační integrity.

Pravděpodobně nejspornějším, ale v konečném důsledku kýženým bodem v této oblasti je aktivní centralizovaná obrana proti dezinformacím, jejich aktivní monitoring a realizace strategické reakce vůči propagandě s cílem uvádět tyto informace na pravou míru. Toto úsilí musí být aktivně řízené a legislativně dostatečně podpořené tak, ať se proti této hrozbě stát může bránit stejně efektivně jako např. proti fyzické sabotáži či kybernetickým útokům. A to samozřejmě za předpokladu nastavení kredibilních brzd a protivah do celého systému.

Další oblastí, kde by měla ČR hrát aktivní roli, je podpora společného evropského odstrašování hybridních aktérů. To znamená zapojit se do rychlého uplatňování sankcí proti jednotlivcům a entitám odpovědným za hybridní operace, prosazovat veřejné připisování odpovědnosti za hybridní útoky a podílet se na vytváření právních rámců umožňujících postih těchto operací. Aktivní přístup v této oblasti posílí nejen národní bezpečnost ČR, ale i její reputaci jako spolehlivého a odpovědného partnera v EU a NATO.

V kontextu hybridních hrozeb se ukazuje, že bezpečnost je dnes neoddělitelně propojena s ochranou demokracie, odolností společnosti a schopností reagovat na složité, kombinované a mnohdy skryté formy útoků. ČR by proto měla své kroky stavět na proaktivní, koordinované a hodnotově ukotvené bezpečnostní politice, která bude schopna čelit výzvám současnosti i budoucnosti.

2.2 Další praktické kroky a sektorová doporučení pro ČR

Vzhledem k rostoucímu počtu hybridních hrozeb, zejména ze strany RF, musí ČR přijmout konkrétní, cílená a systematická opatření, která budou reflektovat nejen doporučení domácí bezpečnostní a akademické komunity, ale také zkušenosti získané v dialogu s evropskými a mezinárodními partnery, včetně institucí jako je Evropské centrum excelence pro boj s hybridními hrozbami v Helsinkách. Z navrhovaných opatření vyplývá, že efektivní reakce ČR – a to i v rámci EU[20] – na hybridní hrozby musí být komplexní, proaktivní a zahrnovat všechny klíčové strategické domény – od informační bezpečnosti přes kyberprostor až po ekonomickou, politicko-diplomatickou a vojenskou oblast. Zároveň by měla naplňovat atributy zvyšování nákladů pro pachatele hrozeb v duchu tzv. asymetrické reakce postavené na záměru odradit útočníka prostřednictvím představení následků a nákladů v odpovědi na realizované hybridní operace a agresivní chování vůči evropským demokraciím.

V oblasti informačně-psychologických operací je zásadní veřejně a jednoznačně atribuovat hybridní útoky. ČR by měla aktivně zveřejňovat[21] konkrétní případy a subjekty zapojené do hybridního působení a tím zvyšovat informovanost veřejnosti i mezinárodních partnerů. Součástí této strategie by mělo být i aktivní zapojení do strategického informačního působení proti propagandě zahraničních aktérů, které by mělo systematicky vyvracet dezinformační narativy,

[20] Ondřej Ditrych and Steven Everts, „Unpowering Russia – How the EU Can Counter and Undermine the Kremlin", *EU ISS*, https://www.iss.europa.eu/sites/default/files/2025-05/CP_186.pdf.
[21] Joint Cybersecurity Advisory, „Russian GRU Targeting Western Logistics Entities and Technology Companies", March 2025, https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF.

oslabovat jejich účinnost a snižovat dopad maligního informačního vlivu na českou veřejnost. Klíčové je rovněž paralyzovat a sankcionovat prokazatelně propagandistická média a platformy působící na území ČR a v širším evropském prostoru.

V oblasti kybernetické bezpečnosti by ČR měla posílit schopnosti realizovat kybernetické protioperace, jejichž cílem by bylo paralyzovat identifikované maligní hybridní aktéry a minimalizovat jejich schopnost provádět kyberútoky proti ČR. Budování masivních kybernetických obranných kapacit je samozřejmostí, a toto doporučení bylo již adresováno výše.

Ve společensko-kulturní a politické doméně by ČR měla aktivně rozvíjet strategická partnerství se zeměmi Východního partnerství, jako je Ukrajina, Moldavsko nebo Gruzie. Podpora demokracie a občanské společnosti v těchto zemích představuje klíčový nástroj boje proti ruskému hybridnímu vlivu v širším evropském prostoru. Česká diplomacie by měla v rámci těchto aktivit flexibilně spolupracovat s podobně smýšlejícími partnery v EU i NATO.

V oblasti vojensko-bezpečnostní by ČR měla posílit schopnost skryté a polootevřené podpory aktérů,[22] kteří přímo bojují proti hybridnímu působení. Může jít jak o poskytování materiální pomoci, tak o zpravodajskou spolupráci. Je zásadní např. realizovat strategické zpravodajské operace zaměřené na identifikaci ruských zpravodajských důstojníků působících na českém území a jejich veřejnou diskreditaci. Dále by ČR měla podporovat vytvoření nové tréninkové mise EU pro Ukrajinu zaměřené na rozvoj kapacit k obraně proti hybridním hrozbám a zároveň aktivně přispívat k navyšování počtu společných vojenských cvičení EU a NATO podél hranic s RF.

Politicko-diplomatická a bezpečnostní opatření by měla zahrnovat obnovení dialogu se třetími zeměmi, zejm. s africkými státy v sektoru bezpečnosti a obrany s cílem omezit ruský a čínský geopolitický vliv na africkém kontinentu[23], který primárně RF využívá k financování svých operací a rozšiřování geopolitického vlivu. Tento přístup však nelze aplikovat na každý stát, protože pro některé z afrických režimů představuje RF a jeho působení, převážně ve formě žoldnéřů z Wagnerovy skupiny (tzv. Africa Corps), kritické garance jejich politického přežití. Na domácí evropské scéně je nutné významně omezit působení ruského diplomatického sboru a eliminovat jeho schopnost realizovat informačně-psychologické operace.

V neposlední řadě je nezbytné posílit ekonomicko-finanční nástroje boje proti hybridním hrozbám. ČR by měla aktivně podporovat zavádění tzv. „sekundárních sankcí" proti subjektům, které napomáhají ruskému hybridnímu působení nebo obcházejí sankce EU. Ať už jde o jednotlivce, firmy, či třetí státy. Dále je nutné cíleně zaměřit finanční a ekonomické sankce proti konkrétním aktérům hybridního působení a příslušníkům ruských silových resortů a zpravodajských služeb. Součástí této strategie by měla být také opatření zaměřená na systematické narušování finančních toků, které podporují hybridní operace vedené proti EU a jejím členským státům.

Komplexní realizace těchto opatření by výrazně posílila schopnost ČR čelit hybridním hrozbám a zároveň by přispěla k vyšší odolnosti EU jako celku. Efektivní boj proti hybridním operacím vyžaduje nejen silné národní kapacity, ale také úzkou koordinaci se spojenci a partnery na evropské a mezinárodní úrovni. Efektivita výše uvedených opatření je však podmíněna proaktivním chování evropských hráčů, kteří

[22] Respekt.cz, „(Ne)bezpečí Ondřeje Kundry – Jejich nepřátelé jsou naši přátelé. Jak Ukrajinci pomáhají bojovat s Rusy v Sýrii i Africe", 23. 12. 2024, https://www.respekt.cz/podcasty/jejich-nepratele-jsou-nasi-pratele-jak-ukrajinci-pomahaji-bojovat-s-rusy-v-syrii-i-africe?srsltid=AfmBOopvtzgfhQz37mbzIDg2GVknt8ZRbxxNce1aW6ZGCouzPIp-sZvo.

[23] Jacob Zenn, „China Sets Sight on Gabon for Second African Military Base", *Foreign Military Studies Office*, 15. 2. 2025, https://fmso.tradoc.army.mil/2025/china-sets-sight-on-gabon-for-second-african-military-base/.

se svými odpověďmi na hybridní působení až příliš dlouho otáleli a byli reaktivní, což se zpětně ukazuje jako chybné rozhodnutí.

3 Jak by měla EU chránit demokratické procesy a jak může aktivně přispět Česko?

Ovlivňování demokratických procesů, obzvláště voleb, představuje v současnosti jednu z nejvýznamnějších podob hybridních hrozeb pro západní demokracie. Zkušenosti z posledních let ukazují, že snahy zasahovat do volebních procesů a veřejné debaty v členských státech EU jsou systematické a intenzivní. RF, ČLR, Írán, Severní Korea i další aktéři přitom využívají sofistikované dezinformační kampaně často realizované proxy aktéry či privátními subjekty, financování spřátelených politických stran a organizací, kybernetické útoky na volební infrastrukturu a přímé snahy o manipulaci s veřejným míněním v cílových zemích.

Hrozby v této oblasti jsou podpořeny dlouhodobými dezinformačními kampaněmi, jejichž cílem je polarizovat společnost, zesilovat extremistické tendence a podkopávat důvěru ve státní instituce. Tyto aktivity mohou mít zásadní dopad na stabilitu politického systému nejen v jednotlivých členských státech, ale i na úrovni celé EU.

Nedávným příkladem aktuálních hrozeb tohoto typu je ruské vměšování se do evropských volebních kampaní v letech 2024 a 2025, zejména v Rumunsku, kde byly odhaleny pokusy o šíření dezinformací zaměřených na destabilizaci veřejné důvěry v demokratické instituce.[24] Jak v případě Rumunska, tak sousedního Polska nebo Německa se přitom ukázalo, že to byla zejména RF, která se ve volebních kampaních intenzivně angažovala, obzvláště skrze sociální sítě a online prostor, který není zdaleka tak regulován – a tím pádem ani kontrolován – jako v případě off-line či analogových médií. Ta přitom ve valné většině evropských států historicky podléhají poměrně striktním pravidlům.

S ohledem na nadcházející sněmovní volby v České republice v říjnu 2025 je pravděpodobné, že podobné snahy zasáhnou i český politický, společenský a informační prostor. S tímto fenoménem má ostatně ČR již zkušenosti, například s ohledem na tzv. kauzu lithium. Ta vznikla v roce 2017 na základě narativu původně zveřejněného dezinformačními médii, který později přebrali političtí hráči. Kromě toho Česko v tomtéž roce evidovalo i další, tentokrát kybernetický, útok proti serverům Českého statistického úřadu, který na čas vyřadil server volby.cz, což mělo za cíl znejistit sčítání hlasů, ale také podkopat důvěru v regulérnost sčítání hlasů.

3.1 Ochrana demokratických procesů

Balíček na obranu demokracie (Defence of Democracy Package) a připravovaný **Evropský štít pro demokracii (Democracy Shield)** představují důležité iniciativy, které:

- posilují transparentnost financování politických stran a kampaní,
- zavádějí mechanismy kontroly zahraničních vlivů,
- podporují mediální gramotnost a odolnost občanské společnosti.

Cílem je snížit zranitelnost evropských demokracií vůči manipulaci, zasahování do volebních procesů a šíření dezinformací. Významnou roli v této oblasti hraje **Akční plán proti dezinformacím**, který klade důraz na detekci falešných zpráv,

[24] Josef Šlerka, „Co víme o tiktokové kampani Călina Georgesca dnes? Průvodce krok za krokem“, *Investigace.cz*, 19. 5. 2025, https://www.investigace.cz/co-vime-o-tiktokove-kampani-calina-georgesca-dnes-pruvodce-krok-za-krokem/.

odhalování vlivových operací, snižování dosahu škodlivého obsahu a/nebo rychlou reakci na dezinformační kampaně.

Kromě toho byla po roce 2016 spuštěna řada dalších opatření, včetně Obecného nařízení o ochraně osobních údajů (GDPR), které mělo reagovat na masivní zneužívání osobních dat a informací v kampaních v anglosaském světě, včetně referenda o setrvání Spojeného království v EU či amerických prezidentských voleb. Daleko zásadněji, než pokusy o vměšování ze strany Ruska byly ovlivněny ze strany společnosti Cambridge Analytica, která pro potřeby politického boje vytvořila masivní databázi psychologických profilů amerických voličů a skrze sociální sítě docházelo k jejich manipulování tzv. *microtargetingem*, tedy cíleným doručováním propagovaných sdělení, a to přímo v masovém měřítku.

Právě rolí sociálních sítí a posílením jejich odpovědnosti za společenské procesy se zabývají evropská regulační opatření typu Aktu o digitálních službách (DSA),[25] Digital Markets Act (DMA)[26] nebo Data Act[27], které zásadním způsobem přenáší zodpovědnost za dění v online prostředí a zejména na tzv. velmi velkých platformách a vyhledávačích na dané komerční společnosti a ukládají jim nové povinnosti z hlediska chování v tržním prostředí, ale také zajištění integrity jejich služeb a prevence systémových rizik. Je to právě DSA, na jehož základě například Evropská komise dokázala síti TikTok nařídit zmrazit data o průběhu prezidentské volební kampaně v Rumunsku na konci roku 2024, případně jinak zakročit vůči digitálním gigantům zodpovědným za manipulaci s veřejným míněním v řadě evropských zemí. V poslední době navíc začalo docházet k poměrně masivnímu udělování pokut pro nedodržování evropského práva.[28] Jakkoliv další osud tohoto postupu Evropské komise bude jistě předmětem diskuzí a možná také vyjednávání se Spojenými státy o celních opatřeních, nedá se předpokládat, že by logika zapojování soukromých společností do řešení společenských problémů měla ustoupit či pod tlakem USA zmizet z evropského přemýšlení.

[25] Evropská rada – Rada Evropské unie, „Akt o digitálních službách“, https://www.consilium.europa.eu/cs/policies/digital-services-act/.
[26] Evropská komise, „Nařízení o digitálních trzích: Zajištění spravedlivých a otevřených digitálních trhů“, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_cs.
[27] Evropská komise, "Vysvětlení aktu o datech“, https://digital-strategy.ec.europa.eu/cs/factpages/data-act-explained.
[28] ČT24, „Apple dostal od Evropské komise pokutu 500 milionů eur, Meta 200 milionů eur“, 23. 4. 2025, https://ct24.ceskatelevize.cz/clanek/svet/apple-dostal-od-evropske-komise-pokutu-500-milionu-eur-meta-200-milionu-eur-360321.

4 Jakou roli v odolnosti Česka a EU vůči hybridním hrozbám hrají občanská společnost a jednotlivý občan?

Hybridní hrozby zasahují nejen státní instituce, ale i samotnou společnost. Posilování **mediální, digitální a informační gramotnosti občanů**, podpora nezávislých médií a fact-checkingových organizací, informování občanů o jejich právech a povinnostech či zvyšování odolnosti komunit vůči polarizačním narativům představují zásadní součást preventivní strategie EU.

S těmito koncepty, včetně zapojení občanské společnosti, proto zcela správně pracuje česká Národní strategie čelení hybridnímu působení a na ni navázaný akční plán,[29] který v jednom z úkolů přímo ukládá české vládě navázat hlubší a systematičtější spolupráci s expertní společností a akademickou obcí, ale také soukromým sektorem. Kromě toho jasně pojmenovává potřebu vzdělávání společnosti od nejútlejšího věku a začlenění mediálního vzdělávání do rámcových vzdělávacích programů na školách. A přestože k naplnění akčního plánu ani po několika letech zcela nedošlo, některé významné kroky v tomto již byly realizovány, což lze jistě vnímat jako posun směrem k odolnější společnosti. Zároveň se v nadcházejícím období připravuje revize těchto dokumentů, což může přinést další příležitosti ke stanovování konkrétních úkolů a zacelování některých slepých míst české odolnosti vůči hybridním hrozbám a dalším rizikům pramenícím jak z vnějšího světa, tak zevnitř české společnosti.

Budování celospolečenské odolnosti se ukazuje jako nezbytný doplněk k technickým a institucionálním opatřením na systémové úrovni. Pouze společnost, která je schopná kriticky vyhodnocovat informace, odolávat dezinformacím a udržet důvěru ve stát a demokratické instituce, může v dlouhodobém horizontu účinně čelit hybridním hrozbám, jak se již ukázalo tolikrát v minulosti. Je to právě spolupráce mezi státem, jeho institucemi a jednotlivcem-občanem a v širším smyslu také organizovanou občanskou společností, která je pro celospolečenský přístup k vypořádávání se s hybridními hrozbami naprosto rozhodující. Bez důvěry, ale také efektivního nastavení pravidel spolupráce a prostředků k její realizaci je však fungující model vzájemné podpory v praxi pouze obtížně realizovatelný.

Právě na to a připravenost společností reagovat na krize upozorňuje také zpráva bývalého finského prezidenta Sauli Niinistö věnující se posilování civilní i vojenské připravenosti a pohotovosti.[30] Právě celospolečenský přístup přitom zpráva považuje za klíč při efektivním řešení komplexních krizí, a to v odlišnosti od reaktivního postupu národních i evropských úřadů, který má vždy nutně pouze omezený efekt. Ve srovnání s dřívějším přístupem evropských institucí se daleko větší míře pozornosti ve zprávě dostává také civilní ochraně, do které mají jak národní státy, tak evropské instituce mnohem více investovat. Za klíčové prvky v zapojení občanů zpráva považuje proaktivní komunikaci, vzdělávání občanů, ale také budování kapacit na straně občanské společnosti a občana jako aktivní jednotky v odolnosti celé společnosti. Kromě toho však bývalý finský prezident přišel také s celou řadou dalších opatření, včetně užší spolupráce mezi evropskými tajnými službami nebo výraznějších zásahů proti špionážním operacím třetích sil, které však v některých případech mohou být s ohledem na politickou citlivost složitě realizovatelné.

Na Niinistöho zprávu reagovalo na české národní úrovni zejména Ministerstvo vnitra, a to například se svou iniciativou a příručkou „Pro případ

[29] Ministerstvo obrany ČR, „Akční plán k Národní strategii pro čelení hybridnímu působení", https://mocr.mo.gov.cz/images/id_40001_50000/46088/app_2022.pdf.

[30] Evropská rada – Rada Evropské unie, „Jak EU reaguje na krize a buduje odolnost – Evropská rada", https://www.consilium.europa.eu/cs/policies/eu-crisis-response-resilience/.

ohrožení",[31] kterou v nadcházejícím období plánuje rozeslat také do českých domácností. V té se přitom mluví o připravenosti občanů bezprostředně reagovat na krizové situace, a to včetně prostřednictvím vlastního vybavení a zajištění základních potřeb v horizontu 72 hodin, které byly určeny jako interval, v němž lze ve většině případů očekávat pomoc ze strany státu a jeho institucí a dalších zplnomocněných orgánů. Krizová připravenost je přitom jednou ze zásadních součástí odolnosti společnosti čelit krizím, ale také hybridnímu působení, které je často manifestováno snahou vyvolat chaos a způsobit paniku ve společnosti podkopávající důvěru ve stát a jeho instituce.[32]

Kromě civilní ochrany a připravenosti občanů čelit krizím tak, jak to pojmenovává přístup Ministerstva vnitra ČR, existuje i mnohem více angažovaný postup v zapojování občanů k obraně státu. Tyto dva proudy některé evropské státy slučují dohromady, ale v českém kontextu je preferován oddělený, jakkoliv provázaný přístup k této problematice.

Tento druhý proud spadá spíše do gesce Ministerstva obrany ČR a například jeho projektu POKOS (Příprava občanů k obraně státu), který se však v minulosti potýkal s celou řadou problémů a v současné chvíli prochází značnými revizemi. Kromě projektu POKOS je zásadní i zapojování občanů do tzv. aktivní zálohy, práce s mladými lidmi nebo i další iniciativy, včetně tzv. dobrovolného předurčení,[33] kterým si Armáda ČR v poslední době začala zjišťovat ochotu a stav připravenosti vlastní společnosti. V každém případě je však v ČR celý tento druhý segment občanské připravenosti se zapojit do řešení zásadních společenských krizí – jakkoliv v poslední době více na vzestupu – stále do velké míry v počátcích a již delší dobu čeká na silnější impulzy a pobídky ze strany státu.

[31] Ministerstvo vnitra ČR, „Pro případ ohrožení: Příručka pro obyvatele – Ministerstvo vnitra České republiky", https://mv.gov.cz/clanek/pro-pripad-ohrozeni-prirucka-pro-obyvatele.aspx.

[32] Tony Havlík a Jakub Štěpánek, „Proč by Rusko chtělo zapalovat v Praze autobusy? Odpovídáme na nejčastější verze zpochybňovačů", *Novinky.cz*, 21. 6. 2024, https://www.novinky.cz/clanek/podcasty-retezak-proc-by-rusko-chtelo-zapalovat-v-praze-autobusy-odpovidame-na-nejcastejsi-verze-zpochybnovacu-40477129.

[33] Ministerstvo obrany ČR, „Dobrovolné předurčení: další možnost pro ty, kteří se chtějí zapojit do obrany vlasti", https://mocr.mo.gov.cz/informacni-servis/zpravodajstvi/dobrovolne-predurceni:-dalsi-moznost-pro-ty--kteri-se-chteji-zapojit-do-obrany-vlasti-245267/.

Závěr

Tento podkladový dokument si klade za cíl analyzovat a popsat existující hybridní hrozby vůči ČR a evropskému společenství a určit, co je jejich cílem a základní motivací pro jejich realizaci, primárně z pohledu třetích sil. Ty nejzásadnější v podobě ochrany demokratických procesů – a zejména pak voleb – potom analýza popsala do větší míry detailu. Podobně podrobně se přitom věnovala zahraničnímu vměšování, včetně zejména ze strany RF, které autoři identifikovali jako nejvíce intenzivní a ohrožující bezpečnostní zájmy Česka.

Materiál přitom navrhl celou řadu konkrétních opatření, která by mohla být při dostatku politické vůle realizována jak na české národní úrovni, tak ve spolupráci s evropskými partnery v rámci EU. A přestože je vypořádávání se s hybridními hrozbami do vysoké míry koncentrováno v rukou státu a jeho institucí, podklad zdůraznil – podobně jako je to trendem jak na evropské, tak stále více i národní úrovni – také nutnost zapojení veřejnosti a občana jako klíčového prvku aktivní a odolné společnosti, která se dokáže s širokým spektrem hybridních hrozeb a společenských krizí efektivně vypořádávat.

Za klíčovou slabinu českého a evropského přístupu k hybridním hrozbám přitom lze označit reaktivní a časově neefektivní vystupování proti hybridním hrozbám, které je v praxi málo účinné, protože nejenže neodradí útočníka, ale zároveň neposkytne včasnou ochranu zasaženým částem společnosti. Za opak tohoto přístupu dokument považuje tzv. asymetrickou reakci na hybridní hrozby, která má zvýšit náklady na straně původce, ale také proaktivněji nabízet řešení celospolečenských problémů a výzev ze strany evropských členských států i institucí.

Mezi nimi publikace upozorňuje v několika klíčových oblastech, včetně kybernetické, společensko-kulturní, vojensko-bezpečnostní nebo diplomatické doméně, například na potřebu efektivnějšího sankcionování a odhalování původců hrozeb, silnější a rychlejší koordinace a výměny informací mezi unijními státy a institucemi, ale také rezolutnější podpory demokratických sil vystupujících proti autoritářským státům a aktérům podílejícím se na hybridním působení proti západním demokraciím. Mezi dalšími vybranými publikace upozornila například na potřebu:

- aktivního zveřejňování a poukazování na konkrétní případy a subjekty zapojené do hybridního působení, čímž dochází ke zvyšování informovanosti veřejnosti i mezinárodních partnerů,
- paralyzování a sankcionování prokazatelně propagandistických médií a platforem působících na území ČR a v širším evropském prostoru,
- investování do programů mediální a digitální gramotnosti napříč celou společností, a to primárně skrze subjekty odlišné od státu, tj. nezávislé fact-checkingové iniciativy a organizace občanské společnosti, akademickou sférou i samosprávy,
- zajištění bezpečnosti volební infrastruktury, včetně elektronických systémů správy voleb či prevenci další delegitimizace volebního procesu.

Samostatnou kapitolu představuje výzva k budování odolné společnosti a tzv. celospolečenského přístupu, který je postaven na aktivním zapojování a spolupráci mezi státem a jeho občany, vzdělávání, ale také budování kompetencí na straně občanské společnosti. Významným impulzem pro rozproudění národní diskuze je zpráva bývalého finského prezidenta Niinistöho.

V této oblasti stojí ještě před českým státem i evropskými institucemi celá řada výzev, které se sice postupně daří adresovat, zatímco zároveň přibývají nové. Proto bude významné využít revize národní strategie čelení hybridnímu působení k pojmenování nových hrozeb a také zadání konkrétních úkolů jednotlivým českým institucím za účelem jejich řešení. Zároveň se ukazuje jako stále potřebnější pokračovat v práci na úrovni EU a NATO, které mohou český přístup k čelení hybridnímu působení učinit ještě robustnějším a komplexnějším.

Asociace pro mezinárodní otázky (AMO)

AMO je nevládní nezisková organizace založená v roce 1997 za účelem výzkumu a vzdělávání v oblasti mezinárodních vztahů. Tento přední český zahraničně politický think-tank není spjat s žádnou politickou stranou ani ideologií. Svou činností podporuje aktivní přístup k zahraniční politice, poskytuje nestrannou analýzu mezinárodního dění a otevírá prostor k fundované diskusi.

+420 224 813 460

www.amo.cz

info@amo.cz

Žitná 608/27, 110 00 Praha 1

www.facebook.com/AMO.cz

www.twitter.com/amo_cz

www.linkedin.com/company/amocz

www.youtube.com/AMOcz

Pavel Havlíček

Pavel Havlíček je analytikem AMO se zaměřením na východní Evropu, zejména Ukrajinu, Rusko a Východní partnerství. Profesně se zabývá také otázkami bezpečnosti, dezinformací a strategické komunikace stejně jako demokratizace a podpory občanské společnosti. Od roku 2023 spolupracuje se zastoupením nadace Konrada Adenauera v České republice jako Central European Fellow for Security Policy.

pavel.havlicek@amo.cz

Lukáš Horák

Lukáš Horák je analytikem AMO se zaměřením na bezpečnost v regionech západního Balkánu a západní Afriky. Profesně se pak také zabývá otázkami jednotlivých bezpečnostních rizik a fenoménů, dezinformacemi, a jednotlivými nástroji a formami vlivového působení Ruské federace, měnící bezpečnostní dynamiku a politickou realitu v cílových regionech.

lukas.horak@amo.cz

Policy brief vznikl jako podkladový dokument pro kulatý stůl Národního konventu o EU, pořádaný dne 6. června 2025.