

POLICY PAPER:

TICHO PŘED BOUŘÍ: STRATEGICKÁ KOMUNIKACE A SYSTÉMOVÁ PŘIPRAVENOST V HYBRIDNÍM KONFLIKTU



AUTOŘI

Veronika Víchová

CENTRUM PRO INFORMOVANOU SPOLEČNOST

Andrea Michalcová

CENTRUM PRO INFORMOVANOU SPOLEČNOST



CENTRUM PRO
INFORMOVANOU
SPOLEČNOST

Centrum pro informovanou společnost (CIS)

je nevládní nezisková organizace, která není spojena s žádnou politickou stranou. Naší vizí je odolné a připravené Česko proti hybridnímu působení a autoritářskému vlivu.

www.informedsociety.cz



CENTRUM PRO
INFORMOVANOU
SPOLEČNOST

Tato publikace byla připravena s podporou
Britského velvyslanectví v Praze.

www.gov.uk/

world/organisations/

british-embassy-prague.cs



British Embassy
Prague

Tato publikace byla připravena na základě závěrů konference Resilient Europe 2025, která byla uspořádána ve spolupráci s **Ministerstvem zahraničních věcí České republiky.**

mzv.gov.cz



Ministerstvo zahraničních věcí
České republiky

Názory vyjádřené v této publikaci jsou názory autorů a nemusí nutně odrážet názory donorů a partnerů.



CENTRUM PRO
INFORMOVANOU
SPOLEČNOST

ÚVOD

Hybridní hrozby - včetně dezinformací, kybernetických útoků, zahraničních vlivových operací a skrytého financování - se pro evropské demokracie staly trvalou a neustále se měnící výzvou. Hrozby využívají zranitelností politických systémů, digitální infrastruktury a narušené důvěry veřejnostispolečenské soudržnosti. Tato publikace čerpá z **konference Resilient Europe 2025, která se konala v květnu 2025 v Praze¹**, a z odborných znalostí více než 200 odborníků z 26 zemí, kteří se zúčastnili diskusních panelů a doprovodných akcí v rámci konference. Přibližuje vyvíjející se povahu hybridních hrozeb, poukazuje na praktické reakce napříč evropskými státy a nabízí státním představitelům a institucím konkrétní doporučení pro zlepšení odolnosti prostřednictvím právních předpisů, komunikace, civilně-vojenské koordinace a digitální regulace.

1 Více informací o konferenci najdete zde:
https://mzv.gov.cz/jnp/cz/udalosti_a_media/tiskove_zpravy/na_mzv_se_konal_druhy_rocnik_mezinarodni.html



1. TRENDY V OBLASTI HYBRIDNÍCH HROZEB: VÝVOJ V OBLASTI TAKTIKY A NÁSTROJŮ

1.1 OD DEZINFORMACÍ K NARATIVNÍMU VÁLČENÍ

Hybridní působení se neomezuje na ojedinělé případy dezinformací. Jedná se o trvalé snahy o manipulaci narativů přijatých ve společnosti, podkopávání demokratické legitimacy a manipulaci s historickou pamětí obyvatel. Ruské operace v Moldavsku a Litvě ilustrují, jak **lze narativy přizpůsobit tak, aby cílily na identitu, historii a geopolitickou orientaci národa**. Příkladem mohou být vykonstruovaná obvinění z "rusofobie", když Moldavsko připomínalo oběti sovětských deportací², nebo šíření prokremelských verzí litevské historie propagovaných ruskými představiteli³. Cílem těchto taktik je dlouhodobě formovat vnímání veřejnosti a polarizovat domácí debaty.⁴

1.2 ZNEUŽÍVÁNÍ TECHNOLOGIÍ

Hybridní působení je exponencionálně posíleno novými technologiemi:

- **Umělá inteligence a deepfakes** se používají k nelegitimnímu simulování politického dění v reálném čase. Ukrajinská reakce prezidenta Zelenského a virální kampaň "Ya tut" ukázaly nezpochybnitelnou hodnotu autenticity.⁵
- **Algoritmická manipulace:** Rumunsko zažilo během volebního období koordinovanou manipulaci s algoritmy platform, která byla zaměřena na mladší voliče s protisystémovými sděleními.⁶
- **Skryté a decentralizované financování:** Moldavsko odhalilo, jak Rusko využívá kryptoměny a neformální peněžní sítě k financování politické destabilizace. Tato problematika byla řešena prostřednictvím spolupráce více agentur zahrnující finanční regulační orgány, celní orgány a zpravodajské služby.⁷

2 "Moldova Denies Soviet Deportation Exhibition as 'Russophobic.'" Balkan Insight. <https://balkaninsight.com/2023/07/14/moldova-denies-soviet-deportation-exhibition-is-russophobic/>.

3 "Russia publishes a book on Lithuanian history, preface written by Lavrov" LRT. <https://www.lrt.lt/en/news-in-english/19/2550706/russia-publishes-book-on-lithuanian-history-preface-written-by-lavrov>.

4 Více informací o narativním válčení najdete zde: <https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-28-moldovas-struggle-against-russias-hybrid-threats-from-countering-the-energy-leverage-to-becoming-more-sovereign-overall/>

5 Více informací o umělé inteligenci a deepfakes najdete zde: <https://www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18/>

6 Více informací o manipulaci algoritmů najdete zde: <https://www.rgsl.edu.lv/uploads/recent-publications-list/82/developing-legal-framework-for-resilient-society.pdf>

7 "INTELLIGENCE REPORT EXPOSES RUSSIAN MEDDLING IN MOLDOVA'S EU VOTE." Vsquare. <https://vsquare.org/intelligence-report-russian-meddling-in-moldova-eu-referendum-sis-ilian-sor/>.



1.3 DOMÁCÍ PROXY-AKTÉŘI A INTERNALIZACE NEPŘÁTELSKÉHO PŮSOBENÍ

Hranice mezi zahraničními a domácími hrozbami se stále více stírá. Rusko a další aktéři využívají **místní politiky, podnikatele, vlivné osoby a média** k šíření dezinformací nebo narušování národní stability. V Rumunsku a Moldavsku tito aktéři často dostávají skrytou finanční podporu a pod záminkou obrany národní suverenity nebo tradičních hodnot opakují narativy v zájmu Kremlu. Tyto subjekty je obtížné regulovat a často působí legálně, což komplikuje určení jejich původu.

1.4 SABOTÁŽE A HROZBY PRO KRITICKOU INFRASTRUKTURU

Hybridní taktiky zahrnují také **sabotáže kritické i nekritické infrastruktury**. V Baltském moři byly cílem sabotáží internetové kabely a energetické potrubí. "Stínové flotily" plavidel bez vlajky nebo s falešnou vlajkou často operují nepozorovaně a využívají mezinárodního námořního práva. Lotyšsko a Estonsko vyzvaly ke zlepšení informovanosti o situaci na moři, k právní reformě a ke společným monitorovacím operacím EU a NATO. Mise NATO Baltic Sentry významným příkladem schopnosti rychlé a vícestranné reakce.



2. PŘÍKLADY DOBRÉ PRAXE A PRAKTICKÁ DOPORUČENÍ

2.1 INSTITUCIONÁLNÍ REAKCE A PRÁVNÍ INOVACE

Moldavsko na hybridní působení reagovalo zřízením národní agentury pro kybernetickou bezpečnost, modernizací legislativního rámce a **zlepšením koordinace mezi finančními a zpravodajskými institucemi**. Tato opatření pomohla zabránit nezákonnému financování během voleb v roce 2024 a **ukončit podezřelé operace financované ze zahraničí**. Moldavsko zastavilo více než 20 milionů EUR v podezření na nezákonné financování volební kampaně spojené s vnějšími aktéry. Rozhodující byla mezinárodní spolupráce s Ministerstvem financí USA a Europol⁸.

Reformy **lotyšského** trestního zákoníku umožňují **stíhat dezinformační a koordinované zahraniční vlivové operace řízené umělou inteligencí**. Tyto zákony poskytují právní základ pro rychlé jednání během volebního období a umožňují použití **kybernetických důkazů** v soudním řízení - tuto inovaci by mohli přijmout i další členové EU. Lotyšsko rovněž prioritizuje pravidelná zasedání své Národní bezpečnostní rady a silné vazby na vojenské zpravodajství.⁹

Česko vytvořilo nové oddělení na Ministerstvu zahraničních věcí specializované na boj proti hybridnímu působení, které zahrnuje politiku sankcí, kybernetickou politiku a strategickou komunikaci. Oddělení rovněž vypracovalo právní výklady, které vyvažují procesní záruky s operativní účinností a umožňují českým orgánům zmrazit aktiva spojená se sankcionovanými aktéry bez předchozího upozornění. Tento nový výklad potvrdila dvě soudní vítězství.

DOPORUČENÍ:

- **Budovat odolné instituce zajištěním meziresortních mandátů, legislativní pružnosti a integrace pod dohledem občanské společnosti.**
- **Podporovat společné pracovní skupiny, které kombinují finanční regulaci, shromažďování zpravodajských informací a vymáhání práva.**

8 "EUPM Moldova: Moving forward towards sustainable security resilience in Moldova." EUPM. https://www.eeas.europa.eu/eupm-moldova/eupm-moldova-moving-forward-towards-sustainable-security-resilience-moldova_en.

9 "Parliament criminalises use of deep fakes that can influence elections." The Global State of Democracy Initiative. <https://www.idea.int/democracytracker/report/latvia/may-2024>.



2.2 INTEGRITA A TRANSPARENTNOST VOLEB

Moldavsko vytvořilo **meziinstitucionální pracovní skupinu pro ochranu voleb**.¹⁰ Mezi hlavní inovace patří:

- Airport monitoring for illicit cash flows
- Real-time monitoring of campaign financing
- Civil society partnerships to report voter manipulation

Zkušenosti **Německa** s hybridní kampaní Storm-1516, která byla napojena na ruskou Agenturu pro výzkum internetu, ukázaly, že i bez technických zásahů může manipulace s narativy podkopat důvěru veřejnosti. Například německá Strana zelených byla prostřednictvím koordinovaných online dezinformačních kampaní obviňována z ekonomických problémů. Úřady proti tomu bojovaly tím, že informovaly novináře, zapojily vlivné osoby a rychle vyvracely narativy pomocí interního ověřování faktů.¹¹

Situace v **Rumunsku** pak demonstrovala, že odolnost vyžaduje nejen vzdělávání veřejnosti, ale také zvýšení nákladů pro protivníky. Rumunský přístup zahrnuje odhalování finančních vazeb mezi domácími aktéry a zahraničními sponzory, legislativní transparentnost a vytrvalé prosazování odpovědnosti platform.¹²

DOPORUČENÍ:

- **Integrita voleb vyžaduje celoroční práci, nejen zásahy těsně před volbami.**
- **Zřídit multidisciplinární jednotky pro monitoring dezinformací, nezákonného financování a ohrožení procesu voleb.**
- **Využívat veřejné kampaně ke zvýšení informovanosti a posílení důvěry voličů. Státní instituce by měly spolupracovat s příslušnými aktéry a komunikátory, včetně organizací občanské společnosti nebo influencerů, aby důvěryhodným kanálem oslovily cílové skupiny.**
- **Využívat možností, které poskytuje Evropská komise (včetně Aktu o digitálních službách), například tlačit na sociální sítě nebo předem testovat volební proces, zda je připravený na zásahy z vnější.**

10 "Combating Corruption in Political Finance." International IDEA.
<https://www.idea.int/sites/default/files/2025-04/combating-corruption-in-political-finance.pdf>.

11 "Germany warns of Russian disinformation targeting election." Reuters.
<https://www.reuters.com/world/europe/germany-warns-russian-disinformation-targeting-election-2025-02-21/>.

12 "How Russia-backed influencers meddled in Romania's vote." Financial Times.
<https://www.ft.com/content/4b00e7ec-2c79-4313-b012-4f09f436f3ed>.



2.3 STRATEGICKÁ A KRIZOVÁ KOMUNIKACE

Země jako Litva, Estonsko a Lotyšsko začaly zavádět systematické modely, které integrují vládní struktury, krizové řízení a technologické inovace.

Litva po osmi letech příprav zahájila v roce 2023 provoz národního centra pro strategickou komunikaci. Funguje na základě vyhodnocení situace a aktuálních hrozeb v reálném čase a úzké spolupráce se soukromým sektorem, který pomáhá s odhalováním falešných zpráv a s finanční podporou nevládních organizací. Veřejná komunikace se řídí zásadami rychlosti a relevance.

Litevské **Národní centrum krizového řízení**¹³ provádí **čtvrtletní simulační cvičení** a koordinuje komunikaci ministerstev prostřednictvím jednotky rychlé reakce. Jejich doktrína "Pokud nereagujete rychle, přijali jste narativ za svůj" je uvedena do praxe **předem schválenými obsahovými rámci** a integrovanými komunikačními týmy.

Estonsko vybudovalo **síť založenou na důkazech a aktivním zapojení médií**. Stále se však potýká s pomalým zveřejňováním zpravodajských informací, a to i v případech, kdy je jejich původ (např. Kreml) jasný. Estonsko institucionalizovalo transparentnost **aktivním zveřejňováním reakcí na dezinformace** a poskytováním školení mediální gramotnosti.

Ukrajina používá i platformy jako TikTok a Telegram, čímž investuje do **mladých digitálních talentů a nevládních organizací, které spoluvytvářejí obsah**. Propojení kulturní odolnosti a sdělení šířených občanskými aktéry na kanálech, které cílové skupiny skutečně používají, pomohlo udržet společenskou soudržnost.

Bez **politického uznání závažnosti** hybridních hrozeb zůstanou i ty nejlépe míněné iniciativy neúčinné. Strategická komunikace se pak často redukuje na symbolická gesta. V rámci státní správy sice vznikají nové útvary či funkce, ale postrádají jasně daný mandát, zdroje a politickou podporu, a tedy i skutečný dopad. Klíčové poučení z celého regionu je následující: **žádná komunikační strategie nemůže být účinná, pokud není zakotvena v širším politickém rámci a není podpořena** skutečnou vůlí chránit demokratické instituce.

Strategická komunikace musí stát mimo politické týmy ministrů. Nemůže být součástí jejich kabinetů, které jsou ze své podstaty politické. Stratcom vyžaduje profesionální, odborně řízenou a dlouhodobě udržitelnou strukturu. Měla by být zakotvena v rámci veřejné správy, konkrétně jako součást agendy zaměřené na odolnost vůči hybridním hrozbám.

13 "Lithuania to establish National Crisis Management Centre." LRT.
<https://www.lrt.lt/en/news-in-english/19/1854923/lithuania-to-establish-national-crisis-management-centre>.



DOPORUČENÍ:

- **Přejít od reaktivní komunikace k proaktivitě.**
- **Obsadit stratcom týmy profesionálů a vytvářet kreativní partnerství s organizacemi občanské společnosti a firmami, vybavit jednotlivá oddělení kvalitními nástroji pro tvorbu obsahu. Institucionalizovat osvědčené postupy prostřednictvím školení a sdílených příruček, případně také legislativy.**
- **Politické vedení musí převzít odpovědnost za to, že hybridní hrozby budou považovány za strategickou prioritu, a zajistit odpovídající mandáty, zdroje a institucionální podporu pro strategickou komunikaci. Stratcom jako takový by však neměly vést politické týmy z ministerských kabinetů, ale profesionálové ze státní správy bez politické agendy.**
- **Ujistit se, že týmy a odborníci na strategickou komunikaci mají jasně dané a transparentní mandáty, abyste se vyhnuli nejistotě, paralýze, šíření mýtů nebo politickému odporu.**
- **Investovat do systémových přístupů, které propojují bezpečnostní analýzu, odborníky na komunikaci a krizové řízení.**
- **Transparentnost a důvěryhodnost musí být v rovnováze s ochranou národních bezpečnostních zájmů. Klíčovými faktory jsou odvaha a důvěra.**



2.4 CIVILNĚ-VOJENSKÁ A MEZISEKTOROVÁ SPOLUPRÁCE

Finská koncepce totální obrany vyžaduje **krizovou připravenost ve všech odvětvích**, včetně soukromé logistiky a regionálních zdravotnických sítí. Vzdělávání a povinná branná povinnost zahrnují digitální gramotnost a psychologickou odolnost.

Armáda České republiky cvičí vojáky v **informační hygieně** a pořádá simulace jako Power of Hope, které připravují vojenské i civilní aktéry na hybridní krizové scénáře. Program klade důraz na empatii, regulaci emocí a koordinovanou komunikaci.

Ukrajinská nadace Come Back Alive je příkladem zakořeněné civilně-vojenské spolupráce. Kromě darování vybavení se podílí na tvorbě strategické komunikace a pomáhá sladit parlament, občanskou společnost a ozbrojené síly.

DOPORUČENÍ:

- **Přijmout civilně-vojenské plánování za běžnou součást národní obranné politiky. Civilně-vojenskou spolupráci již nelze oddělit a měla by být zohledněna v obranném plánování státu.**
- **Investovat do krizového výcviku a účasti civilního obyvatelstva na národních cvičeních.**
- **Podporovat budování důvěry mezi bezpečnostním sektorem a občanskou společností.**



2.5 REGULACE A DIGITÁLNÍ ODOLNOST

Akt o digitálních službách (Digital Services Act, DSA) představuje zásadní regulační základ pro práci s obsahem na sociálních sítích, ale vyžaduje důkladné provádění na vnitrostátní úrovni. Zatímco Litva a Belgie podnikly proaktivní kroky, například zřídily národní střediska pro sledování umělé inteligence a dezinformací, ostatní země zaostávají kvůli nedostatečné zákonné adaptaci, omezenému personálnímu obsazení nebo nejasným mandátům.

Rumunsko ukázalo riziko nedostatečné regulace, když byl TikTok před volbami použit k šíření zpráv podporovaných ze zahraničí. Včas nebyla přijata žádná moderační opatření a občanské subjekty byly ponechány hrozbě napospas.

Česko a **Estonsko** ukazují, že je třeba, aby digitální regulační orgány měly vyšetřovací pravomoci a schopnost spolupracovat s platformami i vnitrostátními bezpečnostními orgány. Požadavky na transparentnost musí být důsledně prosazovány.

DOPORUČENÍ:

- **Adaptovat a implementovat Akt o digitálních službách s vnitrostátními dohledovými orgány, které mohou kontrolovat platformy, vydávat závazná rozhodnutí a provádět vyšetřování.**
- **Podporovat partnerství s občanskými, technologickými a akademickými institucemi s cílem zajistit, aby byl dohled založen na datech.**



2.6 SPOLUPRÁCE S REGIONÁLNÍMI A MÍSTNÍMI AKTÉRY

Pokud stát nezapojí regionální a místní aktéry, oslabuje tím svůj vlastní komunikační dopad. Jak zdůraznilo více příspěvateľů, obce jsou nejbližším spojovacím článkem s občany, ale často zůstávají nevyužity. Iniciativy, jako jsou regionální prohlídky, školení seniorů v oblasti digitální gramotnosti a neformální hospodské akce, ukazují, že místní osobní zapojení funguje.

Obcím však často chybí strategická komunikační podpora. Jako nejdůvěryhodnější úroveň veřejné správy by měly být vybaveny přizpůsobitelnými sadami nástrojů, granty a přímými kanály na národní stratcom týmy.

DOPORUČENÍ:

- **Začlenit komunikační odolnost do programů regionálního rozvoje.**
- **Financovat osvětovou činnost v obcích, formáty mezigeneračního dialogu a partnerství s knihovnami a kulturními institucemi, zejména se zaměřením na zranitelné skupiny.**
- **Vytvořit strukturální rámec pro zapojení obcí do národních komunikačních strategií. Vybavit je znalostmi, nástroji a ověřeným obsahem.**
- **Včasné budování komunit je prioritou: Spolupracovat s organizacemi občanské společnosti a místními aktéry s cílem navazovat nová partnerství. Budování formálních i neformálních komunit a důvěry mezi nimi v době míru bude mít velký dopad, až přijde krize. Prosté vzájemné poznávání napříč institucemi, sektory a regiony je to, co dostane "celospolečenský přístup" z papíru do reality. Někdy to nejlepší, co můžete udělat, je prostě pozvat lidi na pivo.**



ZÁVĚR

Hybridní hrozby se vyvíjejí, ale stejně tak se vyvíjejí i naše protipatření. Konference Resilient Europe 2025 ukázala, že roztříštěné nebo krátkodobé reakce jsou nedostatečné. Odolnost musí být zabudována do institucí, komunit a každodenní komunikace. Cesta vpřed vyžaduje více než jen informovanost. Vyžaduje koordinaci, investice a morální jistotu. Evropské demokracie mají k dispozici nástroje, nyní musí sebrat politickou vůli jednat.

Z diskusí napříč panely a zeměmi jasně vyplývají následující poučení:

1. **Potřebujeme komunikaci založenou na datech.** Strategická komunikace musí být založena na výzkumu cílových skupin, behaviorálních datech a testování sdělení. **Musíme vědět, co říkat, jak to říkat a komu to říkat.** Bez dat hrozí, že komunikační strategie budou reaktivní, špatně nastavené nebo neúčinné.
2. Evropští lídři musí **převzít odpovědnost za to, že obranu proti hybridním hrozbám zařadí mezi strategické priority**, a uznat, že **strategická komunikace je klíčovým pilířem budování odolnosti** proti těmto hrozbám. Verbální shoda v těchto otázkách však nestačí. Jakákoli strategie může být účinná pouze tehdy, pokud jsou instituce schopné jednat, což vyžaduje jasný mandát a zdroje, jakož i legislativu aktualizovanou tak, aby odpovídala současným hrozbám.
3. **Zapojme občanský sektor a nové aktéry.** Kampaně na národní úrovni jsou nezbytné, ale nedostatečné. Změna přichází také zdola. Je třeba posílit nové typy komunikátorů - učitelů, vlivných osobností, komunitních vůdců, knihovníků, veteránů a dalších, aby mohli oslovit různé společenské segmenty, zejména ty, které nedůvěřují tradičním institucím.
4. **Musíme mít odvahu a ochotu jednat.** Čelit hybridním hrozbám vyžaduje víc než jen analýzu. Vyžaduje rozhodné vedení, agilní instituce a legislativní nástroje, které odrážejí složitost dnešních rizik. Je třeba překonat institucionální setrvačnost a politickou opatrnost.

Jak shrnul jeden z účastníků:

"Čelíme zásadní výzvě: lidé se nestarají. Úloha strategické komunikace spočívá právě v tomto: jak přimět lidi, aby se zajímali?"

To je nejtěžší zkouška demokratické odolnosti - nejenže musí odolat vnějším hrozbám, ale také znovu najít jednotu uvnitř své vlastní společnosti.

Evropa může obstát v éře hybridních hrozeb jen tehdy, pokud bude své demokratické zřízení stavět na akceschopných institucích, otevřeném dialogu a dlouhodobé spolupráci napříč společností.

Než přijde další velká krize, nemusíme mít mnoho času - proto bychom měli začít jednat odvážně už nyní.





CENTRUM PRO
INFORMOVANOU
SPOLEČNOST

www.informedsociety.cz