 DOI: 10.3849/2336-2995.35.2026.01.180-199

Recenzovaný článek

Současný stav a některé budoucí výzvy obrany informačního prostředí v České republice a zahraničí

Current Status and Some Future Challenges of Information Environment Defense in the Czech Republic and Abroad

Šárka Tesařová[1], Radomír Ščurek[1]

[1]Univerzita obrany, Brno, Česká republika

Abstrakt: Článek se zabývá problematikou obrany informačního prostředí v současném bezpečnostním kontextu se zvláštním zaměřením na kognitivní válčení jako jednu z klíčových a dynamicky se rozvíjejících výzev posledních let. Cílem tohoto přehledového článku je zasadit uvedený fenomén do širšího bezpečnostně-strategického rámce obrany informačního prostředí a popsat, jakým způsobem je tato oblast koncepčně a institucionálně uchopena jak v České republice, tak u vybraných aliančních spojenců – konkrétně ve Velké Británii, Estonsku, Finsku, Švédsku a na Slovensku. Článek primárně vychází z veřejně dostupných strategických a koncepčních dokumentů a oficiálních politik jednotlivých zemí. Na tomto základě článek identifikuje základní společné rysy a odlišnosti v jejich přístupech k obraně informačního prostředí a zároveň vyvozuje některé budoucí výzvy v této oblasti.

Abstract: The article addresses the issue of information environment defence in the current security context, with a special focus on cognitive warfare as one of the key and rapidly developing challenges of recent years. The aim of this overview article is to place this phenomenon within a broader security-strategic framework of information environment defence and to describe how this area is conceptually and institutionally approached in the Czech Republic and in selected NATO Allies – specifically in the United Kingdom, Estonia, Finland, Sweden, and Slovakia. The article is primarily based on publicly available strategic and conceptual documents and official policies of individual countries. On this basis, the article identifies the basic common features and differences in their approaches to information environment defence, while also drawing conclusions about some future challenges in this area.

Klíčová slova: bezpečnostní politika; hybridní hrozby; informační prostředí; kognitivní válčení; odolnost.

Keywords: Security Policy; Hybrid Threats; Information Environment; Cognitive Warfare; Resilience.

ÚVOD

Dynamický rozvoj informačních a komunikačních technologií, digitalizace a globalizace vedly k zásadním proměnám soudobého válčení. Třebaže, v duchu Clausewitzova pojetí, zůstává povaha války jako násilného aktu směřujícího k podřízení vůle protivníka neměnná, postupně se mění charakter války, tzn. způsob, jakým je válka vedena. Moderní konflikty proto už nejsou omezeny pouze na tradiční fyzická bojiště za použití letálních zbraní na zemi, moři či ve vzduchu, ale podstatná část soupeření se přesunula i do digitální a informační dimenze, což se odráží ve vzniku hybridního, kybernetického a informačního válčení.

Informační prostředí tak tvoří významnou součást bojiště a nelze je již vnímat pouze jako podpůrnou složku, nýbrž jako samostatnou doménu pro soupeření státních i nestátních aktérů. Zejména hybridní konflikty toto prostředí stále více využívají k dosažení strategických cílů, aniž by se přímo uchýlily k otevřené a vyhlášené válce za použití kinetických zbraní. V těchto konfliktech aktéři využívají slabých míst v oblasti důvěry veřejnosti, digitálních platforem a institucionální legitimity k utváření vnímání dějů a manipulaci s informačními toky. Tyto akce destabilizují společnosti, polarizují a radikalizují obyvatelstvo a podkopávají demokratickou správu věcí veřejných spolu s národní suverenitou.

V tomto širším kontextu se do popředí odborného zájmu postupně dostává koncept kognitivního válčení. V odborné literatuře bývá kognitivní válčení často zasazováno do širšího rámce hybridního působení, informačních operací či strategické komunikace. Jednotná a všeobecně přijímaná definice sice zatím neexistuje, ale panuje shoda na tom, že cílem je změnit nejen to, co si lidé i celá společenství myslí, ale i to, jak myslí a jednají a jak se rozhodují. Na rozdíl od tradiční informační války, orientované na kontrolu informací/narativů a šíření propagandy, kognitivní válčení využívá psychologické, emocionální a technologické nástroje k přímému ovlivňování lidského činitele. Ten zůstává klíčovým prvkem rozhodovacích procesů jak v civilní, tak ve vojenské oblasti. V rámci těchto postupů se tak vytváří prostor pro možné cílené ovlivňování morálky ozbrojených sil i nálad obyvatelstva. Právě tato obtížně uchopitelná, avšak potenciálně vysoce účinná dimenze představuje specifickou výzvu pro obranu informačního prostředí.

Obrana informačního prostoru, potažmo čelení kognitivnímu válčení, představuje pro státy tedy nemalou bezpečnostní výzvu. Česká republika, podobně jako další alianční spojenci, jako jsou Velká Británie, Estonsko, Finsko, Švédsko a Slovensko, nabízejí různé přístupy k řešení těchto výzev, které odrážejí různou úroveň připravenosti, dostupnosti zdrojů, odborného a kulturního kontextu. Neméně významným faktorem podtrhujícím

důležitost přípravy a obrany informačního prostředí je ten fakt, že dosud není v rámci NATO jednoznačně definována terminologie ani společné postupy.

Cílem tohoto přehledového článku je zasadit kognitivní válčení do širšího bezpečnostně-strategického rámce obrany informačního prostředí a popsat, jakým způsobem je tato oblast koncepčně a institucionálně uchopena v České republice a zahraničí. Článek primárně vychází z veřejně dostupných strategických a koncepčních dokumentů a oficiálních politik jednotlivých zemí. Pozornost je přitom věnována především identifikaci základních charakteristik těchto přístupů, a nikoliv jejich vyčerpávající komparativní analýze. Na tomto základě článek identifikuje základní společné rysy a odlišnosti v jejich přístupech k obraně informačního prostředí, a zároveň vyvozuje některé budoucí výzvy v této oblasti. Článek představuje úvodní příspěvek k dané problematice a vytváří rámec pro její detailnější rozpracování v připravované disertační práci.

1 KONCEPČNÍ RÁMEC INFORMAČNÍHO PROSTŘEDÍ, HYBRIDNÍHO A KOGNITIVNÍHO VÁLČENÍ

Účelem této kapitoly je konceptualizovat základní pojmy pro tento článek, jimiž jsou informační prostředí, hybridní válčení a kognitivní válčení, a objasnit jejich vzájemné souvislosti.

1.1 Informační prostředí

Jednotlivé události ve světě jsou přenášeny do lidské mysli, resp. jsou šířeny, jako informace prostřednictvím sítí. Jakmile se tyto informace dostanou do cílené oblasti, do lidské mysli, podléhají předběžným představám, interpretaci, zkreslení, agendě, úpravám a změnám případně opětovnému přenosu. Jedná se o informační prostředí, které je definováno v aliančním standardu AJP 10.1 jako *„prostředí složené ze samotných informací, jednotlivců, organizací a systémů, které informace přijímají, zpracovávají a předávají, a kognitivního, virtuálního a fyzického prostoru, ve kterém k tomu dochází“* (NATO 2023, 179).

Informační prostředí zahrnuje tři vzájemně propojené dimenze: 1) fyzickou dimenzi s hmotnou páteřní infrastrukturou (komunikační sítě, satelity, datová centra, aplikační programové prostředky); 2) informační dimenzi, kde je přenášen obsah, včetně faktů, příběhů a dezinformací a 3) kognitivní dimenzi zaměřenou na to, jak jednotlivci a společnosti vnímají, interpretují a reagují na informace (Theohary 2018, 5).

Hlavním prostředím pro sdílení informací je kyberprostor, ve kterém je možno nalézt průsečík všech zmíněných fenoménů. Mezi typy informací, které se objevují v rámci informačního prostředí jako součást informačních operací, patří propaganda, zavádějící informace a dezinformace (Theohary 2018, 2).

Hybridní konflikty, dezinformace a kognitivní válčení mají společné to, že se odehrávají ve výše definovaném informačním prostředí, které se tak stává klíčovým prostředím

(válčištěm) pro úspěšné vedení hybridních konfliktů. Lze tedy říct, že obrana informačního prostředí (válčiště) se stává prioritou každého státu.

1.2 Hybridní válčení

Pojmy jako hybridní válka či hybridní hrozby se stávají v dnešní době moderními pojmy, třebaže nejsou jednoznačně terminologicky vymezeny. Vzestup hybridních válek předpokládal F. Hoffman již v roce 2007, jenž definoval hybridní válčení jako „*celou škálu různých způsobů vedení války včetně konvenčních schopností, pravidelných taktik a formací, teroristických činů včetně nevybíravého násilí a nátlaku a kriminálních nepokojů*“ (Hoffman 2007, 8). R. Glenn tento pohled rozšiřuje o katastrofický prvek a zahrnutí nevojenských prostředků (Glenn 2009, 2). V rámci ruského pojetí pak V. Gerasimov klade důraz na speciální operace, vytvoření „*trvale operující fronty napříč celým nepřátelským územím*“ a nevojenské metody jako primární (Galeotti 2014).

NATO vnímá hybridní válčení jako „*širokou, komplexní a adaptivní kombinaci konvenčních a nekonvenčních prostředků a zjevných a skrytých vojenských, polovojenských a civilních opatření*“ (Warsaw Summit Communiqué 2016, odst. 72). Hybridní válčení charakterizují tak dvě elementární charakteristiky: rozmazaná hranice mezi válkou a mírem a nejednoznačnost připisování útoků (Bilal 2021).

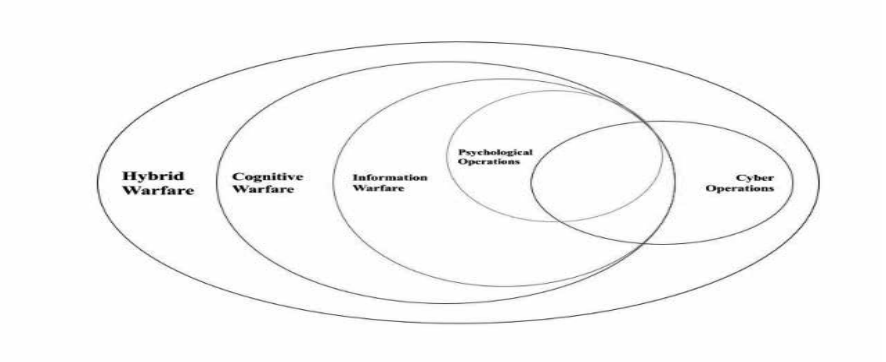
Hybridní útoky byly označeny jak Strategickým konceptem NATO, tak Strategickým kompasem EU a závěry Rady EU ze dne 21. 6. 2022 jako způsobilé pro kolektivní reakci.

1.3 Kognitivní válčení

Jedním z nových konceptů, který se v posledních letech objevuje ve vojenské terminologii, je kognitivní válčení. V kognitivním válčení se „bojištěm“ stává lidská mysl. Do budoucna je přitom predikováno, že v budoucím válčení bude váha kognitivní domény dále narůstat a že operace kognitivního válčení svou dlouhodobostí a zároveň komplexností představují hrozbu s vysokou mírou nebezpečnosti (NATO ACT 2024). Ačkoliv je v literatuře a různých doktrínách možné nalézt mnoho pokusů o definici kognitivního válčení, všeobecně přijímaná definice doposud neexistuje. Zřejmě nejšířeji je pojatá definice od B. Claveriho a F. Du Cluzela, kteří definují kognitivní válčení jako „*nekonvenční formu válčení, která využívá kybernetické nástroje ke změně kognitivních procesů nepřítele, využívá mentální předsudky nebo reflexivní myšlení a vyvolává zkreslení myšlení, ovlivňuje rozhodování a brání jednání s negativními účinky na individuální i kolektivní úrovni*“ (Claverie et al. 2022, 1). Stejně tak O. Backes a A. Swab vnímají kognitivní válčení jako „*strategii, která se zaměřuje na změnu toho, jak cílové obyvatelstvo myslí a jak se chová*“ (Backes and Swab 2019, 8). S ohledem na cíle kognitivního válčení A. Bernal a kol. tvrdí, že je to „*zbrojení veřejného mínění externí entitou za účelem ovlivňování veřejné a/nebo vládní politiky nebo za účelem destabilizace vládních akcí a/nebo institucí*“ (Bernal et al. 2020, 10). Vědecký tým NATO STO pak u kognitivního válčení akcentuje

jeho nebezpečnost v „*invazivní, rušivé a neviditelné povaze*“ a jeho cíl „*využít aspekty poznání k narušení, podkopání, ovlivnění nebo změně lidských rozhodnutí*“ (Masakowski and Janet 2023, 1). V neposlední řadě v aliančním přístupu integruje kognitivní válčení „*kybernetické, informační, psychologické a sociální inženýrství a tyto činnosti, prováděné v synchronizaci s jinými nástroji moci mohou ovlivnit postoje a chování tím, že ovlivní, ochrání/naruší individuální a skupinové poznávání, aby získali výhodu nad protivníkem*“ (NATO ACT 2023).

Existuje velký koncepční přesah mezi kognitivním válčením a dalšími příbuznými koncepty, jako jsou hybridní působení, informační operace, psychologické operace, dezinformace a propaganda. Tyto koncepty jsou často mezi sebou zaměňovány, avšak z obsahového hlediska mezi nimi existují podstatné rozdíly. Následující obrázek znázorňuje mnohem přehledněji vztahy mezi válčením a dalšími příbuznými koncepty.



Obrázek č.1: Znázornění vztahu mezi kognitivním válčením a dalšími příbuznými koncepty
Zdroj: Drmotová and Kutěj 2024

Aktéry využívající kognitivní válčení mohou být státní i nestátní subjekty. Ze státních subjektů vyvinuly hlavně státy jako Rusko a Čína sofistikované schopnosti kognitivního válčení lišící se ve svém pojetí. Ruské pojetí kognitivního válčení spadá pod definici Reflexivní kontrolní doktríny od V. Lefebvreho – je to integrovaná operace, jež nutí protivníka s rozhodovací pravomocí jednat ve prospěch Ruska tím, že změní jeho vnímání světa za použití pravdivých, nepravdivých i zkreslených informací (Du Cluzel 2021, 26). Čínské pojetí je založeno na dosažení „nadřazenosti mysli“ za systematického využití jak kognitivní vědy, tak biotechnologie (Du Cluzel 2021, 27).

V kognitivním válčení se využívá široká škála strategií a taktik s cílem ovlivňovat-chování jednotlivců i celých společenství. Konkrétní taktiky zahrnují např. odvedení pozornosti, vyvolání rozptýlení, vyvolání strachu, zavádění falešných narativů, radikalizaci jednotlivců a zesílení sociální polarizace (Claverie et al. 2022). Kognitivní operace jsou často koordinovány s podkopáváním spolehlivosti a důvěry v kritické systémy a instituce, jako jsou státní správa, státní bezpečnost, sociální sféra, banky, nemocnice, vzdělávací a vědecké instituce a oficiální zdroje informací (Danyk and Briggs 2023, 41). Občas se útočníci spokojí pouze s rozséváním chaosu a nejistoty; kognitivní válčení ovšem může být součástí

většího strategického plánu (Danyk and Briggs 2023, 47). Strategie je celkově úspěšnější v kontextech, kde již došlo k nějakým destabilizačním účinkům (Miller 2023, 5).

Útoky jsou směřovány tak, aby především ovlivnily myšlení politických představitelů, členů celých společenských nebo profesionálních skupin, příslušníků armády až po celé populace – ideálně bez vědomí dotčených subjektů (Claverie et al. 2022, 1). Západ je terčem různých vlivových kampaní pocházejících z Ruska už více než deset let (Burda 2023, 1).[1]

2 PŘÍSTUPY VYBRANÝCH ALIANČNÍCH SPOJENCŮ K OBRANĚ INFORMAČNÍHO PROSTŘEDÍ

Pro potřeby tohoto přehledového článku jsou v následující části zevrubně představeny přístupy k obraně informačního prostředí v pojetí Velké Británie, Estonska, Finska, Švédska a Slovenska, které na základě prvotního zkoumání vykazují odlišné přístupy a lze z nich odvodit dílčí náměty pro aplikaci v České republice.

Důvodem výběru těchto států byl ten fakt, že uvedené přístupy k obraně informačního prostředí vycházejí mimo jiné z rozmanitých geopolitických, institucionálních a kulturních kontextů. Všechny porovnávané státy jsou však evropské země s vazbou na NATO a EU, jejich výdaje na obranu se relativně pohybují v podobném rozmezí, všechny státy čelí hybridním hrozbám především ze strany Ruska a Číny. Naopak se uvedené porovnávané státy odlišují strategickou polohou a vnímáním bezpečnostních hrozeb, popřípadě modely obrany.

Pro účely úvodního zhodnocení a deskripce byly zvoleny následující identifikátory: národní strategické a koncepční dokumenty, institucionální rámec (včetně přítomnosti specializovaných orgánů), veřejná informovanost a mediální gramotnost. Záměrem tohoto článku není provést plnou komparativní analýzu, což by dle názoru autorů přesahovalo rámec tohoto článku, ale shrnutí problematiky k určitému datu a základní kritické utřídění velké šíře poznatků, což je zároveň jeho předností.

V neposlední řadě je třeba uvést, že tato práce se potýká s určitými omezeními, kdy v rámci zhodnocení přístupů aliančních spojenců se vždy nejedná o úplný výčet, jelikož ne všechny informace o konkrétních organizačních, personálních a technických kapacitách jednotlivých států jsou veřejně dostupné.

2.1 Velká Británie

Velká Británie integruje ve svém přístupu ke kognitivnímu válčení zpravodajství, kybernetickou bezpečnost a strategickou komunikaci.

1 Příklady kognitivních operací zahrnují: Facebook-Cambridge Analytica skandál a manipulace voleb, propagace různých konspiračních teorií během pandemie COVID-19, ruská agrese na Ukrajině.

Strategické a koncepční dokumenty

Britský Integrovaný přehled 2021 zdůraznil silnější, integrovaný přístup k odstrašování a obraně uprostřed rostoucích hybridních hrozeb, ten z roku 2023 se pak chce soustředit na stanovení nových norem v kybernetickém i hybridním konfliktu a na regulaci chování s potenciálními formálními dohodami (HM Governement 2023, 33, 43).

Ústředním bodem britského přístupu je tzv. doktrína kognitivního efektu, která využívá techniky mající potenciál zasít nedůvěru, snížit morálku a oslabit schopnost protivníka plánovat a provádět své aktivity efektivně s cílem změnit své chování – to může zahrnovat zabránění teroristickým skupinám ve zveřejňování částí extremistických médií online nebo ztížení státům používat internet k šíření dezinformací (National Cyber Force 2023, 14-16).

Institucionální rámec

Tato doktrína je obsažena v rámci kybernetické strategie, v níž mají klíčovou roli Národní kybernetické síly založené v roce 2020 na pomezí zpravodajských a ozbrojených složek. Přitom veřejně uvádí, že se uvedené složky aktivně podílejí na narušování teroristických aktivit kombinujících operace technického rázu s činnostmi určenými k podpoře nedůvěry a snížení morálky (National Cyber Force 2023, 11, 21). V letech 2018 a 2019 Velká Británie zřídila přímo pro boj s dezinformacemi dvě pracoviště: vládní protidezinformační útvar fungující pod Ministerstvem pro vědu, inovace a technologii a „Rapid Response Unit" podřízenou přímo Úřadu vlády. Účelem protidezinformačního útvaru je porozumět dezinformačním narativům a pokusům o umělou manipulaci informačního prostředí tak, aby vláda pochopila rozsah a dosah škodlivých dezinformací a mohla přijmout vhodná opatření (Gov.uk 2023). „Rapid Response Unit", která byla v roce 2022 rozpuštěna, vytvářela pravidelné mediální souhrny informací převzatých z veřejně dostupných zdrojů (ibid.). Dalším aktérem je Národní bezpečnostní komunikační tým pomáhající řešit komunikační aspekty vzájemně propojených a složitých problémů národní bezpečnosti, včetně dezinformací (Governement Communication Service 2018). Z vojenských složek se na nové formy válčení a informační operace specializuje 77. brigáda (77th Brigade).

Veřejná informovanost a mediální gramotnost

Velká Británie napomáhá k posilování odolnosti společnosti i prostřednictvím komunikačního rámce RESIST, který pomáhá vládním ministerstvům a dalším vládním subjektům bojovat proti dezinformacím (Governement Communications Service 2022).

2.2 Estonsko

Estonsko je dlouhodobě známé jako světový lídr v oblasti digitalizace a kybernetické bezpečnosti, a to zejména díky svým zkušenostem s vůbec prvními rozsáhlými kybernetickými útoky v roce 2007. V reakci na to země vyvinula vysoce odolnou digitální infrastrukturu a komplexní politiku integrující informační bezpečnost, kybernetickou bezpečnost a strategickou komunikaci se zapojením občanské společnosti.

Strategické a koncepční dokumenty

Estonská Národní bezpečnostní koncepce rámuje kybernetickou bezpečnost, psychologickou obranu a strategickou komunikaci jako otázku odolnosti (Juurvee and Arold 2021). Estonská Dlouhodobá strategie Estonsko 2035 a Národní plán rozvoje obrany do roku 2031 kladou důraz na posílení národní informační odolnosti (Buholcs et al. 2024, 21). Estonsko nemá konkrétní zákon pokrývající dezinformace.

Institucionální rámec

Útvar strategické komunikace v rámci Státního úřadu koordinuje práci napříč různými orgány a koordinuje psychologickou obranu, Ministerstvo školství a výzkumu odpovídá za podporu mediální gramotnosti a dále jsou zapojeny také Ministerstvo obrany, Ministerstvo vnitra a Ministerstvo hospodářství a komunikací (Malts 2025, 8). Klíčovou institucí je Centrum excelence pro kooperativní kybernetickou obranu NATO, založené v Tallinu v roce 2008, hrající významnou roli ve výzkumu a výcviku v oblasti kybernetické obrany (CCDCOE).

Veřejná informovanost a mediální gramotnost

Ústředním pilířem estonského přístupu k informačnímu prostředí je podpora mediální gramotnosti a povědomí veřejnosti. Od roku 2014 estonská vláda začlenila kurz mediální gramotnosti do školních osnov a také nabízí granty pro novináře a zpravodajská média, a to i v ruském jazyce (Klyszcz 2024). Občanská iniciativa/blog Propastop sleduje a odhaluje dezinformace se zaměřením na ruskojazyčná média cílící na rusky mluvící menšinu v Estonsku (Propastop 2017).

Příkladem spolupráce s civilním sektorem je společnost Sentinel, která spolupracovala na vývoji komplexní strategie pro boj proti dezinformacím v Estonsku se zaměřením na partnerství veřejného a soukromého sektoru a integraci iniciativ souvisejících s dezinformacemi do stávajících rámců kybernetické bezpečnosti (Accelerate Estonia).

2.3 Finsko

Pro Finsko je charakteristický komplexní celospolečenský přístup k bezpečnosti, který integruje jak úřady státní správy, tak podnikatelskou sféru spolu s občanskou společností až po jednotlivce, a to mimo jiné i v obraně informačního prostředí a boji proti hybridním hrozbám (Valtioneuvosto 2025, 12).

Strategické a koncepční dokumenty

Finská Bezpečnostní strategie pro společnost nastiňuje, že Finsko musí komplexně posílit svou vlastní bezpečnost s důrazem na odolnost, schopnost společnosti reagovat na narušení a krize a klíčovou roli jednotlivců při zvyšování bezpečnosti (Valtioneuvosto 2025). Finsko nemá konkrétní zákon pokrývající dezinformace.

Institucionální rámec

Kromě koordinace se finská vláda rovněž aktivně zapojuje do preventivního odhalování zavádějících narativů s primárním zaměřením na Rusko (Valtioneuvosto). V Helsinkách sídlí Centrum excelence pro boj proti hybridním hrozbám, které se zaměřuje na různé aspekty hybridních hrozeb (Hybrid CoE).

Veřejná informovanost a mediální gramotnost

Klíčovým pilířem finské strategie je výrazné zapojení veřejnosti. Důležitým prvkem tohoto přístupu jsou národní kurzy obrany, jejichž cílem je poskytnout účastníkům většinou z klíčových vedoucích funkcí napříč sektory celkový přehled o zahraniční, bezpečnostní a obranné politice země (Wigell et al. 2021, 28). Příkladem veřejno-soukromé spolupráce je i Národní agentura pro nouzové zásobování provozující Mediapooli jako platformu spojující mediální společnosti a úřady pro řešení otázek kybernetické bezpečnosti, boje proti hybridním hrozbám a dezinformacím, včetně ovlivňování informací nepřátelskými aktéry (Mediapooli).

Obecně Finsko vyniká v boji proti dezinformacím, kdy podle analýzy mediální gramotnosti je celkově nejméně náchylnou zemí k falešným zprávám (Lessenski 2022, 18). Právě vysoká mediální gramotnost je základním kamenem obrany Finska proti dezinformacím. Finský vzdělávací systém již od 50 let 20. století zahrnuje mediální gramotnost a kritické myšlení do svých národních vzdělávacích osnov (Wigell et al. 2021, 30).

2.4 Švédsko

Švédský přístup vychází z konceptu tzv. totální obrany, který integruje vojenské a civilní struktury, aby čelil konvenčním i nekonvenčním hrozbám. Více jak 70 let je jeho součástí taktéž koncept psychologické obrany k udržení vůle obyvatelstva se bránit (Pamment and Elsa Isaksson 2024).

Strategické a koncepční dokumenty

Švédská Národní bezpečnostní strategie zdůrazňuje, že má být posílena schopnost čelit hybridním hrozbám (Governement of Sweden 2024, 30). Švédsko nemá konkrétní zákon pokrývající dezinformace.

Institucionální rámec

V roce 2022 byla zřízena švédská Agentura pro psychologickou obranu, spadající pod Ministerstvo obrany a čítající 60 zaměstnanců, jejímž hlavním úkolem je vést úsilí o koordinaci v rámci švédské psychologické obrany, tzn. identifikovat, analyzovat a poskytovat podporu v boji proti škodlivému informačnímu vlivu a jiným zavádějícím informacím namířeným proti švédským zájmům ze zahraničí (MPF 2024). Švédsko zřídilo Radu pro spolupráci v psychologické obraně sdružující civilní, bezpečnostní a vojenské služby (Tofvesson). Dalšími aktéry jsou švédská bezpečnostní služba (SÄPO) a Agentura pro civilní nepředvídané události (MSB) (Pamment and Isaksson 2024, 31).

Veřejná informovanost a mediální gramotnost

Základním pilířem švédského pojetí je nejen důraz na budování odolnosti obyvatelstva, ale také podpora médií při řešení dezinformací, s nimiž sdílí své znalosti (Tofvesson).

Kupříkladu v letech 2021–2022 čelilo Švédsko masivní kampani šířící dezinformace o tom, že sociální služby unášejí muslimské děti – nově zřízená Agentura tomu čelila veřejným odhalením hrozby, což pomohlo znovu získat kontrolu nad příběhem a celou situaci deeskalovat (ibid.).

3.5 Slovensko

Slovenská společnost se vyznačuje výraznou rozpolceností, polarizací a pocitem ohrožení ze strany jiných zemí/subjektů, což je pravděpodobně příčinou vyšší důvěry v dezinformace a manipulativní tvrzení spolu se sníženou tolerancí k odlišnostem (Globsec 2024). Významným problémem na Slovensku je rovněž vysoký průnik prokremelských dezinformací, které ovlivňují veřejné mínění v bezpečnostních otázkách.[2]

Strategické a koncepční dokumenty

Slovenská Bezpečnostní strategie z roku 2021 výslovně uznává jako strategickou prioritu účinně a koordinovaně reagovat na hybridní hrozby a dezinformace (Vláda Slovenskej republiky 2021, 2). V reakci na to Obranná strategie počítá také se zvyšováním informovanosti obyvatelstva o zajišťování obrany státu, čímž se zvýší odolnost obyvatelstva vůči dezinformacím a škodlivé propagandě (Ministerstvo obrany Slovenskej republiky 2021, 23). V roce 2018 byla přijata Koncepce pro boj proti hybridním hrozbám a dále byla v roce 2024 přijata Koncepce strategické komunikace.

Institucionální rámec

Jako koordinační a komunikační platformy pro širší problematiku hybridních hrozeb fungují Situační centrum při úřadu vlády či Národní bezpečnostně-analytické centrum při Slovenské informační službě (Ministerstvo vnitra 2022, 32). Dále na Slovensku působí Meziresortní konzultační skupina pro boj s dezinformacemi, kterou tvoří Ministerstvo zahraničních věcí a evropských záležitostí, Ministerstvo obrany, Ministerstvo kultury a Ministerstvo školství, vědy, výzkumu a sportu, Policie SR, Slovenská informační služba (ibid.). V rámci Ministerstva vnitra bylo zřízeno Centrum boje proti hybridním hrozbám (Hybridné hrozby na Slovensku). Koordinační roli pro strategickou komunikaci zastává Úřad vlády (ibid.).

Přístup k veřejné informovanosti a mediální gramotnosti

Oblast mediálního vzdělávání byla do školních osnov zařazena v roce 2011 a v této oblasti působí zejména univerzity a občanské organizace (Ministerstvo kultury 2020), v reakci na duplikaci a roztříštěnost aktiv se Rada pro mediální služby zhostila úlohy organizátora a koordinátora pravidelných setkání v rámci Platforma Mediálna gramotnosť+ v roce 2022 (Rada pre mediálne služby). Důležité jsou i iniciativy vedené občanskou společností, jako jsou Demagog.sk a Konšpirátori.sk, které sledují a vyvracejí dezinformace (Demagog.sk; Konspiratori.sk).

2 Např. rozšířené jsou dezinformace o válce na Ukrajině, přičemž více lidí obviňuje Západ nebo Ukrajinu (51 %) než Rusko (41 %) (Globsec 2024).

3 PŘÍSTUP ČESKÉ REPUBLIKY K OBRANĚ INFORMAČNÍHO PROSTŘEDÍ

Účelem této kapitoly je především představit relevantní strategické a koncepční dokumenty a institucionální rámec České republiky k obraně informačního prostředí.

3.1 Strategické a koncepční dokumenty

Již *Audit národní bezpečnosti* z roku 2016 zdůrazňoval, že moderní hrozby, a zejména jejich kombinace, vyžadují mnohem zásadnější pozornost, než tomu bylo v minulosti – mnohem komplexněji by měla být řešena oblast tzv. hybridních hrozeb a s nimi spojených dezinformačních útoků (Ministerstvo vnitra 2016).

V *Bezpečnostní strategii* a *Obranné strategii České republiky*, revidovaných v roce 2023, je z množství odkazů patrný důraz na obranu před nepřátelským hybridním působením, na kybernetickou bezpečnost, na boj proti dezinformacím i na rizika oslabení vlivu a jednoty demokratických zemí (Ministerstvo zahraničních věcí 2023, 27; Ministerstvo obrany 2023, 3). Stát musí předcházet dezinformacím, které zpochybňují principy právního státu a demokracie, zároveň je ovšem klíčové posilování odolnosti společnosti (Ministerstvo zahraničních věcí 2023, 18 a 38). Obranná strategie též uznává, že nastávají změny ve způsobu vedení konfliktů s ohledem na rapidní technologický vývoj a nástup nových a přelomových technologií (Ministerstvo obrany 2023, 6).

Národní strategie pro čelení hybridnímu působení se zaměřuje na posílení společenské a institucionální odolnosti, zlepšení systémů včasné detekce, atribuce a reakce na hybridní útoky a v neposlední řadě integruje celospolečenský přístup (Ministerstvo obrany 2021, 7); na strategii pak navazuje akční plán s konkrétními úkoly a opatřeními. *Národní strategie kybernetické bezpečnosti* klade důraz na posílení ochrany kritické infrastruktury, zvýšení schopnosti kybernetické bezpečnosti a podporu mezinárodní spolupráce, zejména v rámci NATO a EU (Národní úřad pro kybernetickou a informační bezpečnost 2020).

Jediný český koncepční dokument, který explicitně, i když pouze v obecné a stručné rovině reflektuje problematiku kognitivního válčení, je *Koncepce výstavby Armády České republiky 2035*, jež předpokládá budování schopností pro operace v kybernetickém prostoru, schopnost kognitivního působení vůči všem cílovým skupinám a zvyšování odolnosti proti kognitivnímu vlivu nepřítele (Ministerstvo obrany 2024, 22).

Z dokumentu *Analýza připravenosti České republiky čelit závažné dezinformační vlně* vyplývá, že „*Česká republika v současné době nemá koncepční, organizační, personální, procesní, právní ani jiné nástroje a kapacity, které by byly efektivní v reakci na případný útok proti ČR vedený pomocí úmyslně vytvořené nebo spontánně vzniklé závažné dezinformační vlny*“ (Ministerstvo vnitra 2022, 4). Dále se uvádí, že chybí taktéž podpora celospolečenského přístupu skrze podporu mediální gramotnosti (ibid.). Co se týče odolnosti české společnosti vůči dezinformacím, je hodnocena jako nízká a neschopná čelit dlouhodobému a soustavnému působení dezinformací (ibid.).

3.2 Institucionální rámec

V souladu s ustanovením § 28 odst. 1 č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, je za zajišťování obrany a bezpečnosti zodpovědná vláda České republiky (zákon č. 2/1969 Sb.). Gestorem kybernetické bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost (Národní úřad pro kybernetickou a informační bezpečnost 2020, 7), úkol zajišťování kybernetické obrany byl svěřen Vojenskému zpravodajství (Vojenské zpravodajství 2021). Úřad vlády je pověřen koordinací čelení hybridnímu působení a strategické komunikace státu (Ministerstvo obrany 2023, 13), v letech 2024–2025 zde fungoval odbor strategické komunikace a byla dokonce zřízena pozice vládního koordinátora strategické komunikace státu.[3] Při Ministerstvu vnitra funguje také odborné analytické a koncepční pracoviště – Centrum proti hybridním hrozbám – věnující se problematice hybridních hrozeb ve vnitřní bezpečnosti (Ministerstvo vnitra).

Za zabezpečování působení Armády ČR v kybernetické operační doméně a informačním prostředí budou zodpovědné Informační a kybernetické síly (Ministerstvo obrany 2024, 38).

I tak ale chybí prakticky fungující aparát a operativní nástroje, jak účinně čelit hybridnímu působení nepřátelských aktérů (Havlík 2022). Boji s dezinformacemi se v české státní správě věnují jednotky osob (Ministerstvo vnitra 2022, 24).

4 SHRNUTÍ A ZHODNOCENÍ ČESKÉHO A ZAHRANIČNÍCH PŘÍSTUPŮ K OBRANĚ INFORMAČNÍHO PROSTŘEDÍ

Porovnání českého přístupu k obraně informačního prostředí na základě výše uvedených identifikátorů s těmi ve Velké Británie, Estonsku, Finsku, Švédsku a na Slovensku ukazuje následující poznatky:

- Estonsko spolu s Finskem přímo sousedí s Ruskem, což ovlivňuje jejich obranné priority. Finsko a Švédsko byly do roku 2024 vojensky neutrální, a musely tak proto klást větší důraz na zajištění vlastní obrany *vs.* Česká republika je členem NATO od roku 1999.
- Estonské zkušenosti z rozsáhlých kybernetických útoků spolu s vyspělou digitální společností poskytují silný základ pro efektivní obranu informačního prostředí i do budoucna *vs.* spíše průměrná vyspělost české digitální společnosti.
- Typický je multiagenturní přístup dle jednotlivých zaměření.
- Velká Británie zaujímá ke kognitivnímu válčení velmi aktivní přístup, ať prostřednictvím tzv. doktríny kognitivního efektu v rámci kybernetické strategie či aktivním

[3] Od ledna 2026 byl odbor zrušen a pozice vládního koordinátora již od října 2025 není obsazena (Úřad vlády 2026).

přístupem a množstvím specializovaných složek určených k boji proti dezinformacím. Zajímavá je i vysoká míra otevřenosti směrem k veřejnosti o těchto aktivitách.
- Co se týče reflektování kognitivního válčení jako nové výzvy, se jeví švédská Agentura pro psychologickou obranu jako unikátní a nejpokročilejší instituce.
- Estonsko a Finsko bezpochyby těží z přítomnosti Center excelence na svém území.
- Vysoká odolnost Finska vůči dezinformacím může být jednak dána vysokou kvalitou finského vzdělávacího systému a dlouhodobým úsilím o zvyšování mediální gramotnosti, jednak může hrát roli i samotný jazyk, kdy finština představuje jeden z nejunikátnějších jazyků na světě.
- Na Slovensku se úsilí o zajištění informačního prostředí zvyšuje, překážkou je výrazná proruská polarizace společnosti a náchylnost vůči dezinformacím *vs.* v České republice proruská polarizace ve společnosti není tak výrazná, nicméně přetrvávají sklony k přejímání k dezinformací.
- Česká republika má standardně doktrinálně podchyceny všechny klíčové elementy, významným počinem bylo zřízení pozice koordinátora strategické komunikace – tato pozice je ovšem nyní neobsazena a zřejmě dle prohlášení vlády v této činnosti nebude nikdo jiný pokračovat. Nadto přetrvávají nedostatky ohledně fungujícího aparátu a operativních nástrojů. Nicméně na mezinárodním poli v oblasti hybridního působení se aktivně angažuje.

5 BUDOUCÍ VÝZVY PRO OBRANU INFORMAČNÍHO PROSTŘEDÍ

Česká republika, a stejně tak další západní státy, čelí nebo budou čelit při obraně informačního prostředí mnoha výzvám, které lze odvodit z výše uvedeného přehledového pohledu na existující a zmapované skutečnosti.

Největší výzvu bezesporu reprezentuje rychlý technologický pokrok ve všech oblastech lidské činnosti, hlavně však v oblasti výpočetní techniky, informačních systémů a nových softwarových aplikací pro hromadné zpracovávání dat (tzv. data mining), což je umožněno širokou aplikací neuronových sítí a v poslední době pak umělou inteligencí. Pokroky v umělé inteligenci a strojovém učení dnes umožnují vytvářet velmi přesvědčivý falešný obsah, díky čemuž nepřátelští aktéři mohou ovlivňovat veřejné mínění. Sociální média pak šíření tohoto obsahu usnadňují v bezprecedentním měřítku. To vytváří požadavek na nová technologická řešení, která jej dokážou rozpoznat a bojovat proti němu. Rovněž bude potřeba dobře nastavit zásady a postupy týkající se řádné správy a odpovědného využívání umělé inteligence. Významným prvkem se jeví nezbytnost přípravy lidského činitele ke zvýšení jeho odolnosti vůči zvýšené mentální zátěži při řízení zbraňových systémů, zejména s ohledem na potenciální hrozbu kybernetického útoku.

Další výzvou je celkové informační přetížení společnosti spolu s rostoucí nedůvěrou v tradiční média a vládní instituce. Denně se setkáváme s obrovským objemem informací, který může u jednotlivců snižovat schopnost kritické analýzy informací a zapříčinit tím větší náchylnost ke zjednodušeným verzím. S tím je spjata i rostoucí nedůvěra v tradiční média a vládní instituce, kdy veřejný skepticismus vůči oficiálním narativům vytváří úrodnou půdu pro dezinformační kampaně vedoucí často ke společenské polarizaci. Je proto

zásadní, aby nejen vláda a bezpečnostní aparát, ale také mediální organizace a vzdělávací instituce spolupracovaly na budování odolnosti společnosti (Miller 2023, 5).

Co se týče kognitivního válčení, bude nutné se vypořádat se základními mezerami, jako jsou nedostatek jasných definic kognitivního válčení a neexistence konkrétních postupů pro řešení kognitivních hrozeb. Dále to budou problémy spjaté s regulací sociálních médií a digitálních platforem, praktickým prosazováním práva, složitostí připisování útoků konkrétním aktérům a zajištěním rovnováhy mezi občanskými svobodami a bezpečností (Miller 2023, 5).

Jednou z hlavních právních výzev kognitivního válčení je právě potenciální konflikt s občanskými svobodami, obzvláště se svobodou projevu a soukromí. Demokratické společnosti mají v porovnání s autoritářskými společnostmi v tomto ohledu poněkud „svázané ruce" – v liberálních demokraciích armáda nemůže vést operace se zjevným vlivem proti vlastnímu obyvatelstvu, a to navzdory tomu, že je tu reálná možnost snížení schopností jednotlivých členských států i celého NATO (Burda 2023, 10). Otázky ohledně práva na soukromí by též vyvolávalo monitorování sociálních sítí a datových toků. Právní opatření musí proto být pečlivě navržena, aby se předešlo nezamýšleným důsledkům, jako jsou cenzura či potlačování legitimního nesouhlasu.

Nejblíže alespoň k částečnému řešení této problematiky v České republice mohl být zákon pro boj proti dezinformacím, jenž měl navrhovat vypnutí dezinformačních webů s prokazatelným vlivem cizích mocností vytvořených v nepřátelských zemích s cílem poškodit Českou republiku – návrh zákona byl připraven Ministerstvem vnitra v roce 2023, avšak nakonec nebyl vládě vůbec předložen kvůli kritice upozorňující na omezení svobody slova a projevu (Bartoníček 2023). Naproti tomu bezpečnostní experti argumentovali, že takový zákon by posílil obranyschopnost země, k čemuž Náčelník Generálního štábu Armády ČR Karel Řehka konstatoval, že „*obrana země v otevřených konfliktech, jako je válka na Ukrajině, nezávisí jen na bojeschopné armádě, ale i na odhodlání zemi bránit*" (Vávrová 2022).

Významným potenciálem se jeví nutnost zlepšování vzdělávacího systému v oblasti informačních systémů ve společnosti a zvyšování mediální gramotnosti na školách a v mediálních prostředcích.

ZÁVĚR A DOPORUČENÍ

Přehled přístupů České republiky a dalších vybraných aliančních spojenců dle tohoto přehledového článku ukazuje, že ačkoli jednotlivé státy volí odlišná koncepční a institucionální řešení, shodují se v narůstajícím významu a systematičtějším uchopením informační dimenze v posledních letech. Zároveň je patrné, že míra rozvinutosti těchto přístupů je podmíněna bezprostředností bezpečnostní hrozby fungující jako katalyzátor inovací, celkovou úrovní digitalizace a společenské odolnosti i schopností zajistit funkční institucionální koordinaci. Současně obrana informačního prostředí – z pohledu kognitivního válčení – čelí dle tohoto přehledového článku několika strukturálním výzvám, a to zejména absenci jednotného terminologického rámce, neexistenci konkrétních postupů

pro řešení kognitivních hrozeb, praktickému prosazování práva a vymezení odpovědností jednotlivých aktérů.

Za situace, kdy „*strategickou výhodu v kognitivním válčení má ten, kdo se první pohne a zvolí si čas, místo a prostředky útoku*“ (Johns Hopkins University and Imperial College London 2021), se klíčovým předpokladem účinné obrany stává schopnost včasného rozpoznání probíhající kampaně a systematického budování institucionální i společenské odolnosti.

Text vznikl za podpory z projektu LANDOPS – Vedení pozemních operací u Fakulty vojenského leadershipu Univerzity obrany (DZRO-FVL22-LANDOPS).
Autoři prohlašují, že nejsou ve střetu zájmů v souvislosti s publikováním tohoto článku a při jeho přípravě akceptovali všechny etické normy požadované vydavatelem.

SEZNAM ZDROJŮ

“Strategická komunikace na vládě končí. Babiš: Na rozdíl od minulé vlády budeme komunikovat otevřeně.“ *iRozhlas*, 5. 1. 2026. https://www.irozhlas.cz/zpravy-domov/strategicka-komunikace-na-vlade-konci-babis-na-rozdil-od-minule-vlady-budeme_2601051548_jho

77th Brigade. n.d. “77th Brigade Information Operations.“ https://www.army.mod.uk/learn-and-explore/about-the-army/formations-divisions-and-brigades/field-army-troops/77th-brigade-information-operations/

Accelerate Estonia. n.d. “Sentilel: Combating Information Warfare.“ https://accelerate.ee/projects/combating-information-warfare/

Backes Oliver, and Andrew Swab. 2019. *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States*. Cambridge: Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states

Bartoníček, Radek. 2023. “Stát nemá říkat, co je pravda, tvrdí Rakušan. S dezinformacemi chce bojovat vzděláním.” *Aktuálně*.cz, 25. 9. 2023. https://zpravy.aktualne.cz/domaci/dezinformace-vit-rakusan/r~068d31fc5a1711ee9ae20cc47ab5f122/

Bernal, Alonso, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla. 2020. *Cognitive Warfare: An Attack on Truth and Thought*. NATO a John Hopkins University. https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf

Bilal, Arsalan. 2021. “Hybrid Warfare – New Threats, Complexity, and ‘Trust’ as the Antidote.“ *NATO Review*, November 30, 2021. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Buholcs, Jānis, Anastasija Tetarenko-Supe, Sten Torpan et al. 2024. *The Regulation of Fact Checking and Disinformation in the Baltic States*. Tartu: Baltic Engagement Centre for Combating Information Disorder. https://becid.eu/results_and_studies/the-regulation-of-fact-checking-and-disinformation-in-the-baltic-states/

Burda, Robin. 2023. *Cognitive Warfare as Part of Society: Never-Ending Battle for Minds*. Platform Influencing Human Behaviour, Paper 4. https://hcss.nl/wp-content/uploads/2023/06/04-Cognitive_Warfare_as_Part_of_Society__Never_Ending_Battle_for_Minds.pdf

CCDCOE. n.d. "About us." https://ccdcoe.org/about-us/

Clausewitz, Carl. 1984. *On War*. Princeton, New Yersey: Princeton University Press. https://antilogicalism.com/wp-content/uploads/2019/04/on-war.pdf

Claverie, Bernard, Baptiste Prébot, Norbou Buchler, and François Du Cluzel, eds. 2022. *Cognitive Warfare: The Future of Cognitive Dominance*. Bordeaux: NATO Collaboration Support Office. https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf

Council of European Union. 2022. "Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns." June 21, 2022. https://www.consilium.europa.eu/cs/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/

Danyk, Yuriy, and Chad Briggs. 2023. "Modern Cognitive Operations and Hybrid Warfare." *Journal of Strategic Security* 16 (1): 35-50. https://doi.org/10.5038/1944-0472.16.1.2032

Demagog.sk. n.d. "O nás". https://demagog.sk/o-nas

Drmotová, Kristýna, and Libor Kutěj. 2024. "Cognitive Warfare as a New Dimension of Security. A Fictional Concept or a Real Silent Threat?" *Vojenské Rozhledy* 33 (1): 63-83. https://doi.org/10.3849/2336-2995.33.2024.01.063-083

Du Cluzel, François, ed. 2021. *Cognitive Warfare*. Norfolk: Innovation Hub. https://innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf?ref=stratagem.no

European External Action Service. 2022. *A Strategic Compass for Security and Defence*. Brussels. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

Galeotti, Mark. 2014. "The 'Gerasimov Doctrine' and Russian Non Linear War." *Moscow Shadows*. https://cs.brown.edu/people/jsavage/VotingProject/2017_03_09_MoscowsShadow_GerasimovDoctrineAndRussianNon-LinearWar.pdf

Giandomenico, Jessica, and Hanna Linderstål. 2023. *Disinformation Landscape in Sweden*. EU DisinfoLab. https://www.disinfo.eu/wp-content/uploads/2023/05/Sweden_Disinfo-Factsheet.pdf

Glenn, Russel. 2009. "Thoughts on "Hybrid" Conflict." *Small Wars Journal*. 8. https://smallwarsjournal.com/2009/03/03/thoughts-on-hybrid-conflict/

Globsec. 2024. "GLOBSEC Trends 2024 Slovakia." May 27, 2024. https://www.globsec.org/what-we-do/publications/globsec-trends-2024-slovakia

Gov.uk. 2023. "Fact Sheet on the CDU and RRU." https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru

Governement Communications Service. 2022. *RESIST 2: Counter Disinformation Toolkit*. London. https://gcs.civilservice.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf

Governement Communications Unit. 2018. "Alex Aiken introduces the Rapid Response Unit." https://webarchive.nationalarchives.gov.uk/ukgwa/20200203104056/https:/gcs.civilservice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/

Governement of Sweden. 2024. *National Security Strategy*. Stockholm. https://www.government.se/globalassets/government/national-security-strategy.pdf

Havlík, Martin. 2022. "Aktuální přístupy České republiky, EU a NATO k hybridním hrozbám." *Vojenské rozhledy* 31 (2): 3-16. https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-a-obranna-politika/19782-aktualni-pristupy-ceske-republiky-eu-a-nato-k-hybridnim-hrozbam#_ftn12

HM Governement. 2023. *Integrated Review Refresh 2023*. London. https://assets.publishing.service.gov.uk/media/641d72f45155a2000c6ad5d5/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf

Hoffman, Frank G. 2007. *Conflict in the 21 st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Hybrid CoE. n.d. "About us". https://www.hybridcoe.fi/about-us/

Hybridné hrozby na Slovensku. n.d. "Centrum boja proti hybridným hrozbám: úlohy a úspěchy." https://www.hybridnehrozby.sk/2205/zakladne-informacie/

Johns Hopkins University, and Imperial College London. 2021. "Countering cognitive warfare: awareness and resilience." *NATO Review*, May 20, 2021. https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

Juurvee, Ivo, and Uku Arold. 2021. "Psychological Defence and Cyber Security: Two Integral Parts of Estonia's Comprehensive Approach for Countering Hybrid Threats." *ICONO 14 Revista de comunicación y tecnologías emergentes* 19 (1): 70-94. https://www.redalyc.org/journal/5525/552565288004/html/#redalyc_552565288004_ref40

Klyszcz, Ivan U. 2024. "Shadow War: What Estonia and Poland Tell Us About Russia-'s Clandestine Operations in Europe." *Brussels School of Governance – Centre for Security, Diplomacy and Strategy*, July 4, 2024 https://csds.vub.be/publication/shadow-war-what-estonia-and-poland-tell-us-about-russias-clandestine-operations-in-europe/

Konšpirátori.sk. n.d. https://konspiratori.sk/

Lessenski, Marin. 2022. *How It Started, How It is Going: Media Literacy Index 2022. Policy Brief 57*. Open Society Institute – Sofia Foundation. https://osis.bg/wp-content/uploads/2022/10/HowItStarted_MediaLiteracyIndex2022_ENG_.pdf

Malts, Kaili. 2025. *Disinformation Landscape Estonia*. EU DisinfoLab. https://www.disinfo.eu/wp-content/uploads/2025/01/20250110_Disinfo-landscape-in-Estonia.pdf

Μασακοωσκι, Ψωννε P., ανδ Θανετ M. Βλατνψ, εδσ. 2023. *Mitigating and Responding to Cognitive Warfare: NATO STO*

Technical Report. Neuilly-sur-Seine: NATO STO. https://www.researchgate.net/publication/369305190_Mitigating_and_Responding_to_ Cognitive_Warfare

Mediapooli. N.d. "Our Mission." https://mediapooli.fi/en/our-mission

Miller, Seumas. 2023. "Cognitive Warfare: An Ethical Analysis." *Ethics and Information Technology* 25 (46): 1-10. https://doi.org/10.1007/s10676-023-09717-7

Ministerstvo kultúry Slovenskej republiky. 2020. "Koncepcia mediálnej výchovy v SR." 19. 3. 2020. https://www.culture.gov.sk/uncat/koncepcia-medialnej-vychovy-v-sr/

Ministerstvo obrany České republiky. 2021. *Národní strategie pro čelení hybridnímu působení*. Praha. https://mocr.mo.gov.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf

Ministerstvo obrany České republiky. 2023. *Obranná strategie České republiky*. Praha. https://mocr.mo.gov.cz/images/id_40001_50000/46088/obranna__strategie-_c_r_2023_final.pdf

Ministerstvo obrany České republiky. 2024. *Koncepce výstavby Armády České republiky 2035*. Praha. https://mocr.mo.gov.cz/images/id_40001_50000/46088/KVA__R_2035_Final.pdf

Ministerstvo obrany České republiky. 2025. *Akční plán k Národní strategii pro čelení hybridnímu působení na rok 2025*. Praha. https://mocr.mo.gov.cz/images/id_40001_50000/46088/Ak__n___pl__n_k_N__rodn___strategii_pro___elen___hybridn__mu_p__soben___na_rok_2025.pdf

Ministerstvo obrany Slovenskej republiky. 2021. *Obranná stratégia Slovenskej republiky*. https://www.mosr.sk/data/files/4286_obranna-strategia-sr-2021.pdf

Ministerstvo vnitra České republiky. 2016. *Audit národní bezpečnosti*. Praha. https://vlada.gov.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

Ministerstvo vnitra České republiky. 2022. *Analýza připravenosti České republiky čelit závažné dezinformační vlně*. Praha. https://mv.gov.cz/chh/soubor/analyza-pripravenosti-ceske-republiky-celit-zavazne-dezinformacni-vlne.aspx

Ministerstvo vnitra České republiky. n.d. "Centrum proti hybridním hrozbám." https://mv.gov.cz/chh/

Ministerstvo zahraničních věcí České republiky. 2023. *Bezpečnostní strategie České republiky*. Praha. https://mzv.gov.cz/file/5161086/Bezpecnostni_strategie_2023.pdf

Moilanen, Panu, Miriam Hautala, Dominic Saari. 2023. *Disinformation Landscape in Finland*. EU DisinfoLab. https://www.disinfo.eu/wp-content/uploads/2023/05/Finland_DisinfoFactsheet.pdf

MPF. 2024. "Our Mission.". April 3, 2024. https://mpf.se/psychological-defence-agency/about-us/our-mission

Národní úřad pro kybernetickou a informační bezpečnost. 2020. *Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025*. Brno. https://nukib.gov.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

National Cyber Force. 2023. *The National Cyber Force: Responsible Cyber Poder in Practice*. https://www.gchq.gov.uk/files/NCF_Responsible_Cyber_Power_In_Practice.pdf

NATO ACT. 2023. “Kognitivně Warfare: Strengthening and Defending the Mind.“ 5. 4. 2023. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/

NATO ACT. 2024. *Strategic Foresight Analysis 2023*. Norfolk, Virginia. https://www.act.nato.int/wp-content/uploads/2024/01/SFA2023_Final.pdf

NATO. 2016. “Warsaw Summit Communiqué.“ July 9, 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm#hybrid

NATO. 2022. *NATO Strategic Concept*. Brussels. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

NATO. 2023. *AJP 10.1 Allied Joint Doktríně For Strategic Communications*. https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf

NATO. 2024. “Countering hybrid threats.“ https://www.nato.int/cps/on/natohq/topics_156338.htm

Pamment, James, and Elsa Isaksson. 2024. *Psychological Defence: Concepts and principles for the 2020s*. https://mpf.se/download/18.34845f44192b793f4ee27d9/1730120674895/241017_Psychological-Defence-Concepts-and-principles-for-the-2020s_rapport.pdf

Propastop. 2017. “What is Propastop?“ March 6, 2017. https://www.propastop.org/en/2017/03/06/what-is-propastop/

Rada pre mediálne služby. n.d. “Platforma Mediálna gramotnosť+.“ https://rpms.sk/

Theohary, Cathrine A. 2018. *Information Warfare: Issues for Congress*. Washington: Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R45142/5

Tofvesson, Mikael. n.d. “Defence Against the Dark Arts: Sweden’s Psychological Defence Agency.“ *Chandler Institute of Governance* https://www.chandlerinstitute.org/governancematters/defence-against-the-dark-arts-swedens-psychological-defence-agency

Valtioneuvosto. 2025. “Overview of information influence activities“. https://valtioneuvosto.fi/en/government-communications/overview-of-information-influence-activities?gsid=0c7a8cee-84c0-44c1-b5e3-09bef4c56ce1

Valtioneuvosto. 2025. *Security Strategy for Society*. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/166026/VN_2025_3.pdf?sequence=4&isAllowed=y

Vávrová, Iveta. 2022. “Zákon proti dezinformacím? „Nejde o omezení svobody tisku, ale o obranyschopnost země,“ argumentují bezpečnostní experti.“ *Radiožurnál*, 11. 10. 2022. https://radiozurnal.rozhlas.cz/zakon-proti-dezinformacim-nejde-o-omezeni-svobody-tisku-ale-o-obranyschopnost-8845428

Vláda České republiky. 2026. *Pracovní a poradní orgány*. https://vlada.gov.cz/cz/pracovni-a-poradni-organy-vlady/#zmocnenci

Vláda Slovenskej republiky. 2021. *Bezpečnostná stratégia Slovenskej republiky*. https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf

Vojenské zpravodajství. 2021. “Vojenské zpravodajství se podílí na zajišťování kybernetické obrany České republiky.“ https://www.vzcr.cz/kyberneticka-obrana-46

Wigell, Mikael, Harri Mikkola, and Tapio Juntunen. 2021. *Best Practices in the Whole-of-society Approach in Countering Hybrid Threats*. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU%282021%29653632_EN.pdf

Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky. https://www.zakonyprolidi.cz/cs/1969-2