 DOI: 10.3849/2336-2995.35.2026.01.142-155

Recenzovaný článek

Infiltrace a ovlivňování členů Aktivní zálohy AČR: přehled nekonvenčních rizik pro ochranu kritické infrastruktury

Infiltration and Influence Targeting of the Czech Armed Forces' Active Reserves: An Overview of Non-Conventional Risks to Critical Infrastructure Protection

Ondřej Vozňák

Fakulta Vojenského Leadershipu, Univerzita obrany, Brno, Česká republika

Abstrakt: Článek analyzuje infiltrační a vlivové hrozby zaměřené na členy Aktivní zálohy Armády České republiky jako specifický faktor nekonvenčního rizika pro ochranu kritické infrastruktury. Aktivní záloha, představující klíčové propojení civilní a vojenské sféry, může být vystavena psychologickému a informačnímu působení s dopadem na loajalitu a operační připravenost. Text shrnuje teoretické přístupy k fenoménu insider threat, identifikuje zranitelnosti lidského faktoru a srovnává český přístup s vybranými aliančními a zahraničními modely (NATO, EU, USA). Závěrem formuluje doporučení pro prevenci infiltrace prostřednictvím vzdělávání, kognitivní odolnosti a integrovaného řízení rizik v oblasti obrany a kritické infrastruktury.

Abstract: The article examines infiltration and influence operations targeting members of the Active Reserves of the Czech Armed Forces as a specific non-conventional risk factor for critical infrastructure protection. As a bridge between civilian and military spheres, the Active Reserve is exposed to psychological and informational pressures affecting loyalty and operational readiness. The paper summarizes theoretical approaches to the insider threat phenomenon, identifies human-factor vulnerabilities, and compares the Czech framework with selected NATO, EU, and U.S. models. It concludes with recommendations for preventive measures focused on education, cognitive resilience, and integrated risk management within national defense and critical infrastructure protection.

Klíčová slova: Aktivní záloha; nekonvenční hrozby; kritická infrastruktura; vnitřní hrozba; psychologické ovlivňování.

Keywords: Active Reserve; Non-conventional Threats; Critical Infrastructure; Insider Threat; Psychological Influence.

ÚVOD

Současné bezpečnostní prostředí je charakterizováno rostoucí provázaností civilních a vojenských struktur a nárůstem hybridních hrozeb. Tyto hrozby rozostřují hranice mezi mírem a konfliktem. Státy i nestátní aktéři stále častěji využívají informační, ekonomické a psychologické prostředky k oslabení vůle a odolnosti společnosti bez nutnosti přímého vojenského střetu.

Jedním z citlivých prvků národní bezpečnosti je ochrana kritické infrastruktury (KI)[1]. V době krize nebo ohrožení státu mohou být do jejího střežení nasazeni i členové Aktivní zálohy Armády České republiky (AZ AČR), kteří doplňují profesionální složky a zajišťují ochranu vybraných objektů. Tento model přináší významné přínosy z hlediska obranné politiky a zapojení občanské společnosti, avšak současně vytváří nový typ zranitelnosti. Příslušníci Aktivní zálohy působí mimo každodenní vojenské struktury, často v civilním prostředí, a mohou se tak stát cílem infiltračních či vlivových operací nepřátelských aktérů.

Zatímco zahraniční bezpečnostní doktríny (např. NATO, EU, USA) dlouhodobě integrují problematiku tzv. *insider threats*[2] do systémů řízení rizik, v českém prostředí tato dimenze dosud není dostatečně rozpracována. Strategické dokumenty sice reflektují význam lidského faktoru, avšak chybí systematický rámec pro prevenci infiltrace, kognitivního ovlivňování a psychologického nátlaku na členy záloh.

Cílem článku je:

- Zmapovat a přehledně shrnout dosavadní poznatky o nekonvenčních formách infiltrace a ovlivňování vojenského personálu, se zvláštním zřetelem na Aktivní zálohu AČR.
- Identifikovat klíčové faktory zranitelnosti lidského prvku, které mohou zvyšovat riziko infiltrace či manipulace při ochraně kritické infrastruktury.
- Porovnat český přístup s vybranými zahraničními koncepcemi prevence *insider threats*.
- Formulovat návrhy opatření v rovině organizační, vzdělávací a bezpečnostně-psychologické, která by mohla posílit odolnost Aktivní zálohy a systému ochrany KI.

Článek odpovídá na otázky, jaké formy infiltrace mohou reálně ohrozit schopnost Aktivní zálohy plnit úkoly při ochraně KI, jaké jsou hlavní psychologické a organizační

1 Kritická infrastruktura – Systémy, *jejichž narušení by mělo závažný dopad na bezpečnost, ekonomiku nebo základní fungování státu – např. energetika, doprava, zdravotnictví či komunikační sítě.* (ISO, 2018)

2 Insider threat – Bezpečnostní *riziko pocházející zevnitř organizace – tedy od osoby s oprávněným přístupem, která může úmyslně nebo neúmyslně způsobit škodu.* (Shaw & Fischer, 2005)

faktory zranitelnosti a jak lze tyto faktory integrovat do systému řízení rizik. Přístup je přehledový a syntetický, vychází z analýzy domácí a zahraniční literatury, strategických dokumentů a komparace přístupů k ochraně lidského faktoru v ozbrojených silách a v systémech kritické infrastruktury.

Předkládaný článek má charakter přehledové a analytické studie (*literature review*), zaměřené na identifikaci a syntézu poznatků o infiltračních a kognitivních hrozbách v kontextu Aktivní zálohy AČR. Využívá metodu kvalitativní analýzy odborných a strategických dokumentů, zahraničních studií a norem z oblasti řízení rizik, bezpečnostní politiky a kognitivní bezpečnosti. Analýza je koncepčního a komparativního charakteru, přičemž se zaměřuje na srovnání českého institucionálního rámce s přístupy NATO, EU a USA. Cílem není empirické ověření hypotéz, ale vytvoření teoretického rámce pro pochopení rizik lidského faktoru a návrh preventivních opatření využitelných v praxi obranného plánování. Článek je koncipován jako přehledová analytická studie, která shrnuje a syntetizuje existující poznatky o nekonvenčních infiltračních rizicích v kontextu Aktivní zálohy AČR a ochrany kritické infrastruktury.

1 POSTAVENÍ AKTIVNÍ ZÁLOHY AČR V SYSTÉMU OBRANY STÁTU

Koncept Aktivní zálohy Armády České republiky představuje specifickou formu doplnění ozbrojených sil, která integruje civilní prvek do systému obrany státu a zvyšuje odolnost společnosti vůči krizím. (Ministry of Defence Czech Republic, 2020) Je právně zakotven v zákoně č. 45/2016 Sb., o službě vojáků v záloze, a zákoně č. 219/1999 Sb., o ozbrojených silách České republiky. Aktivní záloha doplňuje profesionální složky, podílí se na obraně území, ochraně vybraných objektů a podpoře složek integrovaného záchranného systému. (Ministry of Defence Czech Republic, 2019)

Zvláštní význam získává její zapojení do ochrany kritické infrastruktury, zejména během krizových stavů. Záložníci mohou zajišťovat ochranu energetických uzlů, dopravních terminálů, komunikačních center či průmyslových závodů, jejichž fungování je nezbytné pro obranu státu. Tento model zvyšuje schopnost AČR reagovat na rozsáhlé incidenty, ale současně vytváří zranitelnosti spojené s lidským faktorem. Členové AZ AČR působí většinu roku v civilním prostředí, mimo přímou vojenskou kontrolu, a jsou proto vystaveni vlivům, které mohou ovlivnit jejich postoje a rozhodování. (Černochová, 2025; Ghafir, 2018)

Strategické dokumenty (Ministry of Foreign Affairs Czech Republic, 2023) zmiňují význam lidského faktoru a odolnosti vůči hybridním hrozbám, avšak systematická prevence infiltrace či psychologického ovlivňování členů záloh dosud chybí. (Ministry of Foreign Affairs Czech Republic, 2023; Inayat, 2024) Dosavadní opatření se soustřeďují na bezpečnostní prověrky a základní vzdělávání v oblasti etiky a informovanosti. Tento přístup však nereflektuje současné formy cíleného působení na jednotlivce prostřednictvím digitálních kanálů, sociálních sítí či ekonomického nátlaku. (Paul & Matthews, 2016)

Z uvedeného vyplývá, že AZ AČR představuje současně přínosný i citlivý prvek systému obrany. Její silnou stránkou je propojení armády s civilní společností, avšak právě tato vazba zvyšuje pravděpodobnost infiltračního působení. To vyžaduje nové přístupy

k ochraně lidského faktoru, které překračují tradiční pojetí vojenské kázně a kontrolních mechanismů.

1.1 Hybridní hrozby a infiltrační dimenze lidského faktoru

Hybridní působení kombinuje vojenské, kybernetické, informační a ekonomické prostředky k dosažení politických cílů bez přímého vojenského střetu[3]. (Bachmann, 2021) V praxi se projevuje zejména působením v tzv. *grey zone*, kde jsou využívány techniky manipulace, dezinformací a infiltrace struktur, jejichž narušení může mít strategické dopady. Klasické pojetí hybridních hrozeb se tak rozšiřuje o oblast kognitivní a psychologické bezpečnosti, kde se cílem stává lidská mysl a rozhodovací proces. (Chong, 2022)

V tomto významu nabývá na významu pojem *insider threat* – tedy hrozba plynoucí zevnitř organizace, často zneužitím zaměstnance, člena nebo spolupracovníka. (Greitzer, Strom & Moore, 2019) Výzkumy ukazují, že v prostředí obranných struktur mohou být takoví jednotlivci ovlivňováni kombinací ideologických, osobních nebo ekonomických motivací. (Borum, 2020; Khan, 2021) Zvláště v prostředí záloh, kde jsou členové vystaveni dvojí identitě – civilní a vojenské – může docházet k postupnému posunu loajality či kognitivnímu ovlivnění. (Janis, 1982; Reason, 2016)

Hybridní aktéři využívají zpravodajské, informační i psychologické prostředky k cílenému oslabování soudržnosti jednotek, podkopávání důvěry a vytváření rozporů mezi loajalitou k armádě a osobními či občanskými postoji. (NATO COE, 2022) Takové působení je typické zejména pro tzv. *cognitive warfare*[4], v jehož rámci je lidská psychika považována za klíčové bojiště 21. století. (Paul & Matthews, 2016; Chong, 2022)

1.2 Normativní a bezpečnostní rámce

Řízení rizik spojených s lidským faktorem je dlouhodobě ukotveno v mezinárodních standardech. Norma ISO 31000:2018 zdůrazňuje potřebu integrovat lidský faktor do všech fází procesu řízení rizik – od identifikace po prevenci. (ISO, 2018) Směrnice NIS2 a pokyny ENISA dále rozšiřují tuto perspektivu o oblast kybernetické a organizační bezpečnosti, zejména u provozovatelů kritické infrastruktury. (ENISA, 2025)

V obranné sféře se obdobné principy uplatňují v rámci politik NATO a EU, které definují požadavky na ochranu vnitřní integrity a psychologickou odolnost personálu. Dokumenty Národní pracovní skupiny pro vnitřní hrozby (NITTF) / Úřad ředitele národního

3 Hybridní hrozby – Pojem *označuje koordinované využívání vojenských i nevojenských prostředků (např. kybernetických útoků, dezinformací, ekonomického tlaku či zpravodajských operací) s cílem dosáhnout strategických cílů bez vyhlášení války.* (Bachmann, 2021)

4 Cognitive warfare = Kognitivní doména – Součást *moderního pojetí války zaměřená na ovlivňování vnímání, rozhodování a morálky protivníka prostřednictvím informací, emocí a symbolů.* (Chong, 2022)

zpravodajství USA (ODNI) (NITTF & ODNI, 2024; Director of National Intelligence, 2019) a NATO Center Of Excelence (NATO COE, 2022) zdůrazňují multidisciplinární přístup – propojení bezpečnostní prověrky, vzdělávání a behaviorální analýzy. Česká republika zatím tyto rámce adaptuje jen částečně, zejména prostřednictvím koncepce výstavby AČR 2035 (Ministry of Defence Czech Republic, 2024) a zpráv NÚKIB o stavu kybernetické bezpečnosti. (NÚKIB, 2025)

Shrnuto, mezinárodní bezpečnostní rámce i odborná literatura se shodují, že lidský faktor je současně nejzranitelnějším a nejstrategičtějším prvkem systému obrany. Jeho ochrana vyžaduje nejen technická, ale i kognitivní a vzdělávací opatření, která snižují pravděpodobnost infiltrace, manipulace a zneužití.

2 NEKONVENČNÍ HROZBY A LISDKÝ FAKTOR V AKTIVNÍ ZÁLOZE AČR

Současné bezpečnostní prostředí se vyznačuje vysokou mírou propojení mezi vojenskými, informačními a společenskými procesy. Státní i nestátní aktéři proto stále častěji využívají nekonvenční formy působení, jejichž cílem je oslabit vůli a soudržnost protivníka bez přímého ozbrojeného střetu. (Rid & McBurney, 2012; Libicki, 2017) Tyto tzv. hybridní operace propojují kybernetické útoky, dezinformační kampaně, ekonomický nátlak a psychologické působení s cílem ovlivnit rozhodovací procesy a hodnotové postoje. Jejich klíčovou rovinou je kognitivní dimenze, zaměřená na manipulaci s informacemi a emocemi. (Paul & Matthews, 2016; Chong, 2022)

V tomto kontextu se zvláštní pozornost soustřeďuje na fenomén *insider threat* (Shaw & Fischer, 2005). Takové riziko může mít podobu úniku informací, sabotáže nebo psychologického působení, často bez přímého úmyslu aktéra. (Greitzer, Strom & Moore, 2019) V případě Aktivní zálohy Armády České republiky (AZ AČR) představuje tuto zranitelnost zejména propojení civilní a vojenské identity. Záložníci se pohybují mezi dvěma hodnotovými systémy, což může oslabovat pocit loajality a přináležitosti. (Černochová, 2025; Soeters, Winslow & Weber, 2006) Model MICE[5] přitom ukazuje, že motivy neloajálního jednání často pramení z kombinace finanční tísně, ideologického působení či osobní frustrace. (Borum, 2020)

Riziko infiltrace zvyšuje také sociální a digitální expozice záložníků. Dobrovolnický charakter služby vede k silné vnitřní kohezi, ale i k neformálním tlakům a uzavřenému myšlení, jež může oslabovat schopnost kritické reflexe. (Janis, 1982) Současně členové záloh běžně využívají otevřené komunikační platformy, kde se stávají cílem vlivových operací a dezinformací. (Paul & Matthews, 2016; NATO COE, 2022) Absence systematického vzdělávání v oblasti informační bezpečnosti a mediální gramotnosti tuto zranitelnost dále prohlubuje.

5 Model MICE (Money–Ideology–Coercion–Ego) - *Analytický rámec používaný k vysvětlení motivací osob ke spolupráci s nepřátelským aktérem: finanční zisk, ideologická identifikace, donucení a ego či potřeba uznání.* (Borum, 2020)

Z organizačního hlediska představuje problém omezená kontinuita velení, rotace personálu a nedostatečná koordinace mezi armádní a civilní složkou. Tyto faktory komplikují včasnou detekci změn v chování nebo psychologické zátěže. (Greitzer, Strom & Moore, 2019; Khan, 2021) Morální integrita, pocit uznání a důvěra ve vedení přitom fungují jako nejúčinnější prevence infiltračních hrozeb. (Bachmann, 2021) Prostředí, které umožňuje otevřenou komunikaci a poskytuje psychologickou podporu, je výrazně odolnější než hierarchicky uzavřená struktura. (Khan, 2021)

Z hlediska strategického řízení rizik se ukazuje, že efektivní obrana vůči nekonvenčním a kognitivním hrozbám vyžaduje systematické zapojení lidského faktoru do všech fází bezpečnostního plánování. To zahrnuje rozvoj mediální a kognitivní gramotnosti, behaviorální monitoring,[6] finanční stabilitu a etickou kulturu služby. (Reason, 2016; ENISA, 2025) V českém prostředí sice strategické dokumenty – Bezpečnostní strategie ČR 2023 a Koncepce výstavby AČR 2035 – reflektují hybridní a informační rizika (Ministry of Foreign Affairs Czech Republic, 2023; Ministry of Defence Czech Republic, 2024), nicméně komplexní přístup k prevenci *insider threat* v oblasti Aktivní zálohy zatím chybí.

Posílení odolnosti záložníků proto vyžaduje zavedení vzdělávacích programů zaměřených na kritické myšlení, digitální bezpečnost a psychologickou prevenci, doplněných o etické vedení a komunikaci důvěry. Takový model, vycházející z principů *human-centric security*[7], chápe člověka nikoli jako nejslabší článek systému, ale jako klíčový pilíř jeho stability a resilience.

3 ZAHRANIČNÍ PŘÍSTUPY K PREVENCI INFILTRACE A OVLIVŇOVÁNÍ

Prevence infiltrace a cíleného ovlivňování vojenského personálu je v zahraničních bezpečnostních systémech dlouhodobě chápána jako součást komplexního řízení rizik. Přístupy jednotlivých států se liší podle legislativních a organizačních rámců, avšak společným jmenovatelem je důraz na proaktivní práci s lidským faktorem – tedy kombinaci prověřování důvěryhodnosti, psychologické podpory a vzdělávání v oblasti informační a kognitivní bezpečnosti. (Greitzer, Strom & Moore, 2019; NATO COE, 2022)

3.1 Alianční a evropský rámec

NATO i Evropská unie chápou problematiku *insider threat* jako vícevrstvou hrozbu vyžadující propojení technických a behaviorálních přístupů. Dokument *NATO*

6 Behaviorální monitoring – Systematické *sledování změn v chování a postojích osob s cílem odhalit rané známky stresu, neloajality nebo infiltračního působení.* (Inayat, 2024)

7 Human-centric security = bezpečnost zaměřená na člověka – Koncept, *který chápe lidský faktor nikoli jako slabinu, ale jako klíčový prvek resilience systému. Zdůrazňuje vzdělávání, kulturu důvěry a psychologickou odolnost.* (ENISA, 2025)

Counter-Intelligence Policy (UK Ministry of Defence, 2021) a publikace *Insider Threats in Military Organizations* (NATO COE, 2022) stanovují tři pilíře prevence:

- *Trust but verify* – systematické prověrky a monitorování přístupu k citlivým informacím;
- Vzdělávání a resilience – pravidelný trénink o hybridních hrozbách, sociálním inženýrství a dezinformacích;
- Behaviorální indikátory – sledování změn v postojích a chování, které mohou signalizovat riziko infiltrace.

Tyto principy jsou integrovány do širšího konceptu *Cognitive Security*, jenž posiluje odolnost vůči psychologickým operacím a informačním manipulacím. (Chong, 2022) Praktická implementace probíhá v rámci aliančních cvičení Locked Shields či Cyber Coalition, kde se testují scénáře infiltrace lidského faktoru v prostředí kritických týmů. (NATO CCDCOE, 2023)

Evropská unie aplikuje obdobný přístup zejména v oblasti kybernetické bezpečnosti a ochrany kritické infrastruktury. Směrnice NIS2 z roku 2022 a *EU Cybersecurity Strategy* z roku 2020 ukládají členským státům povinnost zavést postupy pro ověřování důvěryhodnosti personálu, řízení přístupových práv a školení o manipulačních technikách. (European Commission, 2020; ENISA, 2019) Koordinační roli zde hraje *European Centre of Excellence for Countering Hybrid Threats*, který se zaměřuje na výměnu osvědčených postupů a posilování kognitivní odolnosti armádních i civilních struktur. (Hybrid COE, 2022)

3.2 Americký, britský a kanadský model

Spojené státy disponují nejrozvinutějším systémem prevence vnitřních hrozeb. Po událostech roku 2001 a úniku informací *Edwarda Snowdena* (v roce 2013) vznikl federální program *National Insider Threat Task Force* (Director of National Intelligence, 2019), koordinovaný US Ministry of Defence a ODNI (NITTF & ODNI, 2024). Americký model využívá integrovaný prediktivní přístup, který kombinuje bezpečnostní prověrky, kontinuální sledování digitální stopy a psychologické hodnocení. Systém *See Something, Say Something* podporuje včasné hlášení podezřelého chování bez obav z postihů. (U.S. Department of Defense, 2024) Paralelně běží výzkumný program *Countering Cognitive Warfare Initiative*, zaměřený na rozvoj kritického myšlení a psychologické odolnosti vojáků. (U.S. Army War College, 2023)

Velká Británie i Kanada zvolily holistický přístup propojující bezpečnostní, etickou a psychologickou dimenzi. Britské Counter-Intelligence and Security Directorate, Ministry of Defence provozuje systém *Vetting & Behavioural Monitoring*, který kombinuje prověrky, koučink a školení etické odolnosti. (UK Ministry of Defence, 2021) Kanada implementovala strategii *Human Security and Resilience in Defense* (Department of National Defence Canada, 2021), jež akcentuje psychologické zdraví, otevřenou komunikaci a vzdělávání o kognitivních hrozbách. Oba modely staví na kultuře důvěry a transparentnosti, nikoli na represivním dohledu, čímž podporují dlouhodobou loajalitu personálu.

3.3 Implikace pro české prostředí

Zahraniční praxe ukazuje, že účinná prevence infiltrace musí být součástí kultury organizace, nikoli izolovaným opatřením. Klíčové principy lze shrnout následovně:

- Integrace lidského faktoru do systému řízení rizik;
- Multidisciplinární spolupráce bezpečnostních, psychologických, IT a personálních složek;
- Vzdělávání zaměřené na kognitivní odolnost a mediální gramotnost;
- Otevřená komunikace a důvěra mezi vedením a personálem;
- Využití datové a behaviorální analýzy pro včasnou detekci anomálií.

Pro Českou republiku z toho vyplývá potřeba rozšířit rámec bezpečnostních prověrek o systematické vzdělávání členů Aktivní zálohy, zejména v oblasti psychologické odolnosti, informační bezpečnosti a rozpoznávání vlivových technik. Inspirací může být alianční koncept Cognitive Security, který kombinuje technické a lidské dimenze ochrany, a tím posiluje celkovou odolnost systému obrany státu i kritické infrastruktury.

4 MOŽNOSTI PREVENCE A MITIGACE V PODMÍNKÁCH ČR

Ochrana obranného systému České republiky před nekonvenčními hrozbami vyžaduje systematické uchopení problematiky infiltrace a cíleného ovlivňování lidského faktoru, zejména v rámci Aktivní zálohy Armády ČR. Tato složka propojuje civilní a vojenské prostředí, čímž posiluje flexibilitu ozbrojených sil, ale současně vytváří prostor pro infiltrační, psychologické a informační působení. Zkušenosti NATO, EU i USA ukazují, že efektivní ochranou není represivní kontrola, nýbrž prevence založená na vzdělávání, včasné detekci rizik a posilování kognitivní odolnosti. (NITTF & ODNI, 2024; NATO COE, 2022)

4.1 Modelové hrozby a prostředí infiltrace

Zahraniční praxe potvrzuje, že infiltrace probíhá nejčastěji kombinací tří dimenzí – informační, sociální a finanční. (Bachmann, 2021; Bartlett & Miller, 2012) Typickým scénářem je situace, kdy záložník aktivní na sociálních sítích naváže kontakt s osobou vystupující jako bývalý voják či odborník, která postupně získává jeho důvěru, ovlivňuje jeho postoje a nabízí finanční nebo profesní výhody. Takový proces často probíhá nenápadně, v delším časovém horizontu, a vede k erozi loajality i šíření citlivých informací.

Prevence těchto jevů vyžaduje citlivé, nikoli represivní nástroje. Klíčovým opatřením je vzdělávání v oblasti digitální hygieny, informační bezpečnosti a rozpoznávání manipulačních technik. Každý výcvik členů AZ AČR by měl zahrnovat modul o bezpečném chování v online prostoru a práci s dezinformacemi. (Ministry of Defence Czech Republic, 2024) Doporučuje se rovněž zřídit etický kodex komunikace na sociálních sítích a dobrovolný

systém monitoringu otevřených zdrojů (OSINT) zaměřený na odhalování falešných profilů a infiltračních aktivit. (Paul & Matthews, 2016)

4.2 Prevenční mechanismy

Lidská zranitelnost často nesouvisí s ideologií, ale s psychologickým tlakem a osobními problémy. Mezi nejvýznamnější faktory patří finanční potíže, které podle modelu MICE[8] představují častý motiv k neloajálnímu jednání. (Borum, 2020) Doporučuje se proto vytvořit preventivní poradenský rámec umožňující diskrétní konzultace s finančními poradci a vojenskými psychology, který by pomáhal řešit ekonomické i osobní problémy bez stigmatizace.

U Aktivní zálohy nasazované k ochraně kritické infrastruktury by měly být součástí personálního hodnocení indikátory finanční stability a psychické zátěže, a to v souladu s principy ochrany osobních údajů. Takový přístup odpovídá metodice amerického Ministerstva obrany, kde jsou finanční obtíže považovány za včasný varovný signál infiltrace. (Greitzer, Strom & Moore, 2019)

Součástí prevence by měla být i kognitivní a mediální gramotnost. Výcvik by měl využívat interaktivní metody – scénářové simulace, table-top cvičení či modelové situace psychologických operací, které učí záložníky rozpoznávat dezinformační techniky a argumentační manipulaci. (ENISA, 2025; NATO CCDCOE, 2023) Doporučuje se zavést povinný kurz *Kognitivní bezpečnost a kritické myšlení*, který by byl součástí základního i opakovacího výcviku AZ AČR.

4.3 Kultura bezpečnosti a komunikace důvěry

Prevence může být účinná pouze tehdy, pokud je založena na otevřené a důvěryhodné organizační kultuře. Důležitou součástí je vytvoření prostředí, kde je běžné sdílet obavy, nejistoty či podezřelé chování bez rizika sankce. Model *See something, say something* využívaný v USA či Kanadě (NITTF & ODNI, 2024; Department of National Defence Canada, 2021) ukazuje, že neformální komunikace a dostupnost konzultačních kanálů (vojenský psycholog, mentor, kaplan) významně zvyšují šanci na včasné odhalení infiltrace.

Prostředí důvěry musí být posíleno jasnými etickými pravidly, pozitivní motivací a transparentním vedením. Bezpečnostní kultura postavená na loajalitě, vzdělávání a vzájemném respektu představuje nejúčinnější nástroj dlouhodobé prevence.

[8] Model MICE je analytický rámec používaný v oblasti kontrašpionáže a bezpečnostních studií, který vysvětluje motivace neloajálního jednání jednotlivců prostřednictvím čtyř základních faktorů: finančního zisku (Money), ideologie (Ideology), donucení (Coercion) a ega či potřeby uznání (Ego). (Borum, 2020)

4.4 Doporučení

Pro podmínky České republiky lze formulovat tyto klíčové kroky:

- Zavedení povinného výukového modulu *Kognitivní bezpečnost a kritické myšlení* pro všechny členy AZ AČR;
- Vytvoření metodiky bezpečného chování na sociálních sítích a systému OSINT monitoringu;
- Zřízení poradenské platformy pro finanční a psychologickou prevenci nátlaku;
- Implementace anonymního systému hlášení podezřelých kontaktů;
- Prohloubení spolupráce Ministerstva obrany, NÚKIB a akademické sféry při výzkumu lidského faktoru.

Dlouhodobě udržitelná obrana proti infiltračním a psychologickým hrozbám vyžaduje kombinaci vzdělávání, finanční stability, etické kultury a kritického myšlení. Takový přístup posiluje nejen odolnost členů Aktivní zálohy, ale i důvěryhodnost a stabilitu celého systému ochrany kritické infrastruktury České republiky.

5 DISKUZE

Zjištění potvrzují, že infiltrace a cílené ovlivňování členů Aktivní zálohy AČR představují komplexní bezpečnostní riziko, které se dotýká lidského faktoru, informační integrity i organizační stability. Současný rámec AČR poskytuje funkční právní a kontrolní základ, avšak postrádá integrovaný přístup, který by tyto dimenze spojil do jednotného systému řízení rizik v souladu s principy ISO 31000:2018. (ISO, 2018; Ministry of Defence Czech Republic, 2024)

5.1 Lidský faktor a informační prostředí jako klíčové proměnné rizika

Moderní přístup k bezpečnosti chápe člověka jako nejsilnější i nejzranitelnější článek systému. (Greitzer, Strom & Moore, 2019) Lidský faktor proto musí být hodnocen stejně systematicky jako technologická či kybernetická infrastruktura. To zahrnuje indikátory loajality, morální integrity, finanční stability i mediální expozice personálu. (Bachmann, 2021; Borum, 2020)

Informační prostředí, v němž se prolíná civilní a vojenská sféra, představuje významný zdroj rizik. Sociální sítě a online komunity se staly nástrojem infiltračních a psychologických operací zaměřených na záložníky působící mimo vojenské struktury. (Paul & Matthews, 2016) Z pohledu řízení rizik je proto nutné k informačnímu prostoru přistupovat obdobně jako k fyzické infrastruktuře – monitorovat, analyzovat a vzdělávat. Preventivní strategie by měly zahrnovat mediální gramotnost, kritické myšlení a včasnou detekci psychologických operací. (ENISA, 2025; NATO CCDCOE, 2023)

5.2 Psychologická, sociální a finanční stabilita jako prediktory loajality

Ekonomická i osobní stabilita mají přímý dopad na chování jednotlivce a jeho odolnost vůči nátlaku. Finanční problémy, zadlužení či pocit nedocenění patří mezi hlavní motivační faktory ke spolupráci s nepřátelským aktérem. (Borum, 2020) V zahraničí jsou tyto aspekty běžně integrovány do bezpečnostních prověrek a preventivních poradenských programů (NITTF & ODNI, 2024).

Pro české prostředí je žádoucí zavést diskrétní mechanismy včasné detekce – anonymní konzultační kanály, finanční a psychologické poradenství či systém dobrovolných screeningů. Současně je nutné rozvíjet vzdělávání zaměřené na kognitivní odolnost, které posiluje schopnost rozpoznávat manipulaci a stresové faktory ohrožující loajalitu. (UK Ministry of Defence, 2021; Department of National Defence Canada, 2021)

5.3 Organizační kultura, vzdělávání a meziresortní koordinace

Nejúčinnější prevencí je kultura bezpečnosti založená na důvěře, vzdělání a otevřené komunikaci. (Greitzer, Strom & Moore, 2019) Vedení by mělo vytvářet prostředí psychologické bezpečnosti, kde lze upozornit na podezřelé chování bez obav z postihu. Tím se posiluje morální integrita

i kolektivní odolnost organizace.

Z pohledu řízení kritické infrastruktury je nezbytné chápat členy AZ AČR jako součást širšího bezpečnostního ekosystému. Jejich výcvik a prověřování by měly být sladěny s postupy provozovatelů KI, zejména v oblastech energetiky, dopravy a komunikací. To vyžaduje meziresortní spolupráci Ministerstva obrany, Ministerstva vnitra a NÚKIB, včetně společných krizových simulací a red-teamových cvičení. (NÚKIB, 2025)

Integrace lidského faktoru do rámce ISO 31000:2018 Risk Management může vytvořit jednotný systém hodnocení rizik v celé infrastruktuře státu. Spojením technických, psychologických a organizačních přístupů lze zvýšit odolnost českého obranného systému vůči nekonvenčním hrozbám a minimalizovat riziko infiltrace v prostředí Aktivní zálohy.

Diskuse potvrzuje, že odolnost vůči nekonvenčním hrozbám není pouze otázkou technických prostředků, ale především lidského faktoru. V podmínkách České republiky je klíčové propojit bezpečnostní prověrky, finanční stabilitu a vzdělávání v oblasti kritického myšlení do jednoho konzistentního rámce. Takto pojatá prevence zvyšuje nejen bezpečnost vojenského personálu, ale i stabilitu celého systému ochrany kritické infrastruktury.

ZÁVĚR

Současné bezpečnostní prostředí je charakterizováno rostoucí provázaností civilních a vojenských struktur, což zvyšuje význam lidského faktoru jako klíčového prvku obranyschopnosti státu. Aktivní záloha Armády České republiky představuje most mezi společností

a ozbrojenými silami, avšak tato hybridní pozice z ní činí také zranitelný cíl infiltračního a psychologického působení. Analýza ukázala, že nekonvenční hrozby, zejména informační manipulace, finanční nátlak a ideologické ovlivňování, mohou významně ovlivnit integritu a efektivitu obranného systému. Nejúčinnější ochranou proto není pouhá kontrola, ale prevence postavená na vzdělávání, finanční a psychologické stabilitě a posilování kognitivní odolnosti členů záloh. (Greitzer, Strom & Moore, 2019; NATO COE, 2022)

Pro praxi z toho vyplývá nutnost integrovat lidský faktor do systému řízení rizik v souladu s principy ISO 31000 a NIS2. Prioritou by mělo být zavedení vzdělávacích programů kognitivní bezpečnosti, rozvoj mediální a digitální gramotnosti a vytvoření metodiky bezpečného chování na sociálních sítích. Důležité je rovněž posílení finančního a psychologického poradenství a zavedení anonymních konzultačních kanálů, které umožní včasnou detekci stresových nebo nátlakových faktorů. Na strategické úrovni se doporučuje meziresortní platforma propojující Ministerstvo obrany, NÚKIB, Ministerstvo vnitra a provozovatele kritické infrastruktury pro sdílení poznatků o infiltračních a vlivových hrozbách. (NÚKIB, 2025)

Závěry této studie vycházejí z analýzy sekundárních zdrojů, oficiálních dokumentů a odborné literatury. Článek proto nepředstavuje empirický výzkum a jeho závěry mají převážně teoreticko-analytický charakter. Další výzkum by měl být zaměřen na kvantitativní a kvalitativní ověření zjištěných hypotéz, obzvláště v oblasti psychologické odolnosti, vlivových mechanismů a institucionální praxe Aktivní zálohy AČR.

Budoucí výzkum by měl empiricky zkoumat zranitelnost lidského faktoru v Aktivní záloze AČR, zejména vztah mezi vzděláním, psychickou odolností a náchylností k manipulaci. Perspektivní oblast představuje využití behaviorální analýzy a umělé inteligence pro včasnou detekci anomálního chování a vývoj integrovaného modelu psychologické a organizační resilience. Dlouhodobá bezpečnost státu totiž nespočívá pouze v technologiích, ale v odolnosti, loajalitě a vzdělanosti lidí, kteří systém tvoří. Aktivní záloha může být buď slabinou, nebo pilířem obrany, podle toho, jak budou řízení rizik, vzdělávání a prevence začleněny do strategické kultury bezpečnosti České republiky.

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

SEZNAM ZDROJŮ

Bachmann, S. D. 2021. *Hybrid Threats and the Law of Armed Conflict: Grey Zone Conflicts Examined*. Cham: Springer. ISBN 978-3-030-62682-2.

Bartlett, J. and Miller, C. 2012. "The Edge of Violence: Towards Telling the Difference Between Violent and Non-Violent Radicalization". *Terrorism and Political Violence*, 24(1), pp. 1–21. ISSN 0954-6553.

Borum, R. 2020. *Psychology of Terrorism and Violent Extremism*. New York: Routledge. ISBN 978-0-367-46683-8.

Černochová, V. 2025. „Analýza výcviku a nasazení Aktivní zálohy AČR“. *Vojenské rozhledy*, 34(1), pp. 42–57. ISSN 1210-3292.

Department of National Defence (Canada). 2021. *Human Security and Resilience in Defense*. Ottawa: Government of Canada. ISBN 978-0-660-40713-5.

Director of National Intelligence (DNI). 2019. *National Insider Threat Task Force – Strategic Plan 2019–2024*. Washington, DC: Office of the Director of National Intelligence.

ENISA (European Union Agency for Cybersecurity). 2019. *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. Athens/Brussels: ENISA.

ENISA (European Union Agency for Cybersecurity). 2025. *Technical Implementation Guidance on Cybersecurity Risk-Management Measures (NIS2)*. Version 1.0. Athens: ENISA. ISBN 978-92-9204-637-2. Available at: https://www.enisa.europa.eu/publications/technical-implementation-guidance-on-cybersecurity-risk-management-measures-nis2.

European Commission. 2020. *The EU Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission. ISBN 978-92-76-25334-3.

Ghafir, I. 2018. “Security Threats to Critical Infrastructure: The Human Factor”. *The Journal of Supercomputing*, 74(12), pp. 6794–6817. ISSN 0920-8542.

Greitzer, F. L., Strom, B. K. and Moore, A. P. 2019. *Analysis of Insider Threat Mitigation Strategies in Defense Organizations*. Washington, DC: Carnegie Mellon University. ISBN 978-1-937473-98-4.

Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats). 2022. *Annual Report 2022*. Helsinki: Hybrid CoE. ISBN 978-952-7472-20-5.

Chong, A. 2022. *Cognitive Warfare: The Battle for the Human Mind*. Rome: NATO Defense College, Research Paper No. 15. ISSN 2617-9748.

Inayat, U. 2024. “Insider Threat Mitigation: Systematic Literature Review”. *Computers & Security*, 135, art. 102085. ISSN 0167-4048.

ISO (International Organization for Standardization). 2018. *ISO 31000:2018 Risk Management — Guidelines*. Geneva: ISO. ISBN 978-92-67-10604-6.

Janis, I. L. 1982. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*. Boston: Houghton Mifflin. ISBN 978-0-395-31787-2.

Khan, N. 2021. “Understanding Factors that Influence Unintentional Insider Behaviour”. *Frontiers in Psychology*, 12, art. 732041. ISSN 1664-1078.

Libicki, M. C. 2017. *What Is Information Warfare?* Washington, DC: National Defense University Press. ISBN 978-1-58487-743-1.

Ministry of Defence (Czech Republic). 2019. *The Czech Armed Forces Development Concept 2030*. Prague: Ministry of Defence. ISBN 978-80-7278-748-1.

Ministry of Defence (Czech Republic). 2024a. *The Czech Armed Forces: Vision of Future Warfare Beyond 2040*. Prague: Ministry of Defence.

Ministry of Defence (Czech Republic). 2024b. *Koncepce výstavby Armády České republiky 2035*. Praha: Ministerstvo obrany ČR.

Ministry of Foreign Affairs (Czech Republic). 2023. *Security Strategy of the Czech Republic 2023*. Prague: Ministry of Foreign Affairs.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2023. *Cyber Defence Exercises: Locked Shields*. Tallinn: NATO CCDCOE.

NATO Centre of Excellence for Defence Against Terrorism. 2022. *Insider Threats in Military Organizations*. Brussels: NATO COE. ISBN 978-92-845-0215-8.

National Insider Threat Task Force (NITTF) / Office of the Director of National Intelligence (ODNI). 2024. *Insider Threat Guide to Accompany the National Insider Threat Policy and Minimum Standards*. Washington, DC: ODNI.

NÚKIB. 2025. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024*. Brno: Národní úřad pro kybernetickou a informační bezpečnost.

Paul, C. and Matthews, M. 2016. *The Russian "Firehose of Falsehood" Propaganda Model*. Santa Monica, CA: RAND Corporation. ISBN 978-0-8330-9348-0.

Reason, J. 2016. *Managing the Risks of Organizational Accidents*. Farnham: Ashgate. ISBN 978-1-4724-7004-8.

Rid, T. and McBurney, P. 2012. "Cyber-Weapons". *The RUSI Journal*, 157(1), pp. 6–13. ISSN 0307-1847.

Shaw, E. D. and Fischer, L. F. 2005. *Ten Tales of Betrayal: The Threat to Corporate Infrastructure by Information Technology Insiders – Analysis and Observations*. Washington, DC: Defense Personnel Security Research Center. ISBN 978-1-932946-05-9.

Soeters, J., Winslow, D. and Weber, G. 2006. "Military Culture". In: Caforio, G. (ed.), *Handbook of the Sociology of the Military*. New York: Springer, pp. 237–254. ISBN 978-0-387-32456-3.

UK Ministry of Defence. 2021. *JSP 440: Defence Manual of Security – Personnel Security*. London: Ministry of Defence.

U.S. Department of Defense. 2024. *DoD Instruction 5205.16: The Insider Threat Program*. Washington, DC: Department of Defense.

US Army War College. 2023. *Countering Cognitive Warfare: Concepts, Challenges, and Implications*. Carlisle Barracks, PA: Strategic Studies Institute.