VOJENSKÉ ROZHLEDY

Czech Military Review

3

2020

VOJENSKOTEORETICKÝ ČASOPIS

VOJENSKÉ ROZHLEDY

3

ROČNÍK 29 (61)

 DOI: 10.3849/2336-2995.29.2020.03.003-024

Recenzovaný článek

Řízení rizik v procesu plánování rozvoje Armády České republiky

Risk Management in the Armed Forces of the Czech Republic Development Planning Process

Miroslav Chylík, Josef Procházka

Abstrakt: Autoři předkládají výsledky výzkumu, který se zaměřil na posouzení současného stavu řízení rizik v procesu plánování rozvoje Armády České republiky. Na základě zjištěných výsledků a zvážení soudobých teoretických poznatků a přístupů nejlepší praxe navrhují ucelený přístup k řízení rizik v procesu plánování rozvoje. Smyslem návrhu je posunout řídící praxi od administrativního pojímání tohoto procesu odtrženého od zájmu vedoucích pracovníků směrem k uplatňování řízení rizik jako účinného manažerského nástroje v prostředí rostoucí míry nejistoty. Jako vhodný nástroj předkládají tzv. plán řízení rizik a možný způsob jeho implementace do podmínek Armády České republiky.

Abstract: The authors offer the research outcome focusing on the assessment of risk management practices applied in the Armed Forces development planning process. Based on analytical outcomes, contemporary theory and best practices authors outline comprehensive approach to risk management within the Armed Forces development planning process. The purpose of the article is to enhance effectiveness of existing managerial process and elevate risk management from rather administrative exercise to effective management tool in the time of growing level of uncertainty. As the most suitable instrument, the Risk Management Plan is developed including the necessary implementation measures within the Armed Forces of the Czech Republic.

Klíčová slova: Plánovací proces; plánování rozvoje; cíl; úkol; riziko; řízení rizik; plán řízení rizik.

Key words: Planning Process; Development Planning Process; Objective; Task; Risk; Risk Management; Risk Management Plan.

ÚVOD

Řízení rizik je nedílnou součástí řídící praxe každé úspěšné organizace. V prostředí s rostoucí mírou nejistoty nelze v podstatě dosáhnout ideálního stavu, kdy nebude vystavena žádnému riziku. Důvodem je působení okolního prostředí a vždy omezená dostupnost zdrojů nezbytných k dosažení stanovených cílů. Pokud nejsou rizika vhodným způsobem řešena, mají následné dopady zpravidla negativní vliv na schopnost organizace naplňovat své poslání.

Řízení rizik lze chápat jako proces, kdy se organizace snaží nalézt a aplikovat řešení, které umožní omezit negativní dopady související s existencí rizik. Správně aplikovaný systematický přístup k řízení rizik s jasně nastavenými pravidly napomáhá k omezení nepříznivých dopadů prostřednictvím včasné identifikace, ohodnocení rizika a přijetí opatření vedoucích k omezení rizika. Umožňuje reflektovat požadavky a omezení vnějšího prostředí, realisticky stanovit potřeby organizace z pohledu zdrojů, koordinovat plánovací aktivity, a účelně, efektivně a hospodárně řídit rozvoj schopností. Zároveň má potenciál přispět k motivaci nejen řídících pracovníků, ale i všech zainteresovaných stran podílet se na dalším rozvoji organizace.[1]

V podmínkách ČR jsou požadavky na řízení rizik stanoveny zákonem.[2] Řízení rizik by nemělo být vnímáno pouze jako povinnost při správě svěřených aktiv, ale zároveň jako příležitost k dosažení maximálních možných výsledků prostřednictvím omezení dopadů hrozeb a správného nastavení priorit na cestě ke splnění cílů organizace.

V rámci rezortu Ministerstva obrany (ReMO) je komplexní systém řízení rizik vytvářen od roku 2013.[3] V podřízenosti NGŠ AČR je koordinací řízení rizik pověřen ředitel Sekce plánování schopností.[4] Rizika jsou identifikována, analyzována a hodnocena ve všech oblastech činnosti ReMO.[5] Řízení rizik je tedy prováděno i v rámci existujících plánovacích procesů.[6]

Vzhledem ke skutečnosti, že v reálném světě neexistuje organizace, která by mohla být plně spokojena s nastavením svých vnitřních procesů, realizovali autoři výzkum, který byl zaměřen na posouzení současné řídící praxe s cílem identifikovat odchylky od soudobých teoretických poznatků a přístupů nejlepší praxe řízení rizik a navrhnout ucelený přístup vedoucí k posílení účinnosti řízení rizik v procesu plánování rozvoje AČR.

---

1 *NATO ARAMP-1: NATO Risk Management Guide For Acquisition Programmes*, str. 3.

2 *Zákon č. 320/2001 Sb.: Zákon o finanční kontrole ve veřejné správě.*

3 PITAŠ, Jaromír, CRHÁK, Milan. *Řízení rizik jako podpora rozhodovacího procesu v resortu Ministerstva obrany*, str. 114-124.

4 *Organizační řád Ministerstva obrany ze dne 17. prosince 2019*

5 *Rozkaz ministra obrany č. 20: Řízení rizik v rezortu Ministerstva obrany.*

6 *Rozkaz ministra obrany č. 66: Plánování činnosti a rozvoje v rezortu Ministerstva obrany*.

1 METODOLIGICKÝ RÁMEC

Pro hodnocení současného stavu řízení rizik v procesu plánování rozvoje Armády České republiky (AČR) byla provedena obsahová analýza odborné literatury a vnějších a vnitřních regulátorů řízení. Provedeno bylo dotazníkové šetření a polostrukturované rozhovory s vybranými odborníky z praxe (správci rizik a manažeři cílů 3. úrovně). Jednalo se o reprezentativní vzorek odborníků z nejvyšší úrovně velení AČR.

Na získané datové podklady byla aplikována metoda logické indukce k vytvoření závěrů obecnějšího charakteru.

K hodnocení současného stavu řízení rizik byla využita analýza SWOT. Analýza vnitřních silných a slabých stránek byla provedena s využitím tzv. funkčních oblastí (doktriny – D; organizace – O; výcvik –T; materiál – M; velení a řízení – L; personál – P; infrastruktura – F; interoperabilita – I). Pro strukturovanou analýzu vnějšího prostředí zahrnující příležitosti a hrozby pro další rozvoj systému řízení rizik v podřízenosti NGŠ byla využita metoda PESTLEM (politika – P; ekonomika – E; sociální oblast – S; technologie – T; právo – L; prostředí – E; vojenství – M).

Při tvorbě návrhu byly využity přístupy nejlepší praxe identifikované v rámci obsahové analýzy domácích i zahraničních pramenů. S využitím syntézy získaných poznatků a metody analogie aplikované zejména na systém řízení rizik využívaný v USA[7] byly zpracovány návrhy využitelné v prostředí AČR, resp. ReMO.

Návrhová část byla zaměřena primárně na úpravu znění vnitřních regulátorů řízení pro plánování činnosti a rozvoje ReMO. V rámci tvorby návrhu řízení rizik byla pozornost zaměřena na řízení rizik v podřízenosti NGŠ AČR, a to pro potřeby plánování rozvoje AČR.

2 VAZBA MEZI SYSTÉMEM ŘÍZENÍ RIZIK A SYSTÉMEM PLÁNOVÁNÍ

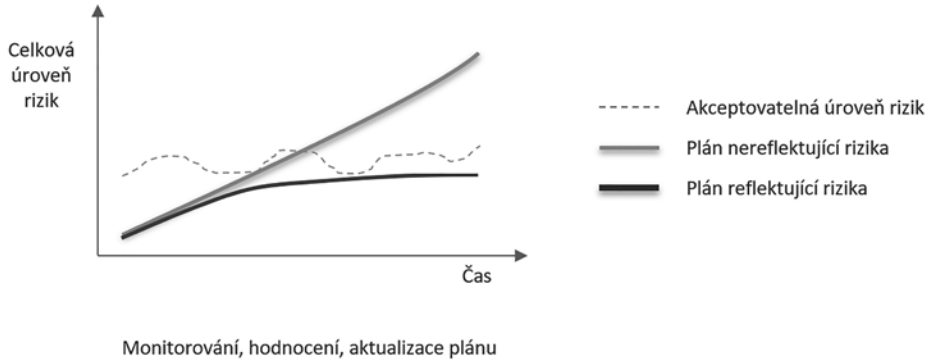
Proč se zamýšlíme nad využitím řízení rizik v procesu plánování? Odpověď je poměrně jednoduchá. Každý plán je zatížen významnou mírou nejistoty. Nejistota může být spojena s vývojem jak vnějšího prostředí, tak i s vývojem dostupných zdrojů. Snahou plánovacích orgánů je vytvářet realistické plány a vytvořit co nejlepší podmínky pro jejich realizaci. Důležitým aspektem je, aby omezené prostředky byly alokovány na realizaci těch nejvýznamnějších priorit, přičemž priority v sobě odrážejí nejvyšší míru rizika pro zajištění bezpečnosti občanů a obrany státu a plnění úkolů ze strany AČR.

V tomto smyslu je důležité, aby především tvorba rozvojových plánů byla podpořena odpovídajícími nástroji pro řízení rizik, protože tyto plány mají dlouhodobý charakter a jsou zatíženy nejvýznamnější mírou nejistoty.

7 *ATP 5-19: Risk Management*. Washington, DC: Headquarters, Department of the Army, 2014; *Composite Risk Management*. Washington, DC: Headquarters, Department of the Army, 2006.

Plán rozvoje lze chápat jako záměr adaptace organizace na uskutečněnou nebo očekávanou změnu vnějšího prostředí při zohlednění interních faktorů. Vyjadřuje zámysl řešení požadavků vycházejících ze strategické úrovně řízení prostřednictvím stanovených priorit, hlavních úkolů reagujících mj. na strategické hrozby a související rizika, a dále pak požadavků souvisejících s běžným životem organizace při naplňování jejího poslání.

Cílem procesu řízení rizik při plánování rozvoje organizace by mělo být napomoci usměrnit plány organizace takovým způsobem, aby se úroveň souvisejících rizik pohybovala na akceptovatelné úrovni, a tím byly vytvořeny vhodné podmínky pro jejich realizaci. Vztah mezi adaptací organizace a celkovou úrovní rizik je naznačen na obrázku č. 1.



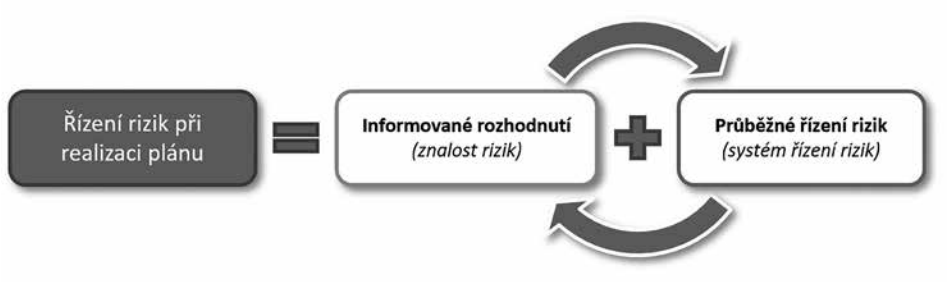
Obrázek č. 1: Adaptační opatření ke snížení rizik
Zdroj: NASA 2012 Climate Risk Management Plan and Report[8]

Integrace řízení rizik do procesu plánování rozvoje napomáhá k posílení schopnosti adaptace organizace na změny vnějšího prostředí a jejímu efektivnímu rozvoji.

Tvorba plánu probíhá obvykle iterativním způsobem, tj. dochází k jeho postupnému zpřesňování a optimalizaci až do okamžiku, kdy je zajištěna jeho technická a ekonomická realizovatelnost[9]. Identifikovaná rizika jsou v tomto případě jedním z významných faktorů, které je třeba zohlednit. Na řízení rizik v procesu plánování rozvoje lze poté pohlížet jako na kombinaci informovaného rozhodnutí na základě znalosti rizik a kontinuálně prováděného řízení rizik, jak naznačuje obrázek č. 2.

8 *NASA 2012 Climate Risk Management Plan and Report.*, str. 8

9 FOTR, Jiří, VACÍK, Emil, SOUČEK, Ivan, ŠPAČEK, Miroslav, HÁJEK, Stanislav. *Tvorba strategie a strategické plánování (Teorie a praxe)*, str. 88.



Obrázek č. 2: *Řízení rizik při realizaci plánu rozvoje*
Zdroj: NASA Risk management handbook[10]

Účinné plánování rozvoje AČR se neobejde bez silné podpory, která spočívá především v řízení rizik založeném na znalostech. Řízení rizik není možné vnímat jako administrativní zátěž, ale je nezbytné je posunout do kategorie nezbytných manažerských nástrojů v době enormního nárůstu míry nejistoty, v jejímž rámci jsou plány připravovány, následně realizovány a hodnoceny.

3 ANALÝZA SOUČASNÉHO STAVU

Kapitola odpovídá na otázku, jaké je systémové nastavení řízení rizik v ReMO a do jaké míry podporuje řízení rizik proces plánování rozvoje AČR. V kapitole budou předloženy závěry z komplexního hodnocení řízení rizik. Pozornost bude zaměřena na posouzení regulátorů řízení, SW nástroje a názory odborníků. Předložena bude komplexní matice SWOT hodnotící vnitřní i vnější prostředí řízení rizik.

3.1 Hodnocení regulátorů řízení

Systém řízení rizik v ReMO směřuje k naplnění požadavků stanovených **zákonem o finanční kontrole ve veřejné správě**. Hlavním cílem je zajištění ochrany veřejných prostředků proti rizikům, nesrovnalostem nebo jiným nedostatkům způsobených zejména porušením právních předpisů, nehospodárným, neúčelným a neefektivním nakládáním s veřejnými prostředky nebo trestnou činností. Zákon ukládá všem vedoucím zaměstnancům orgánu veřejné správy v rámci vymezených povinností, pravomocí a odpovědností povinnost zajistit fungování vnitřního kontrolního systému a zároveň podávat vedoucímu

10 *NASA Risk Management Handbook*, str. 3.

orgánu veřejné správy včasné a spolehlivé informace o vzniku významných rizik, o závažných nedostatcích v činnosti orgánu veřejné správy a o přijímaných a plněných opatřeních k jejich nápravě.[11]

V podmínkách ReMO je řízení rizik prováděno podle **rozkazu ministra obrany – řízení rizik**.[12] Systém řízení rizik je pojímán jako součást systému řízení a vnitřní kultury MO, přičemž rizika jsou řízena ve všech oblastech činnosti ReMO. Základními komponenty systému řízení rizik jsou subjekty, procesy a programové vybavení k podpoře procesu řízení rizik. Dokumenty v systému řízení rizik jsou vedeny v elektronické podobě v rámci určeného SW nástroje „Modul rizik". Proces řízení rizik zahrnuje následující fáze (identifikační, analytická a hodnoticí; zvládání rizik; monitorovací, komunikační a vykazovací), které jsou v souladu s mezinárodním standardem.[13]

Metodické pokyny[14] objasňují způsob řízení rizik v jednotlivých fázích procesu řízení rizik a poskytují podrobný návod k SW aplikaci. Jednoznačné odpovědi na otázky „proč" a „jakým způsobem" rizika řídit, jak je provázat a sladit nejsou metodicky rozpracovány.

V procesu plánování ReMO je řízení rizik spojeno především s hodnocením činnosti a rozvoje.[15] Tento proces zahrnuje průběžné a čtvrtletní hodnocení plnění opatření a úkolů, které mj. ukládá řídícím pracovníkům informovat své přímé nadřízené o zjištěných nedostatcích a identifikovaných rizicích. Pololetní a roční vyhodnocení cílů zahrnující vyhodnocení cíle včetně návrhů na odstranění nedostatků, zvládání agregovaných rizik a z toho vyplývající návrh na úpravy dokumentace cíle předkládají manažeři cílů 1. úrovně k projednání v Radě ministra obrany pro plánování.[16] Vyhodnocení činnosti a rozvoje ReMO obsahuje roční hodnocení za cíle první úrovně a pololetní hodnocení rizik včetně vyhodnocení rizik. Součástí přehledu za 1. pololetí roku 2019 byla pouze závažná rizika identifikovaná v rámci cyklu bez systémovější vazby na nadřazené dokumenty. Zpráva o zajišťování obrany státu je zpracovávána na začátku kalendářního roku za předchozí rok. Hodnotí stav připravenosti státu k zajišťování své obrany v duchu zákona č. 222/1999 Sb., o zajišťování obrany ČR. Zpráva je předkládána k projednání vládě ČR. Za rok 2018 nezahrnuje žádnou informaci o identifikovaných rizicích, jejich hodnocení a souvisejících realizovaných opatřeních v kontextu nastaveného systému řízení rizik.

11 *Zákon č. 320/2001 Sb.: Zákon o finanční kontrole ve veřejné správě*. § 4.

12 *Rozkaz ministra obrany č. 20: Řízení rizik v ReMO*, čl. 3.

13 *ČSN ISO 31000 Management rizik – Principy a směrnice; ČSN ISO 31000. Management rizik - Směrnice*.

14 *Metodické pokyny k řízení rizik v ReMO a použití Modulu řízení rizik*.

15 *Rozkaz ministra obrany č. 66: Plánování činnosti a rozvoje v ReMO*, čl. 16.

16 *Metodické pokyny pro pololetní a roční hodnocení cílů ReMO*, Příloha 6.

3.2 Posouzení softwarové podpory

Pro podporu řízení rizik je v ReMO využíván softwarový nástroj, který je integrální součástí systému řízení rizik.[17] Modul rizik pokrývá funkční oblastí dle DOTMLPFI a celé spektrum hrozeb – přírodního původu, fyzikálního a technického původu, lidský faktor, organizační faktor, společensko-ekonomický faktor. Výpočet míry kritičnosti rizika je realizován automaticky na základě vyplnění požadovaných parametrů. Míra kritičnosti rizika (kritická, vysoká, střední, nízká) je stanovena jako součin hodnoty míry kritičnosti aktiva (kombinace opravitelnosti, resp. nahraditelnosti a citlivosti, resp. dostupnosti) a hodnoty míry kritičnosti hrozby (kritická nebo nekritická). Za neakceptovatelná rizika, ke kterým je nezbytné přijímat rozhodnutí o způsobu zvládání jsou považována rizika s mírou kritičnosti stanovenou jako „vysoká“ a „kritická“. Nástroj umožňuje zpracovávat mapy rizik a katalog rizik. Neobsahuje však vhodné výstupy podporující řízení rizik v procesu plánování rozvoje zohledňující plánovací cykly, hodnocení trendů vývoje rizik, prioritizaci a balancování požadavků. Modul je propojen pouze s nástrojem pro roční plánování implementovaným v rámci stejného informačního systému. Vazba na nástroj pro podporu střednědobého plánování, nástroj pro věcné plánování obsahující dokumentaci cílů nebo nástroj pro zpracování rozpočtového výhledu a rozpočtování není realizována zejména z důvodu jejich umístění v rámci jiných informačních systémů.

3.3 Analýza připravenosti uživatelů a míry akceptace systému řízení rizik

Ke zjištění připravenosti uživatelů pro práci se systémem řízení rizik a míry akceptace systému řízení rizik bylo realizováno dotazníkové šetření mezi správci rizik a provedeny polostrukturované rozhovory se zástupci manažerů cílů 3. úrovně.

Z analýzy odpovědí obdržených od správců rizik vyplynuly následující závěry:

- Pouze 55 % respondentů je přesvědčeno, že pochopili problematiku.
- Žádný z respondentů nestráví se systémem řízení rizik více, než 2 hodiny týdně.
- 67 % respondentů konstatovalo, že se systému řízení rizik kromě nich věnuje maximálně jedna další osoba.
- 77 % respondentů nemá řízení rizik v náplni práce.
- 33 % respondentů vnímá práci se systémem řízení rizik jako součást pracovní náplně související se zpracováním nebo aktualizací ročního plánu.
- 77 % respondentů vnímá systém řízení rizik pouze jako administrativní nástroj.
- Podle 88 % respondentů nejsou výstupy ze systému řízení rizik využívány pro podporu plánování.
- 50 % respondentů považuje za problematickou využitelnost výstupů nebo nedostatečnou vazbu na plánovací nástroje.

17 *Metodické pokyny k řízení rizik v ReMO a použití Modulu řízení rizik.*

- 43 % respondentů považuje za důležité lepší provázání s plánovacími procesy.

Z polostrukturovaných rozhovorů byly sestaveny následující závěry:

- Systém řízení rizik by mohl být pro výkon manažerské praxe velmi přínosný, nicméně doposud nebyl dostatečně vysvětlen a prosazen do praxe.
- Není jasné, jak se systémem pracovat na všech úrovních. Lidé myšlence řízení rizik nerozumějí, neumějí se systémem pracovat. Nejsou k dispozici snadno pochopitelné ukázkové příklady.
- Řízení rizik není pozitivně vnímáno. Představuje administrativní zátěž. Ve stávající podobě nepomáhá při manažerské praxi.
- Systém řízení rizik neposkytuje přidanou hodnotu pro prioritizaci. Chybí užší provázanost s projekty.
- Správci rizik často řeší a posouvají rizika bez vědomí ředitele/velitele.
- Systém řízení rizik nepodporuje práci s utajovanými informacemi.

Z dotazníkových šetření a provedených polostrukturovaných rozhovorů je zřejmé, že účinnějšímu využití řízení rizik v procesu plánování rozvoje a jeho povýšení z administrativního nástroje na nástroj manažerský brání v podmínkách ReMO stále ještě určitá setrvačnost, nedůvěra v přínos systému řízení rizik v kombinaci se složitostí systémového nastavení a omezenými podmínkami (zejména v personální oblasti) pro odpovídající podporu řízení rizik.

3.4 Shrnutí hodnocení současného stavu

V rámci hodnocení současného stavu řízení rizik ReMO byla posouzena vhodnost systémového nastavení (především regulátorů řízení a SW nástroje) pro potřeby plánování rozvoje AČR.

Výsledky provedených analýz jsou uvedeny v matici SWOT v tabulce č. 1. Hodnocení jsou seřazeny podle jejich významu:[18]

Tabulka č. 1: SWOT matice

Silné stránky (DOTMLPFI)	**Hrozby** (PESTLEM)
D: Systém řízení rizik navržený v souladu s přístupy nejlepší praxe O: Relativně malá administrativní náročnost systému řízení rizik L: Jednoznačně stanovená gesce za systém řízení rizik i koordinaci v podřízenosti NGŠ AČR M: Funkční SW pro administraci rizik	L: Porušení platné legislativy při nesprávně identifikovaných nebo neřešených rizicích E: Snížení rozpočtu MO při neadekvátním zdůvodnění zdrojových potřeb M: Nedostatečné zajištění obranyschopnosti státu při nesprávně identifikovaných nebo neřešených rizicích.

18 K určení pořadí využita metodika uvedená v: GRASSEOVÁ, Monika, DUBEC Radek, ŘEHÁK David. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení.*

Slabé stránky (DOTMLPFI)	**Příležitosti** (PESTLEM[19])
I: Nedostatečná, resp. nejasná vazba systému řízení rizik na plánovací procesy, nezohlednění cykličnosti plánování P: Nedostatečný počet hodnotitelů L: Nízká akceptace systému řízení rizik ze strany managementu, vnímání jako administrativní nástroj T: Nedostatečná proškolenost personálu, nezohlednění odlišných potřeb jednotlivých skupin uživatelů M: SW pro řízení rizik je omezen implementací do neutajovaného systému P: Nezohlednění výkonu role v rámci systému řízení rizik ve funkční náplni zaměstnance	P: Zadání pro rozvoj AČR potvrzené na politické úrovni L: Stabilní struktura plánovacích dokumentů a standardně fungující plánovací prostředí připravené na využití výstupů ze systému řízení rizik M: Jasně definovaný systém nadřízenosti a podřízenosti E: Identifikované přístupy nejlepší praxe využívané v rámci ReMO i v zahraničí

Z hodnocení současného stavu řízení rizik je zřejmá nedostatečná vazba systému řízení rizik na plánovací procesy a nezohlednění specifických potřeb podpory plánování. Nízká je úroveň akceptace řízení rizik pro potřeby řízení ze strany vedoucích zaměstnanců, kteří jej vnímají jako administrativní proces bez přidané hodnoty pro manažerskou praxi.

V podmínkách ReMO jsou sice nastaveny nezbytné regulátory řízení a rámcový systém pro řízení rizik podpořený SW nástrojem, nicméně reálná využitelnost systému řízení rizik především v procesu střednědobého a dlouhodobého plánování rozvoje AČR stále neodpovídá potřebám řídící praxe.

4 NÁVRH ŘEŠENÍ

4.1 Požadavky na řízení rizik

Hodnocení současného stavu a poznatky získané z odborné literatury umožnily definovat základní požadavky na další rozvoj systému řízení rizik ReMO. Návrh na úpravu současného systémového nastavení řízení rizik by měl být především jednoduše realizovatelný, srozumitelný a akceptovatelný všemi zainteresovanými stranami. Návrh by měl být adresný a umožňovat hierarchický přístup. Měl by být provázán s plánovacími cykly a především umožnit provázání rizik s prioritami a se zdroji. Návrh by měl umožnit sledování trendů vývoje rizik v čase. Podstatné je, aby návrh umožnil pružně reagovat na potřeby manažerů cílů při balancování jejich záměrů s dostupnými zdroji.

K hledání návrhu řešení bylo preferováno využití přístupů nejlepší praxe přizpůsobených podmínkám ReMO. Návrh řešení je zaměřen primárně na využitelnost v podřízenosti NGŠ AČR. Ten může v souladu s platnými normativy v případě potřeby změny

19 PESTLEM – Political, E – Economical, S – Social, T – Technological, L – Legal, E – Ecological, M - Military

v nastavení systému řízení rizik a zapracování problematiky do vnitřních předpisů mimo jeho působnost[20] navrhnout gestorovi systému řízení rizik.

Návrh musí provázat plánování rozvoje a řízení rizik. Užší provázání systému řízení rizik s řízením a plánováním by mělo být provedeno v rovině horizontální a vertikální. **Horizontální rovina zahrnuje** sladění řízení rizik s cykly plánování a vyhodnocení. V podmínkách rezortu MO určovanými zejména RMO 66. **Vertikální rovina umožňuje** sladění řízení rizik s hierarchickým přístupem k rozpracování a vyhodnocení plánů. V podmínkách rezortu MO zejména soustavou cílů rezortu, se kterou je systém plánování podle RMO 66 úzce provázán.

Na horizontální úrovni by měl být systém řízení rizik co nejtěsněji provázán s plánovacími procesy, avšak umožnit samostatnou aktualizaci a vyhodnocení rizik. Tento přístup je využíván v rámci projektového řízení,[21] kdy pro potřeby řízení rizik projektu je výhodné zpracovat plán řízení rizik projektu. S využitím analogie lze k cyklu tvorby, aktualizaci a vyhodnocení plánu přistupovat projektově[22]. Tento přístup umožňuje zjednodušení rozhodovacího problému souvisejícího s implementací systému řízení rizik do podmínek plánování.

Při rozdělení zpracování plánů podle RMO 66 na izolované projekty, jejichž vstupem jsou informace obsažené v interních regulátorech, nadřazených dokumentech a informace z předchozích plánovacích cyklů, je vhodné integrovat činnosti související s řízením rizik těchto jednotlivých izolovaných projektů do jednoho procesu.

K vytvoření strukturované vazby v procesu plánování na systém řízení rizik je tak vhodné vypracovat **Plán řízení rizik** (dále jen PŘR), který je modifikován pro potřeby řízení rizik jednotlivých plánů činnosti a rozvoje.

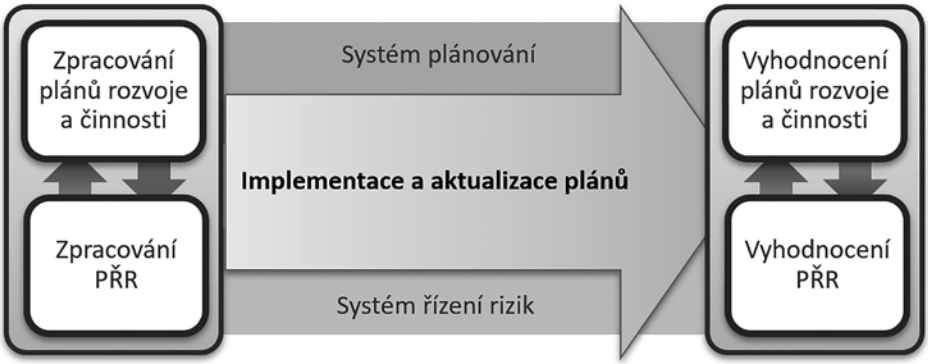
Využití PŘR zmiňuje i Metodická pomůcka pro tvorbu koncepčních dokumentů rezortu MO (MPKD), která však neřeší formu, obsahovou strukturu PŘR ani konkrétní provázanost se systémem řízení rizik nebo systémem plánování.

Návrh možné výchozí vazby mezi systémem plánování a systémem řízení rizik s využitím PŘR a jejich vyhodnocení je patrný z obrázku č. 3.

20 *Rozkaz ministra obrany č. 20: Řízení rizik v rezortu Ministerstva obrany*, čl. 4, odst. 3.

21 SVOZILOVÁ, Alena. *Projektový management: Systémový přístup k řízení projektů*. 3. aktualizované a rozšířené vydání. Praha: Grada Publishing, 2016. ISBN ISBN 978-80-271-9472-8 (pdf).

22 Např. *NATO ARAMP-1*, Příloha C, str. c-4.



Obrázek č. 3: Provázání rozvojových plánů a Plánů řízení rizik

PŘR s vazbou na systém řízení rizik umožní zohlednit při přípravě plánů činnosti a rozvoje identifikovaná rizika. PŘR poskytne přehled o „transferu“ opatření souvisejících se zvládáním rizik v horizontálním i vertikálním směru (např. z krátkodobého časového horizontu do střednědobého časového horizontu, z nižší úrovně velení na vyšší úroveň velení nebo obráceně apod.).

V rámci vertikálního směru při rozpracování PŘR je reflektován přístup shora dolů (TOP-DOWN), kdy nadřazená úroveň řízení je jedním ze vstupů a tvoří zadání pro nižší úroveň. Při vyhodnocení plánů je však aplikován přístup zdola nahoru (BOTTOM-UP), kdy manažerské vyhodnocení rizik na nižší úrovni řízení je jedním ze vstupů pro vyhodnocení rizik na vyšší úrovni.

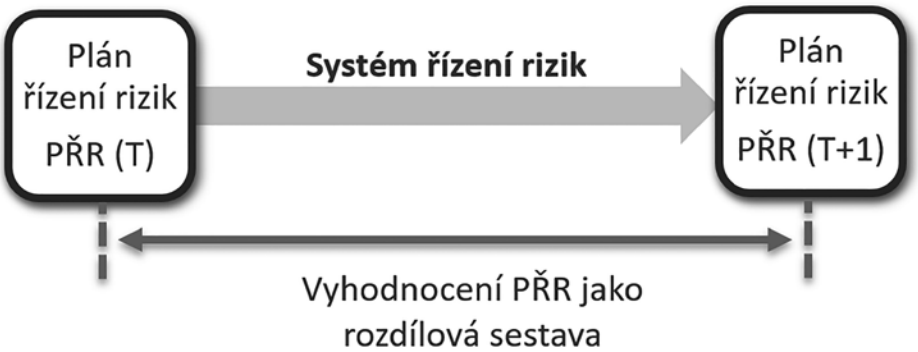
Sestavení a vyhodnocení PŘR by mělo probíhat v intervalech sladěných s intervaly sestavení a vyhodnocení plánů rozvoje a činnosti nastavených v rámci RMO 66. To umožní kontrolu provázanosti s plány rozvoje, posílí důraz na vydávání informovaných rozhodnutí ze strany manažerů a vedoucích pracovníků souvisejících s realizací plánů rozvoje a činnosti.

4.2 Základní struktura a pozice Plánů řízení rizik

Pozice Plánu řízení rizik ve vztahu k systému řízení rizik je naznačena na obrázku č. 4.

Obrázek č. 4: Vztah PŘR a systému řízení rizik
Zdroj: NASA GOES[23]

PŘR vytvoří obraz identifikovaných rizik vázaných ke konkrétnímu časovému okamžiku. Tím se stane výchozím bodem pro porovnání změn, které nastaly v průběhu plánovacího období – např. čtvrtletí, poletí, rok. Porovnání změn mezi obdobími lze následně využít k vytvoření rozdílové sestavy jako základu pro další vyhodnocení, jak naznačuje obrázek č. 5. Je tak možné sledovat trendy hodnocených rizik.



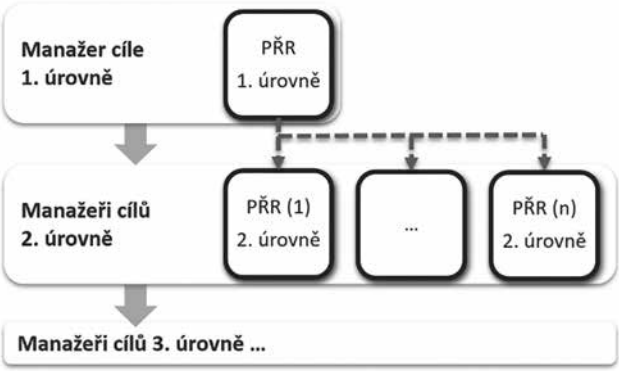
Obrázek č. 5: Využití změn mezi PŘR pro vyhodnocení vývoje rizik

V průběhu plánovacího období je aplikován systém řízení rizik, který zajistí aktualizaci rizik. Po uplynutí plánovacího období je sestaven aktualizovaný PŘR (T+1). Rozdíl mezi PŘR (T+1) a PŘR (T) umožní identifikovat trendy ve vývoji rizik (zánik nebo snížení rizika, nárůst rizika, nově vzniklé riziko). Vytvořen je tak úplný obraz o identifikovaných rizicích

[23] *Geostationary Operational Environmental Satellite (GOES): GOES-R Series Risk Management Plan*. s.16.

a jejich vývoji v čase jako základ pro aplikaci informovaných manažerských rozhodnutí ve vztahu k požadovaným změnám plánů činnosti a rozvoje.

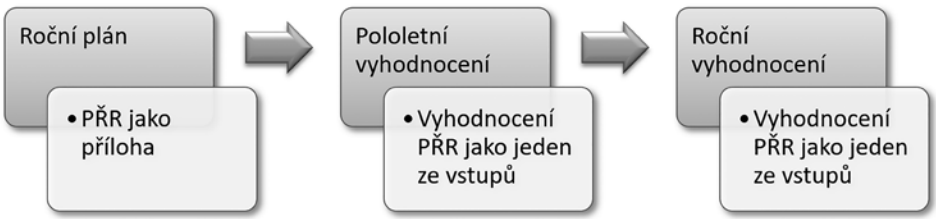
Při využití PŘR lze zjednodušeně za projekt považovat rozvoj AČR se stanovenými milníky rozvoje. Z hlediska sladění se stávajícím systémem plánování a systémem řízení rizik je PŘR sestavován postupně na úrovni manažerů cílů 1. až 3. úrovně s respektováním přístupu „shora-dolů“, jak ukazuje obrázek č. 6.



Obrázek č. 6: Kaskádové rozpracování PŘR

Obsah PŘR je přizpůsobován potřebám řízení, pro které jsou sestavovány, při zachování jejich vzájemné provázanosti prostřednictvím soustavy cílů rezortu. Tím je zajištěno transparentní sledování rizik na dané úrovni řízení. Případné změny jsou zaznamenány a komentovány ve vyhodnocení plánů řízení rizik na horizontální úrovni. Umožněna je i realizace vertikální vazby, kdy PŘR na vyšší může být jedním ze vstupů pro sestavení PŘR na nižší úrovni, a zároveň při vyhodnocení PŘR je možné agregovat z nižších úrovní směrem k úrovním vyšším.

Mezi nástroje pro řešení identifikovaných rizik pak lze zařadit např. střednědobý plán, roční plán rezortu a roční plány organizačních útvarů. Z důvodu sladění se systémem plánování a vyhodnocení podle RMO 66 je tvorba a vyhodnocení PŘR harmonizována s cyklem zpracování ročních plánů a pololetním, resp. ročním vyhodnocením. Základní myšlenka je naznačena na obrázku č. 7.



Obrázek č. 7: Vazba zpracování a vyhodnocení PŘR na roční plánovací cyklus

PŘR může být zpracován jako samostatný dokument nebo jako jedna z příloh plánů[24]. Výhodnou se jeví varianta zpracování jako příloha ročních plánů, neboť upřesňující pokyny ke zpracování PŘR mohou být součástí každoročně aktualizovaných metodických pokynů ke zpracování ročních plánů rezortu[25] vydávaných v gesci NGŠ AČR. Zároveň tak bude zajištěna provázanost se Směrnicí[26] zahrnující politicko-vojenského zadání včetně plánovacích předpokladů, priority ministra obrany, strategické a zvlášť významné projekty, resp. omezení pro plánování[27], a dále bude možné sladit termín vyhodnocení PŘR s termíny vyhodnocení uvedenými v RMO 66 bez zbytečných zásahů do řídících dokumentů.

4.3 Obsahová náplň Plánu řízení rizik

Pro potřeby plánování a řízení v rámci podřízenosti NGŠ AČR jako manažera cíle 1. úrovně je PŘR jednoduše sestavitelný s využitím informací již obsažených v softwarovém nástroji „Modul rizik“, maximálně srozumitelný a při odpovídajícím sestavení použitelný i jako základní nástroj pro podporu reportingu. Zároveň umožňuje snadnou aktualizaci a podporuje transparentní vyhodnocení mezi obdobími. Takový přístup podpoří snadnou pochopitelnost a akceptovatelnost ze strany plánovacích orgánů, správců rizik i manažerů cílů.

Obecně může PŘR na úrovni manažerů cílů obsahovat:

- Rizika identifikovaná na nadřazené úrovni, resp. v rámci strategických a koncepčních dokumentů
- Rizika řešená na úrovni konkrétního manažera cíle 1. až 3. úrovně
- Přehled významných rizik řešených v rámci podřízenosti manažera cíle
- Upřesňující pokyny pro řízení rizik v rámci nadcházejícího období v podřízenosti manažera cíle

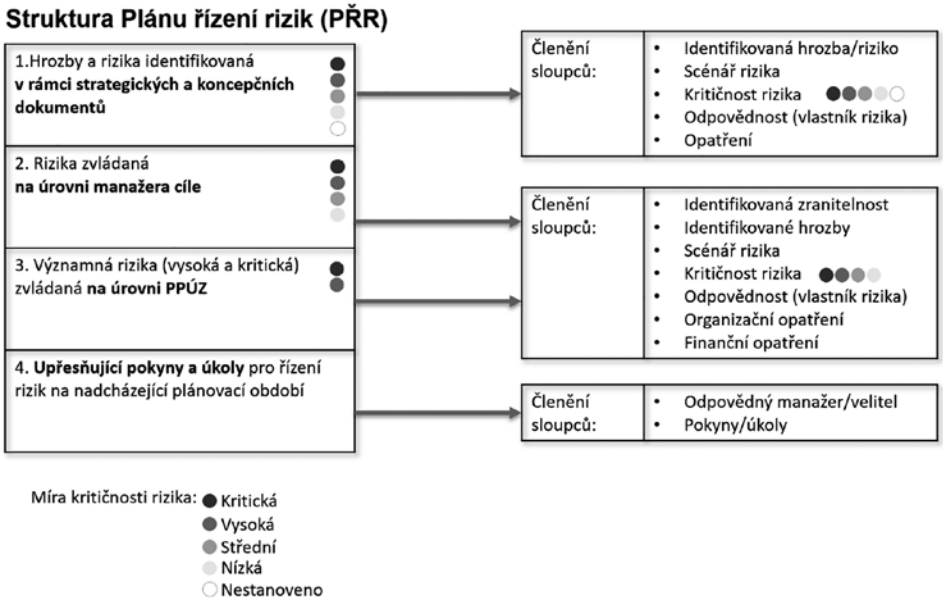
Pro snadnou vizuální identifikaci míry kritičnosti rizik je vhodné využít vizualizaci dat např. s využitím tzv. „semaforu“. Rámcový obsah PŘR je naznačen na obrázku č. 8.

24 *Metodika přípravy veřejných strategií – šablona Plánu řízení rizik tvorby strategie*, str. 1.

25 *Metodické pokyny ke zpracování plánu činnosti rezortu na rok 2020*.

26 *Směrnice ministra obrany pro plánování činnosti a rozvoje rezortu MO na roky 2020 - 2027 s výhledem do roku 2035*.

27 *Rozkaz ministra obrany č. 66: Plánování činnosti a rozvoje v rezortu Ministerstva obrany*, čl. 11.



Obrázek č. 8: Rámcový obsah PŘR

Takto sestavený PŘR umožní manažerovi cíle udělat si rychlý obraz o rizicích řešených na jeho úrovni a zároveň významných (vysokých a kritických) rizicích identifikovaných v rámci jeho podřízenosti. V případě potřeby mu umožní vydat upřesňující pokyny pro řešení oblasti rizik na nadcházející plánovací období (v případě zpracování PŘR jako přílohy ročního plánu je plánovacím obdobím jeden rok).

První část PŘR zaměřená na řešení rizik identifikovaných v rámci strategických a koncepčních dokumentů není v současné době v rezortu MO podrobněji rozpracována. Konkrétní způsob rozpracovávání rizik na strategické úrovni bude nezbytné řešit ve spolupráci se SOPS MO, nicméně pro návrh obecné struktury PŘR není kritickou součástí a lze využít generický přístup stávajícího systému řízení rizik. Pouze je nezbytné zohlednit fakt, že v rámci koncepčních a strategických dokumentů zaměřených na delší časový horizont nemusí být vždy jasná míra kritičnosti rizika v okamžiku zpracování PŘR, proto jsou položky v 1. části doplněny o ukazatel „NESTANOVENO“.

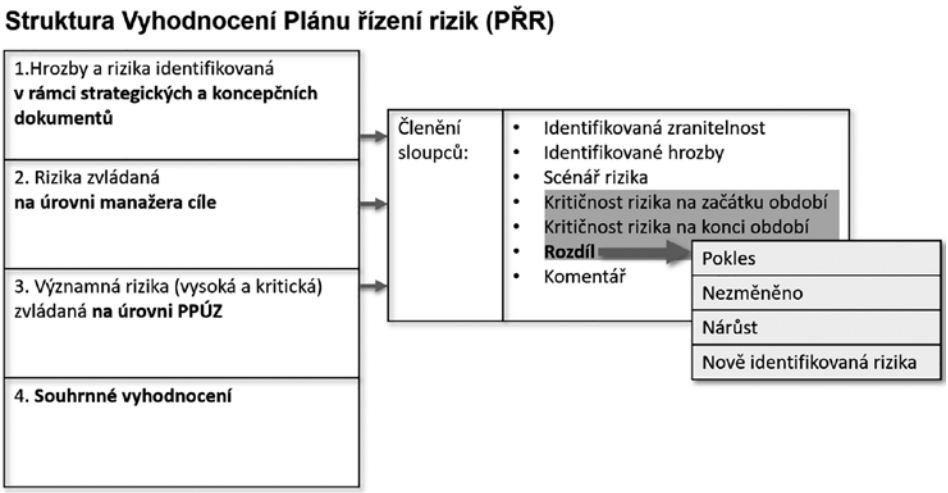
Druhá a třetí část tvoří těžiště PŘR, neboť má přímý dopad na alokaci zdrojů v krátkodobém a střednědobém plánovacím horizontu. Obsah maximálně využívá existující databázi v „Modulu rizik“ tak, aby mohl být PŘR jednoduše generován. Zároveň umožňuje rozlišit opatření organizačního charakteru od opatření vyžadujících alokaci finančních zdrojů v rámci střednědobého plánu, resp. střednědobého rozpočtového výhledu.

Čtvrtá část PŘR obsahuje upřesňující pokyny a úkoly související s oblastí řízení rizik. Jednoznačně identifikuje manažera nebo vedoucího pracovníka odpovědného za jejich plnění.

4.4 Vyhodnocení Plánu řízení rizik

Vyhodnocení PŘR je sladěno s pololetními, resp. ročními intervaly hodnocení podle RMO 66. Tím je zajištěna konzistentnost, synchronizace a integrace procesů plánování, naplňování cílů procesů plánování a identifikovaných rizik[28].

Vyhodnocení PŘR je zpracováno jako **rozdílová sestava** obsahující přehled rizik na začátku plánovacího cyklu a po skončení plánovacího cyklu, doplněná o stručné manažerské shrnutí komentující hlavní změny. Rámcový obsah vyhodnocení je sladěn s PŘR s výjimkou 4. části, která obsahuje stručné manažerské shrnutí. Obsah vyhodnocení je naznačen na obrázku č. 9.



Obrázek č. 9: Rámcový obsah vyhodnocení PŘR

V rámci 1., 2. a 3. části je možné rozdílovou sestavu jednoduchým způsobem generovat porovnáním kritičnosti rizik na začátku a na konci plánovacího období s případným doplněním komentářů.

Vzhledem k tomu, že v průběhu sledovaného období se mohou vyskytnout nově identifikovaná rizika, je nezbytné tuto skutečnost zohlednit ve sloupci „Rozdíl“.

28 *Rozkaz ministra obrany č. 66: Plánování činnosti a rozvoje v rezortu Ministerstva obrany*, čl. 3.

Zpracované vyhodnocení PŘR tvoří podklad pro hodnocení zpracovávané v souladu s RMO 66. Zároveň je jedním ze vstupů pro zpracování aktualizovaného PŘR na další období.

5 OPATŘENÍ K REALIZACI NÁVRHU ŘEŠENÍ

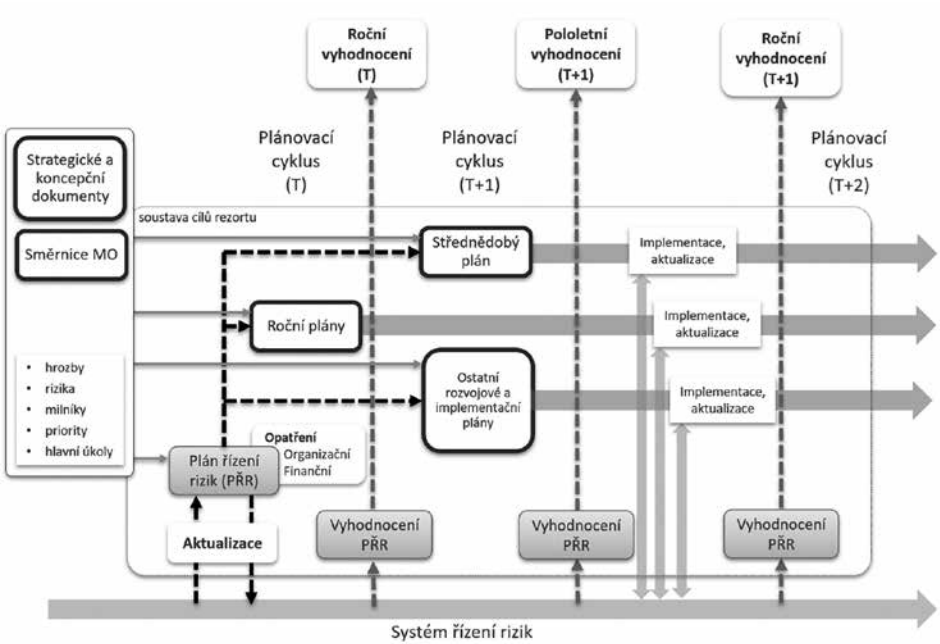
K realizaci implementace PŘR a vyhodnocení PŘR byl navržen rámcový implementační plán shrnutý do tabulky č. 2:

Tabulka č. 2: Doporučení k implementaci Plánu řízení rizik

Fáze	Úkoly k realizaci	Odpovědnost/gesce
Ověření návrhu řešení	• Ověření návrhu, zpracování vzorových sestav PŘR a vyhodnocení PŘR pro vybrané organizační prvky s využitím obsahu Modulu rizik • Upřesnění obsahu PŘR a vyhodnocení PŘR v součinnosti gestorem řízení rizik • Zpracování vzorových PŘR za úroveň manažera cíle 1., 2., 3. úrovně • Přednesení návrhu Velení AČR	SPS MO *Součinnost gestor řízení rizik*
Přípravná fáze	• Zpracování specifikací k implementaci potřebných změn do Modulu rizik: • Uživatelské rozhraní • Úprava databázových položek • Tiskové sestavy	SPS MO *Součinnost gestor řízení rizik*
Implementační fáze	• Implementace požadovaných změn do Modulu rizik	Dodavatel Modulu rizik
	• Ověření technické implementace PŘR a vyhodnocení PŘR • Dopracování metodické pomůcky ke zpracování a vyhodnocení PŘR včetně aktualizovaných vzorů.	SPS MO *Součinnost gestor řízení rizik*
	• Aktualizace metodických pokynů ke zpracování Ročního plánu – doplnění úkolu zpracovat PŘR jako přílohy • Aktualizace metodických pokynů ke zpracování pololetního a ročního vyhodnocení • Informování Velení AČR	SPS MO *SOPS MO*

Fáze	Úkoly k realizaci	Odpovědnost/gesce
Realizační fáze a zahájení rutinního provozu	• Realizace školení: • Správců rizik • Hodnotitelů rizik • Plánovacích orgánů • Seznámení manažerů cílů	SPS MO SOPS MO *Součinnost gestor systému řízení rizik*
	• První zpracování PŘR jako přílohy ročních plánů	MC 1.,2.,3. úrovně
	• První vyhodnocení PŘR	MC 1.,2.,3. úrovně

Implementací PŘR bude posílena vazba mezi systémem řízení rizik podle RMO 20 a systémem plánování podle RMO 66. PŘR poskytne manažerovi i uživatelům jasnou představu o aktuálním stavu řešených rizik ve vazbě na hrozby, rizika, milníky, priority a hlavní úkoly identifikované v rámci strategických dokumentů, Směrnice MO, případně hlavní úkoly stanovené NGŠ AČR v rámci daného plánovacího období. Vazba mezi systémem řízení rizik a systémem plánování s využitím PŘR je naznačena na obrázku č. 10.



Obrázek č. 10: Vazba PŘR na systém řízení rizik, tvorbu a vyhodnocení plánů

Před zahájením zpracování ročních plánů organizačních prvků na další plánovací cyklus (T+1) je PŘR vygenerován z aktuálních podkladů dostupných v rámci Modulu rizik.

V něm obsažená opatření a pokyny/úkoly jsou upraveny a doplněny podle potřeby, přičemž jedním ze vstupů je poslední vyhodnocení PŘR, Směrnice MO na další plánovací období, případně další aktualizované strategické a koncepční dokumenty. Díky softwarovému provázání se systémem řízení rizik je výsledek ihned promítán do karet rizik a aktualizovaná opatření/úkoly se stávají součástí postupů zvládání rizik.

Aktualizovaný PŘR tvoří přílohu ročního plánu organizačního prvku, přičemž navržená opatření jsou jedním ze vstupů k rozpracování v rámci ročního plánu, střednědobého plánu, ale i dalších plánů podle charakteru opatření, včetně aktualizace rozpočtového výhledu.

V průběhu kalendářního roku je roční plán realizován a aktualizován standardním způsobem. Standardním způsobem je rovněž aktualizován střednědobý plán a prováděny všechny fáze systému řízení rizik. Opatření organizačního a finančního charakteru uvedená v PŘR jsou realizována podle potřeby a po vyhodnocení jejich účinnosti dochází ke změně míry kritičnosti souvisejícího rizika. Díky SW provázání jsou informace automaticky součástí PŘR, který je vždy aktuální. V rámci pololetního, resp. ročního vyhodnocení je vygenerována rozdílová sestava k vyhodnocení PŘR, kterou lze jednoduchým způsobem okomentovat. PŘR tak respektuje cyklickou povahu plánů, poskytuje informace pro jejich sestavení, aktualizaci nebo vyhodnocení formou aplikace SW filtru na existující systém řízení rizik bez dalších omezení systému plánování nebo systému řízení rizik.

Klíčovým parametrem implementace navrhovaného řešení je průběžné seznamování Velení AČR s návrhy a stavem řešení tak, aby bylo zajištěno akceptování návrhu ze strany TOP managementu a včasné zapracování připomínek. Tento parametr je zohledněn v rámci návrhu implementačního plánu.

Předpokladem pro úspěšnou implementaci PŘR je realizace některých dalších dílčích opatření k odstranění nedostatků identifikovaných v rámci analytické části, zejména rozšíření počtu hodnotitelů a přizpůsobení školení potřebám různých skupin uživatelů. Identifikované nedostatky a navrhovaná doporučení jsou uvedeny v tabulce č. 3 a v případě potřeby je lze realizovat jak v rámci podřízenosti NGŠ AČR, tak v rámci celého rezortu MO.

Tabulka č. 3: Matice nedostatků a doporučení

Identifikovaný nedostatek	Doporučení a zdůvodnění
Nedostatečný počet hodnotitelů	**Doporučení:** Rozšíření počtu hodnotitelů v rámci systému řízení rizik o vedoucí pracovníky a specialisty v rámci organizačních prvků. **Zdůvodnění:** Systém řízení rizik je mj. založen na principu včasného varování, pro jehož správnou funkčnost je nezbytný co nejširší přehled o možných rizicích. Od správce rizik nelze realisticky očekávat, že bude schopen odborně pokrýt celou oblast působnosti organizačního prvku. Informaci o specifické hrozbě, zranitelnosti a souvisejícím riziku zná specialista, neboť je součástí jeho pracovní náplně. Není proto důvod, aby byli z procesu identifikace rizik v rámci systému řízení rizik specialisté a jejich nadřízení pracovníci vyloučeni.

Identifikovaný nedostatek	Doporučení a zdůvodnění
Neoficiální výkon rolí v rámci systému řízení rizik.	**Doporučení:** Posílení adresného přístupu. Výkon rolí v rámci systému řízení rizik v ideálním případě zapracovat do popisu funkční náplně, v minimalistické variantě do organizačního rozkazu vydávaného na začátku kalendářního roku. V rámci SPS MO postupně rozvíjet koordinační roli Odboru věcného a zdrojového plánování/ Analytického oddělení vyplývající z organizačního řádu. Problematiku postupně rozvíjet v úzké součinnosti s gestorem řízení rizik. **Zdůvodnění:** Součástí akceptace systému řízení rizik je jeho zviditelnění a „čitelnost“ napříč působnostmi a pracovními povinnostmi. Doporučení je v souladu s požadavkem uvedeným v RMO 20.
Nezohledňování potřeb jednotlivých skupin uživatelů – manažerů cílů, správců rizik, hodnotitelů	**Doporučení:** Všechna školení by měla klást důraz na seznámení s problematikou řízení rizik formou jednoduchých praktických příkladů. Jakékoliv použité obrázky by měly být jednoduché a snadno srozumitelné. Školení samotné je nezbytné přizpůsobit potřebám jednotlivých subjektů v rámci systému řízení rizik: • Hodnotitelé – důraz na schopnost identifikace a vyhodnocení rizik • Správci rizik – důraz na schopnost identifikace rizik a správné zapracování do systému • Manažeři cílů – důraz na vysvětlení přínosu systému, vysvětlení principu včasného varování a vazby na systém řízení a plánování Rozsah školení u správců a hodnotitelů rizik lze realisticky odhadnout cca na 4 hodiny (2 hodiny teorie, 2 hodiny praktická část). U manažerů cílů by školení nemělo přesáhnout půl hodiny. Dále je doporučeno zavedení pravidelných metodických dnů zaměřených zejména na vzdělávání správců rizik s důrazem na sjednocení přístupu k problematice a předávání zkušeností, případně využití odborných zaměstnání na úrovni organizačního prvku následně zaměřených na sdílení zkušeností a identifikaci rizik. To přispěje k posílení okruhu uživatelů, kteří budou schopni identifikovat možná rizika. **Zdůvodnění:** Využitá analogie: přístupy ke školení plánovacích orgánů a vedoucích pracovníků v rámci ročního plánování, resp. pravidelná zaměstnání zaměřená např. na prevenci patologických jevů.
Omezení implementace systému řízení rizik na neutajovaný systém	**Doporučení:** Postupná migrace Modulu rizik do systému umožňujícího pracovat s klasifikovanými informacemi. **Zdůvodnění:** Přehled identifikovaných rizik poskytuje neustále zpřesňovaný přehled o slabinách systému. Již dnes některé informace nelze v SW nástroji pro řízení rizik zpracovávat. Postupné rozšiřování databáze způsobí, že v určitém okamžiku nebude možné systém provozovat bez porušení související legislativy.

Práce na odstranění dílčích nedostatků je možné zahájit okamžitě. V souladu s působností by implementace v podřízenosti NGŠ AČR měla být koordinována z úrovně SPS MO, ideálně v součinnosti s gestorem systému řízení rizik.

ZÁVĚR

Příspěvek předkládá závěry z výzkumu zaměřeného na řízení rizik v podmínkách ReMO. Návrh řešení má potenciál posílit účinnost řízení rizik v procesu plánování rozvoje AČR. Navrhovaná opatření směřují k posílení funkčnosti systému řízení rizik a zlepšení provázanosti se systémem plánování. Návrh spočívá ve zpracování Plánu řízení rizik. Proces jeho tvorby je přizpůsoben specifickým podmínkám řízení AČR a respektuje platné regulátory řízení ReMO – zejména RMO 66 pro oblast plánování a RMO 20 pro oblast řízení rizik.

Řešení klade důraz na evoluční přístup bez požadavků na zásadní přepracování stávajícího systému plánování nebo řízení rizik. PŘR tak plní mj. úlohu nástroje pro včasné varování umožňující manažerům cílů i plánovacím orgánům získat strukturovaný pohled na rizika související s realizací plánů činnosti i rozvojových plánů v rámci jejich působnosti. Implementace PŘR přispěje k posílení realističnosti zpracovaných plánů.

Důležitým parametrem návrhu je variabilnost, flexibilita a opakovatelnost. Obsahová struktura PŘR není fixní, může reflektovat specifické potřeby konkrétního vedoucího zaměstnance a zaměřit se na rizika související s naplňováním priorit nebo hlavních úkolů konkrétního plánovacího období. Forma PŘR a jeho vyhodnocení umožňuje jednoduchou implementaci do stávajících softwarových nástrojů a následné automatické generování z dostupných datových podkladů. V případě potřeby řešení vybraných rizik v režimu vyžadujícím ochranu utajovaných informací lze pracovat s registrem vybraných rizik, který bude zcela oddělený od hlavní databáze „Modulu rizik“, bez dopadu na využitelnost navržené struktury PŘR pro podporu plánovacích procesů.

Návrh zohledňuje aktuální stav implementace systému řízení rizik a potřebu získání větších praktických zkušeností na úrovni manažerů cílů 1. až 3. úrovně v procesu plánování rozvoje AČR. Navržená opatření lze do praxe zavádět postupně tak, jak se vyvíjí zkušenosti z procesu řízení rizik v ReMO.

Autoři: ***Plk. gšt. Ing. Miroslav CHYLÍK,*** *nar. 1975. Absolvoval Vysokou školu ekonomickou v Praze, obor Podniková ekonomika. Po výkonu základních vojenských funkcí zastával pozice na úrovni Generálního štábu zaměřené zejména na softwarovou podporu, střednědobé a roční plánování. V letech 2014 – 2016 působil na stálé delegaci ČR při NATO se zaměřením na obranné a zdrojové plánování NATO. V roce 2020 absolvoval Kurz Generálního štábu v Brně. V současné době se zaměřuje na oblast krátkodobého a střednědobého plánování.*

Ing. Josef Procházka, Ph.D., narozen 1966. *V roce 1990 absolvoval Vojenskou akademii Antonína Zápotockého v Brně. Zastával základní a štábní vojenské funkce v oblasti logistiky. V letech 1999 a 2004 působil v zahraničních misích SFOR a EUFOR. V letech 2000 – 2007 působil na Ústavu strategických studiích Univerzity obrany v Brně. Po odchodu do zálohy v roce 2007 se*

podílel na formulování obranné politiky a strategie ČR a působil na velitelství NATO v oblasti řízení obranných zdrojů. V současné době je zástupcem ředitele Centra bezpečnostních a vojenskostrategických studií Univerzity obrany v Brně. Přednáší a publikuje v oblasti obranné politiky, řízení obrany a obranného plánování, logistiky a vyzbrojování.

Jak citovat: CHYLÍK, Miroslav and Josef PROCHÁZKA. Řízení rizik v procesu plánování rozvoje Armády České republiky. *Vojenské rozhledy*. 2020, 29 (3), 003-024. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenske-rozhledy.cz

 DOI: 10.3849/2336-2995.29.2020.03.025-040

Peer-reviewed

Situational Awareness and Current Information Environment

Znalost situace a současné informační prostředí

Marek Fiebich

Abstract: The article deals with providing situational awareness in operations at the operational level of command in the context of the information environment, the current nature of which significantly affects the execution of this capability. It examines the influence of three selected aspects – information overload, the expansion of advanced information technology and the growing importance of the cyber domain – on generating, maintaining and sharing situational awareness in planning and conduct of operations. It identifies and characterizes the respective sub-capabilities within the information area, necessary for operational headquarters to effectively provide situational awareness, and outline possible ways to develop these capabilities in terms of internal processes, technical equipment and personnel.

Abstrakt: Článek pojednává o zajišťování znalosti situace v operacích na operační úrovni velení a řízení v kontextu informačního prostředí, jehož současný charakter zásadním způsobem realizaci této schopnosti ovlivňuje. Zkoumá vliv tří vybraných aspektů – informačního zahlcení, rozmachu pokročilých informačních technologií a rostoucího významu kybernetické domény – na utváření, udržování a sdílení znalosti situace při plánování a vedení operací. Identifikuje a charakterizuje odpovídající dílčí schopnosti v rámci informační oblasti, kterými musí operační velitelství disponovat k účinnému zajišťování znalosti situace, a nastínit možný způsob rozvoje těchto schopností z pohledu vnitřních procesů, technického vybavení a personálu.

Key words: Situational Awareness; Operating Environment; Information Environment; Cyberspace.

Klíčová slova: Znalost situace; operační prostředí; informační prostředí; kyberprostor.

INTRODUCTION

The current complex and dynamic nature of the operating environment places high demands on the armed forces and their development within a large spectrum of activities. One of these activities is also generating and maintaining situational awareness in the battlefield, which is essential for successful planning and conduct of operations. Moreover, the importance of this capability will continue to grow in connection with future operations, which will be conducted across operational domains[1], and for the coordination of which a thorough knowledge of the situation will be one of the decisive factors. With regard to the nature of the current operating environment and the aspects of situational awareness, it can be argued that it is the developments within the information environment that influence this capability the most. That is also why a considerable importance is being attached to the information environment in relation to situational awareness in current and future operations:

"*Good situational awareness of all levels of the deployed forces is crucial for [European Union] Member States' militaries to gain and maintain advantages over the adversaries of 2035 and beyond. This will require an acknowledgement of the increasing importance of understanding the information environment…*"[2]

It is practically impossible to provide comprehensive situational awareness in today's operating environment without advanced information technology to process an enormous amount of information, the ability to effectively control this technology or a large information infrastructure enabling prompt and secure sharing with all participants of an operation at all levels of command. Moreover, cyberspace, as a subset of the information environment, has itself become part of the battlefield, and the information acquired from and on it is becoming an integral part of situational awareness, which is thus taking on completely new dimensions. In order for the headquarters to be able to generate and maintain thorough situational awareness in such an environment, appropriate efforts reflecting the latest developments of the information environment and its aspects must be taken to develop existing and build new capacities and functions to support this crucial command and control capability. This applies particularly at the operational level where the execution of this capability seems to be most problematic. Operational headquarters face an enormous amount of information flowing from an increasingly dynamic tactical level, an increasing range of aspects that must be addressed through a joint effort; all while being coordinated by the strategic level within the comprehensive approach.

1 Air, land, maritime, space and cyberspace.

2 KEPE, Marta, James BLACK, Jack MELLING and Jessica PLUMRIDGE. *Exploring Europe's capability requirements for 2035 and beyond: Insights from the 2018 update of the long-term strand of the Capability Development Plan*. Brussels: European Defence Agency, 2018, p. 22.

1 SITUATIONAL AWARENESS

1.1 Definition of situational awareness

Within NATO, situational awareness is defined as "*the knowledge of the elements in the battlespace necessary to make well-informed decisions.*"[3] Although this definition, providing only a general framing of the term, may be adequate with regards to its purpose of Allied standardization, it does not provide the necessary appreciation of the nature and the scope of situational awareness.

To define the term in more detail, it seems appropriate to use the definition of M. R. Endsley, which arose from an American research project within military aviation and became the underlying definition of situational awareness in many disciplines (from civil aviation to engineering to medicine or psychology). Although her concept is also used for defining situational awareness in the NATO Consultation, Command and Control Board taxonomy[4], it has surprisingly not been included in NATO's official definition. Endsley defines situational awareness as "*the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.*"[5] The main benefit of this definition – and a significant difference from NATO's official definition – is that it divides situational awareness into three successive phases (levels) that must be reached to achieve thorough knowledge, thereby covering all important aspects of situational awareness:

1) The perception of elements in the environment in time and space represents the ability to perceive the status, characteristics and dynamics of relevant elements of this environment.
2) The comprehension of the current situation is based on a synthesis of individual elements of the environment. It is not mere awareness of the elements in the environment, but the ability to understand the environment as a whole, with all its (relevant) elements and the significance of these elements.
3) Based on knowledge of the status and dynamics of the elements (Phase 1) and subsequent understanding of the situation (Phase 2), it is possible to achieve the ability to project, that means to some extent the ability to predict, possible activities of elements in the environment in the near future. Only at this stage does

3 *AAP-6, Edition 2019, NATO Glossary of Terms and Definitions (English and French)*. Brussels: NATO Standardization Office, 2019, p. 118.

4 *C3 Taxonomy Perspective, Baseline 2.* 0. 2015. Brussels: NATO Consultation, Command and Control Board.

5 ENDSLEY, Mica R. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society* [online]. 1995, 37(1), 32-64 [cit. 2020-03-12]. ISSN 0018-7208. Available at: http://journals.sagepub.com/doi/10.1518/001872095779049543, p. 36.

situational awareness gain the added value necessary to support the decision--making process.[6]

To demonstrate the process in the deployed headquarters settings, enemy or own units, their location, size, capabilities or activities in the area of operations, as well as civilian gatherings and incidents or events in the area are good examples of the perceived elements in the environment (Phase 1). Understanding the situation (Phase 2) would then mean to realize that the activities of particular enemy units can, in relation to activities of its other forces, or of own forces, indicate the enemy's intentions. Similarly, local gatherings may be a response to an incident that has occurred within (or even outside) the area of operations. Completing these two phases then allows the staff or the task force commander to assume (Phase 3) that and how the enemy plans to attack, as well as to assume that the mood of the crowd and the entire local population may grow into aggression provided that the consequences of the incident are not dealt with.

In the context of conduct of operations, using both of the above-mentioned definitions, and for the purposes of this article, situational awareness can best be defined as *"the knowledge of the elements in the battlefield based on the perception of these elements in time and space, comprehension of their meaning and projection of their status in the near future, and created and maintained to support the well-informed decision--making in operations."*

1.2 Situational awareness in terms of its users

In general, situational awareness is seen as the knowledge of an individual. This individual knowledge, however, can be used to contribute to the knowledge of a group that the individual is a part of, to the benefit of an organization.[7] Thus, although we can, in relation to the conduct of military operations, refer to situational awareness as the knowledge of each staff member or the commander, situational awareness is in this respect most often understood as group knowledge. This group knowledge is provided by the operations centre as a whole (a group) in terms of a product for the benefit of the commander and the entire headquarters (an organization). At the operational level, this group is represented by the Joint Operations Centre (JOC), or the Combined Joint Operations Centre (CJOC), which is responsible for generating and maintaining situational awareness of the Joint Task Force headquarters (JTF HQ).

Situational awareness created within a given headquarters, which is distributed outside this headquarters, is referred to as "shared situational awareness". Its purpose is to ensure that all entities (individual subordinate headquarters, partner units, non-military

6 Ibid, p. 36-37.

7 CANAN, Mustafa and Bulent SOYKAN. Shared Situational Awareness / Understanding: A Key Attribute of Mission Command Concept for NATO. In: *21st ICCRTS: C2 in a Complex Connected Battlespace* [online]. London. [cit. 2020-03-23]. Available at: https://www.researchgate.net/publication/307923119_Shared_Situational_Awareness_Understanding_A_Key_Attribute_of_Mission_Command_Concept_for_NATO.

actors and other elements) participating in the operation in all affected domains have the same up-to-date knowledge in support of well-informed decision-making and effective synchronization of the joint effort. The relationship of these individual "types" of situational awareness generated within the JTF HQ is schematically depicted in Figure 1.

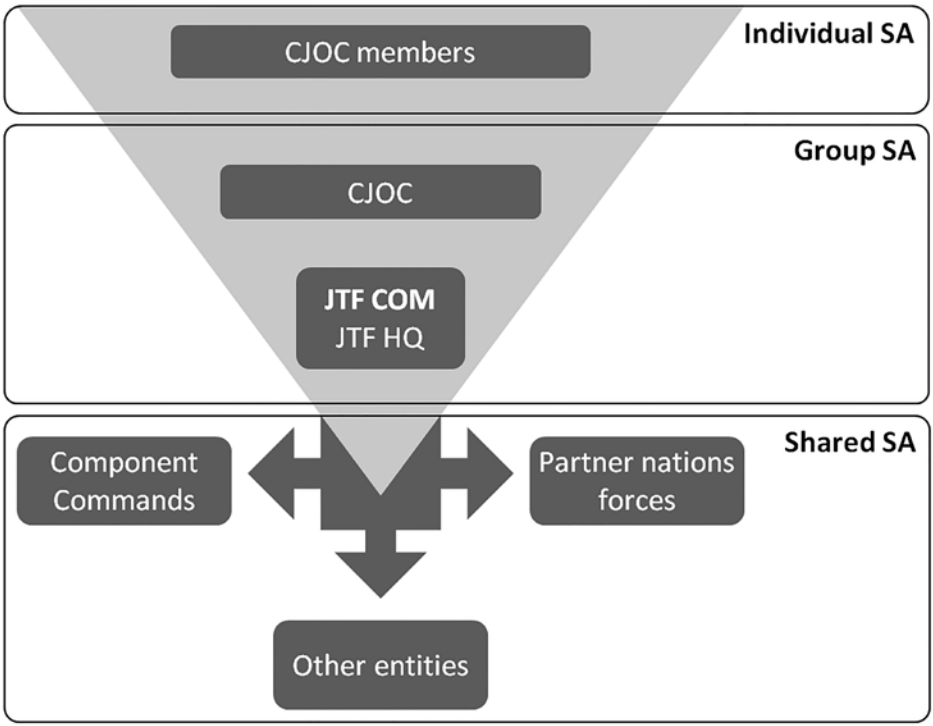


Figure 1: Individual, group and shared situational awareness

2 SELECTED ASPECTS OF THE CURRENT INFORMATION ENVIRONMENT

The expansion of the information environment[8] and particularly the advances of the information technology, which *"have increased the speed and range of information, diffused power over information, and shifted socio-cultural norms,"*[9] fundamentally affect all aspects of operations, including situational awareness. The possibility (and capability), through advanced information technology, to collect a wide range of information from a variety of sources on all aspects of the operating environment, transmit this information promptly to the headquarters often located far away from the battlefield, transform it into concise yet thorough information products, and distribute these promptly within and outside the headquarters, provides an invaluable knowledge support to the decision-making process in planning and conduct of operations within the complex and dynamic operating environment.

2.1 Information overload

However, the immediate access to a large amount of information from the operating environment does not guarantee better situational awareness, nor does it guarantee better decision-making. Often the opposite is true. The extensive amount of easily accessible information represents for the headquarters of the deployed forces, and mainly their operational centres that serve as information gateways to these headquarters, a significant challenge or even an obstacle to successful operations. Thus, while in the past the main problem related to the decision-making process in operations was the lack of information, now the problem lies in the excessive amount of information. The need to process every piece of available information, analyse only the information that is relevant to the operation and distribute it to those (and only those) elements of the headquarters, units and other entities that necessarily need this information for their decision-making, this brings a number of negative consequences.

The main drawback related to the enormous amount of information is information overload associated with the difficulty of "*finding, within the mass of data available,*

8 The NATO Allied Joint Doctrine for the Conduct of Operations defines the information environment as *"a composite of the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs."* (See *Allied Joint Publication-3. Allied Joint Doctrine for the Conduct of Operations.* AJP-3. 2019. Brussels: NATO Standardization Office, LEX-6).

9 *Joint Concept for Operating in the Information Environment (JCOIE)*. 2018. Washington, D.C.: Joint Chiefs of Staff, p. vii.

those precise bits of information that are needed to make an informed, reasoned decision."[10] Although it is the members of the operations centre, which serves as an information hub responsible for the entire "operational" information management, that struggle with this issue the most, information overload does not only concern the initial recipients of the information. In fact, every staff member and also the commander can be overloaded with information, and this often really is the case. As the input grows, so does the amount of information and information products further distributed to the commander, staff and entities outside the headquarters, thus spreading information overload across headquarters and the deployed forces. This very often prevents these subsequent recipients from understanding the complex situation in the battlefield thoroughly and making the necessary well-informed decisions. Additionally, the information systems of the given operations centre or the entire headquarters may also be overwhelmed with the enormous information flow, disabling the systems temporarily or even permanently.

Information overload can thus hamper the provision of situational awareness, the execution of command and control as well as the entire operation. As Cochran and Shaw put it, *"information overload creates analysis paralysis and ultimately impacts efficient tactical, operational and strategic operations."*[11] In order to avoid paralyzing the information analysis, a robust information infrastructure must be established and suitably set up within the headquarters, in addition to proper Information Management (IM) processes, which will enable the staff to handle the enormous amount of information both effectively and efficiently.

2.2 ADVANCED INFORMATION TECHNOLOGY

Given the nature of the current operating environment and the scale of operations to be conducted, generating and maintaining situational awareness would be practically impossible without the use of advanced information technology tools and systems, and these need to be a regular part of every operational headquarters of the deployed forces. Moreover, their role will increase even more in future operations. As Reilly puts

10 STRATER, Laura, FAULKNER, Laurie, HYATT, John, ENDSLEY, Mica. *Supporting Situation Awareness Under Data Overload in Command and Control Visualizations*. 2006. [cit. 2020-03-12]. Available at: https://www.researchgate.net/publication/252218394_Supporting_Situation_Awareness_Under_Data_Overload_in_Command_and_Control_Visualizations, p. 2.

11 COCHRAN, John and Michael SHAW. Mission Command as Applied by US Army - Aviation Perspective. In: *NATO COMMAND & CONTROL CENTRE OF EXCELLENCE SEMINAR: C2 ON THE MOVE.* [online]. 2015, Den Helder, p. 64-69. [cit. 2020-03-17]. Available at: https://c2coe.org/download/c2-on-the-move-seminar/, p. 68.

it, global proliferation of advanced information technology is the principal factor driving the so-called multi-domain operations.[12]

An important role in situational awareness, and the conduct of operations in general, is played by the growing integration of commercial aspects into the military field, such as the Internet of Things or the so-called commercial off-the-shelf products, ranging from social media-based platforms[13] to complex software and hardware solutions to transmit, process and visualize data from the battlefield at all levels of command. Another example of indispensable information technology, usually provided by the commercial sphere, is the software designed to analyse so-called big data[14]. Without big data analytics, providing accurate situational awareness during current and future operations would be practically impossible. The big data analytics allows *"examining massive data sets containing a variety of data types to uncover hidden patterns, correlations and other strategic business and operational information"*[15] related to the situation in the battlefield, and thus *"may help the commander pursue understanding, to overcome the risk of information overload."*[16]

With a further increase of the amount of information and the interrelationship of information with all other elements of the operating environment, the importance of the big data analytics capability will continue to grow accordingly. The British Ministry of Defence anticipates that the operating environment actors, including non-state actors, will make a significant effort in the coming years to build the big data analytics capability to gain information superiority.[17] As a result *"language processing, anomaly detection and visualisation tools will be far more prevalent and will identify activities and trends much earlier than conventional techniques."*[18] The big data analytics, as well as a number of other information technology capabilities, is thus likely to join other areas in which the differences in capabilities between actors with greater combat potential and those with lower combat potential are being diminished, or in which a reverse difference is being created in favour of the otherwise weaker actors. In situations where actors possess the same or similar resources, it is necessary, in order to achieve dominance, to focus on developing those capabilities that will leverage the effects of such resources. In the case of achieving information superiority to support the provision of situational awareness with

12 REILLY, Jeffrey. Multi-Domain Operations. In: *Joint Air & Space Power Conference 2019: Shaping NATO for Multi-Domain Operations of the Future* [online]. 2019, Kalkar: Joint Air Power Competence Centre, p. 15-24. [cit. 2020-04-02]. Available at: https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf.

13 See FORRESTER, Bruce. *Integrating Social Media Tools with Command and Control (C2): What are the Possibilities?* [online]. 2016, Québec. Available at: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc229/p803913_A1b.pdf. Scientific Report. DRDC – Valcartier Research Centre.

14 Velká data (big data) lze chápat jako objem dat, který vzhledem k jeho velikosti není možné přijímat, zpracovávat, ukládat a analyzovat běžnými databázovými nástroji.

15 FABER, Isaac and Ellisa ZADROZNY. OPEN SOURCE BIG DATA. *ARMY AL & T* [online]. 2016, 56(3), 104-109 [cit. 2020-03-12]. Available at: https://asc.army.mil/docs/magazine2/armyalt-jul-sep-2016.pdf, p. 105.

16 *Future Operating Environment 2035*. 2015. London: Ministry of Defence UK, p. 42.

17 *Future Operating Environment 2035*. 2015. 1. London: Ministry of Defence UK.

18 Ibid UK, p. 19.

similarly advanced information technology, increasing the skills of personnel who work with these systems to process the information from the battlefield seems to be the most effective way. The last chapter of this article elaborates on this issue further, offering specific aspect of personnel development to focus on.

2.3 Information security in cyberspace

Another aspect also inherently connected with the dynamic development of the information environment and particularly the information technology is the increased need to protect information within cyberspace. Information, being most vulnerable when being processed and transmitted, needs to be protected from potential cyber threats as well as technical failure.[19] Insufficient protection of information, especially in the context of shared situational awareness, can, in case of damage or theft of this information, deprive the headquarters of the information advantage or provide the enemy with information on current or planned activities of own forces and thus jeopardize the security of this forces or threaten the success of the entire operation.

The need for information and network protection increases with respect to the aforementioned growing share of the Internet of Things and commercial products in the conduct of operations. As Fučík et al. point out, although the complex interconnection of the systems in cyberspace allows, among others, for real-time decision-making (contingent on achieving real-time situational awareness), it also *"deepens the overall dependence on a stable and effective operation of this area,"*[20] which places high demands on ensuring security in cyberspace. Measures to ensure the resilience of networks and information security in generating and sharing situational awareness (especially when distributed outside the information system of the headquarters) must then be one of the main priorities for the operation to be successful. This implies that, for example, a thorough examination of the credibility and reliability needs to be conducted in relation to the integration of commercial deployable information systems to maintain the integrity of the transmitted data.[21]

---

19 LEEVINSON, J., V. VIJAYARAGHAVAN and M. DAMMODARAN. Blockchain Mechanisms as Security-Enabler for Industrial IoT Applications. MAHMOOD, Zaigham, ed. *The Internet of Things in the Industrial Sector: Security and Device Connectivity, Smart Environments, and Industry 4.* 0. Cham: Springer, 2019, s. 145-162. ISBN 978-3-030-24891-8.

20 FUČÍK, Jakub, Fabian BAXA, Libor FRANK and Josef PROCHÁZKA. 2019. *Technological Development: The Implications for the Capabilities of the Armed Forces of the Czech Republic 2018*. 1. Brno: University of Defence in Brno, 24 p., p. 9.

21 WRONA, Konrad. 2015. Securing the Internet of Things a military perspective. In: *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* [online]. Milan, p. 502-507. Available at: https://ieeexplore.ieee.org/document/7389105.

3 INFORMATION ENVIRONEMT AND SHARED SITUATIONAL AWARENESS

To serve its purpose of supporting decision-making, situational awareness generated during the operation has to be shared by all who need to make decisions based on it within that operation. This need increases in complex operations involving a large number of diverse task forces and entities, such as in the multi-domain operations. Within the U.S. Armed Forces "Multi-Domain Operations" concept, shared situational awareness is, together with an adequate effort to exercise these multi-domain activities and the coordination of synchronic operations, considered as one of the critical conditions that the forces of participating states have to meet to successfully conduct these operations.[22] A research conducted for the European Defence Agency puts the "*efficient information sharing with joint multinational forces and with other military and civilian actors on the ground…*"[23] to the role of an underlying requirement of all main military capabilities. Similarly to generating and maintaining situational awareness, it will be necessary to face the challenges that result from the nature of the information environment, mainly in the form of growing amount of information available, keeping pace with the ongoing advancement of information technology, and meeting the demands for prompt (immediate) information sharing.

More than ever before, the selection and the level of detail of information shared across the entities involved in the operation are essential to handle the increased amount of information. The fact that information is shared does not alone guarantee organization's better knowledge of the situation. Although it is the purpose of shared situational awareness to ensure a common understanding of the situation in the battlefield across the entities involved in the operation, it is substantially counterproductive for everyone to be informed of everything as it wide-spreads information overload. As an experiment conducted at a joint task force headquarters during a large-scale military exercise of the U.S. Army demonstrates, during which the entire operational communication of the whole headquarters was monitored, once the amount of information shared reached a certain threshold, the knowledge of the situation in the battlefield of the staff began to decrease from that moment on.[24] In rare occasions is this phenomenon caused by a faulty configuration of information systems that process the shared information. In most cases it is the human failure error, nourished by the information overload that causes such situations, in the form of mass information distribution or faulty attribution,

22 WATLING, Jack and Daniel ROPER. 2019. *European Allies in US Multi-Domain Operations*. RUSI Occasional Paper. London: Royal United Services Institute, p. 14.

23 KEPE, Marta, James BLACK, Jack MELLING a Jessica PLUMRIDGE. *Exploring Europe's capability requirements for 2035 and beyond: Insights from the 2018 update of the long-term strand of the Capability Development Plan*. Brussels: European Defence Agency, 2018, p. 21.

24 BUCHLER, Norbou, Sean FITZHUGH, Laura MARUSICH, Diane UNGVARSKY, Christian LEBIERE and Cleotilde GONZALEZ. 2016. Mission Command in the Age of Network-Enabled Operations: Social Network Analysis of Information Sharing and Situation Awareness. *Frontiers in Psychology* [online]. 7:937. Available at: https://www.frontiersin.org/articles/10.3389/fpsyg.2016.00937/full.

in which operational attributes are assigned to the information or information product and distributed accordingly. As a result, such information then may be dealt with by personnel that do not need it, or reversely, the personnel that actually need it do not receive it. In both cases, decision-making of the respective personnel related to the operation can be affected.

4 COMMON OPERATIONAL PICTURE

The common operational picture (COP), as an essential "product" generated for the purpose of providing both the group and shared situational awareness, is the main platform enabling the visualization of situational awareness and its sharing with other users. In NATO, this function is conveyed by the NATO Common Operational Picture (NCOP) system, which is able to process and include in the overall picture information from a number of systems used by component commands, member states and other entities if appropriate. In order for this (or any other similar) system to be able to act as *"a single authoritative source of data which reflects the needs of commanders and staffs"*[25] during operations in the current and future operating environment, its capabilities must necessarily reflect current developments in the information environment.

4.1 Real-time common operational picture

As a result of the dynamic developments throughout the entire operating environment, also the demand for developing the capability of real-time decision-making is also growing. Reaching this capability is conditioned, among other things, by the capability to provide real-time situational awareness. In response to this demand, the common operational picture systems get augmented with additional products and service such as applications to visualize the situation to be used in cell phones or tablets. These mobile applications are now being implemented within modern armed forces, predominantly at the tactical level, allowing for immediate sharing of information from the battlefield between individuals and units in the field and their respective tactical operations centres, and thus supporting real-time decision-making significantly. Immediate access to information from the tactical level, rapid development of the situation in the battlefield and the need to coordinate activities across domains stimulate the demand for real-time (or rather near real-time) decision-making (and situational awareness) at the operational level as well.

[25] FORRESTER, Bruce. 2016. *Integrating Social Media Tools with Command and Control (C2): What are the Possibilities?* [online]. Québec. Available at: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc229/ p803913_A1b.pdf. Scientific Report. DRDC – Valcartier Research Centre, p. 29.

The mobile common operational picture will allow the staff members and especially the commander of the operational headquarters to maintain the knowledge of the situation in the battlefield and to make respective decisions, when appropriate, even when distant from the joint operations centre or their workplaces. As a result, the joint operations centre as a central information hub located in a large room with dozens of screens as known today, may soon not the case anymore.

The integration of the mobile operational picture, the large amount of information and frequent incorrect selection of information to be shared through the common operational picture again creates the issue of a negative impact on understanding the situation by the staff and mainly the commander. With a certain degree of simplification, it can be said that not all information should be placed on the map, because too much information not only reduces the lucidity of the picture, but more importantly, it also may prevent the commander from understanding the situation it depicts.[26] Although the common operational picture allows the "map" to be customized by filtering the information displayed, a judicious selection of information (based on its relevancy and in consideration of the developments in the battlefield) to be included in the common operational picture is necessary.

4.2 Cyber common operational picture

The fact that cyberspace is no longer treated only as a space through which information is being transferred but also became a part of the battlefield in which operations are being conducted, has great implications within situational awareness, as this creates the need for a recognised cyber picture to be generated and incorporated into the common operational picture. Not only will this provide situational awareness in cyber operations, but it will also contribute to the effective coordination of the joint effort in future operations across domains.

In relation to generating the common operational picture, Radabaugh points to the difficult task of appropriate visualisation of cyberspace in a way that will allow it to be perceived it the same way as the air, land, maritime and space battlefields. Only in this way, according to him, will it be possible to achieve an effective integration of information and traditional physical force, necessary to conduct operations across domains.[27] However, the question of the technical complexity of the appropriate visualization of the recognised cyber picture, and its incorporation into the common operational picture, is only one of the possible complications in achieving effective integration of cyber warfare into "traditional" warfare. As Conti, Nelson and Raymond emphasise, not only

26 PAUL, Christopher, Colin P. CLARKE, Bonnie L. TRIEZENBERG, David MANHEIM and Bradley WILSON. 2018. *Improving C2 and Situational Awareness for Operations in and Through the Information Environment*. Santa Monica: RAND Corporation.

27 RADABAUGH, Gregory C. 2018. The Practical Implications of Information as a Joint Function. *Joint Force Quarterly*. 89(2), 15-17.

will cyber support be provided, in some cases, by originally "non-cyber" staff without in-depth knowledge and experience in cyber warfare, but the recognised cyber picture (although simplified) will also be provided to commanders and staff with minimal or no knowledge and experience in such a technically oriented area.[28] Initially, this will prevent them from understanding the cyber situation and from acquiring thorough knowledge of the joint situation in the battlefield within all domains. Therefore, it can be expected that, in order to create conditions for a full integration into the common operational picture, cyber situational awareness will initially be provided either separately (that is only in cyberspace) without the need for being interconnected with other pictures, or only in limited support of the common operational picture.

5 DEVELOPING STAFF SKILLS TO PROVIDE SITUATIONAL AWARENESS

Constant advancement of information technology and its increasing integration into military operations places high demands on personnel with respect to their ability to work effectively with the increasingly complex and technically demanding means to process, evaluate, analyse and share information, and these skills have to be permanently and actively developed. The need to enhance the skills of the staff in this field is also closely connected to the already mentioned phenomenon of gradual diminishing of differences in the information technology capacities possessed by the actors. According to Endsley, however, *"the challenges are not simply in learning to physically perform a task and mastering the motor skills required for performance, but rather in perceptual and cognitive task mastery."*[29] In other words, despite the need for training and subsequent practice in using respective tools and systems, it is necessary, with regard to the enormous information burden, to develop the perception and cognitive functions of the staff, such as memory, concentration, logical reasoning, problem-solving, speed of information processing or the ability of expression.

The way these functions are involved in the process of generating situational awareness can be demonstrated on Endsley's model, which captures situational awareness within the decision-making process (Figure 2). The system factors (depicted in the upper part of the figure) represent those characteristics and means that can be assumed to be available to all actors. In the case of the operational headquarters, or its joint operations centre, its hardware and software used to collect, process and analyse information is an

28 CONTI, Gregory, Robert FANELLI, David RAYMOND and John NELSON. 2013. Towards a Cyber Common Operating Picture. In: *2013 5th International Conference on Cyber Conflict: Proceedings* [online]. Tallinn: NATO CCD COE Publications, p. 279-295. Available at: https://ccdcoe.org/uploads/2018/10/CyCon_2013_Proceedings.pdf.

29 STRATER, Laura, FAULKNER, Laurie, HYATT, John, ENDSLEY, Mica. *Supporting Situation Awareness Under Data Overload in Command and Control Visualizations*. Available at: https://www.researchgate.net/publication/252218394_Supporting_Situation_Awareness_Under_Data_Overload_in_Command_and_Control_Visualizations, p. 1.

example of such factors. Although there are also qualitative developments on the side of the system factors, it is unlikely, given the above-mentioned trend of capacity convergence of actors, that predominance will be achieved in this area. On the other hand, the individual factors, that is the factors on the part of an individual or a group, are mainly comprised of the cognitive functions and experience mentioned (indicated by the bold line in the lower part of the figure). These need to be developed by each actor as they cannot be acquired otherwise (for example, to be purchased), as is the case with most system factor. The possibility of achieving dominance is thus limited only by human potential and the efforts made to utilise this potential.

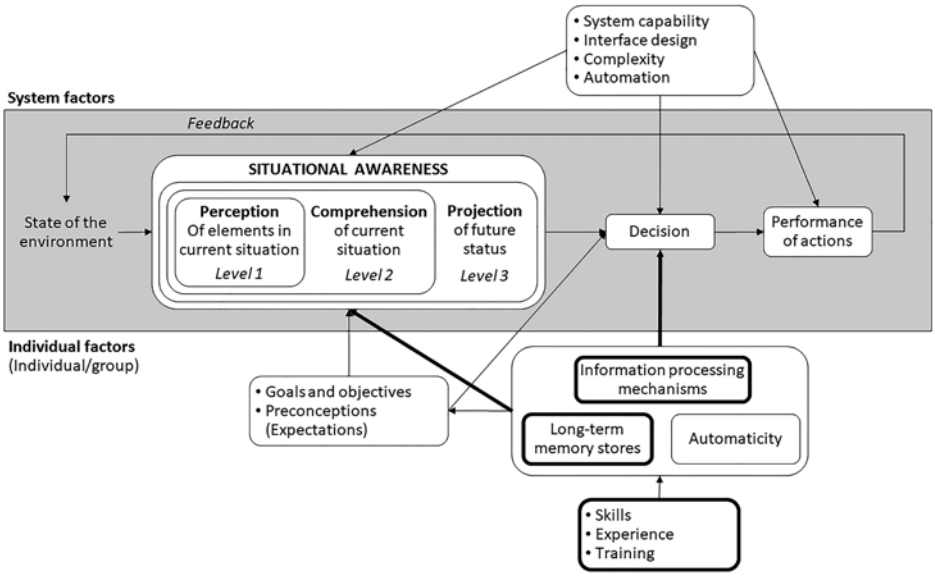


Figure 2: Factors affecting situational awareness and decision-making[30]

In the context of providing situational awareness of the battlefield, the effort to develop these (especially cognitive) functions will increase the ability to maintain awareness of already known facts (the situation), promptly carry out an initial assessment of the importance of the new information, understand this information in the context of the situation, anticipate the possible development of the situation with respect to the new information, and pass it on, in a comprehensible form and with a corresponding level

30 ENDSLEY, Mica R. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society* [online]. 1995, 37(1), 32-64 [cit. 2020-03-12]. ISSN 0018-7208. Available at: http://journals.sagepub.com/doi/10.1518/001872095779049543, p. 35, modified by the author.

of detail, for its further use. To implement specific activities to develop these and many other skills, those findings of the "Cognitive Enhancement"[31] that fall into cognitive psychology or neuropsychology can be used. Considerable effort has already been made in this area within both the military theory[32] and practice[33], and its results can be used as a source of inspiration or a basis for possible further research or practical implementation of appropriate enhancement activities.

CONCLUSION

The dynamic development of the information environment affects all aspects of situational awareness, the considerable importance of which will increase even further in future operations. In order for Joint Task Force Headquarters to be able to provide thorough and accurate situational awareness and to share it effectively across operational domains, it is essential to understand this environment, monitor its development and continuously strive to develop the situational awareness capability accordingly.

To generate and maintain situational awareness, current and future operations cannot do without advanced information technology capable of processing and analysing a vast amount of data from the battlefield, sharing the respective derived information in real time across operational domains, and ensuring their ceaseless protection. However, for the effective use of advanced information technology it is necessary to adapt the settings of the internal operation-related information management processes, and more importantly, to develop the skills of the personnel to work with this technology, its products and information itself. This will be essential to understand the information in the context of the current situation not only within the respective domain but also in general, joint perspective, and to anticipate the impact of these facts on the future situation. More than on technical skills, it is thus particularly important to focus

31 "Cognitive Enhancement" is a discipline that deals with the possible enhancement of the brain performance for the purpose of improving cognitive functions. Although pharmaceuticals are often used in this context, and a considerable attention is being focused on interconnecting advanced technology with, or even its implantation inside the human body, a number of "non-invasive" psychological or neurological techniques is being used, ranging from common "brain training" exercises to meditation to specialized exercises using modifiable simulations of work-related tasks.

32 See BRUNYÉ, Tad T., Randy BROU, Tracy Jill DOTY, Frederick D. GREGORY, Erika K. HUSSEY, Harris R. LIEBERMAN, Kari L. LOVERRO, Elizabeth S. MEZZACAPPA, William H. NEUMEIER, et al. A Review of US Army Research Contributing to Cognitive Enhancement in Military Contexts. *Journal of Cognitive Enhancement* [online]. [cit. 2020-04-19]. DOI: 10.1007/s41465-020-00167-3. ISSN 2509-3290. Dostupné z: http://link.springer.com/10.1007/s41465-020-00167-3.

33 See BAUCOME, Randal G. Military Intelligence Soldiers Receive Cognitive Enhancement. *U.S. Army* [online]. August 18, 2017 [cit. 2020-04-19]. Dostupné z: https://www.army.mil/article/192624/military_intelligence_soldiers_receive_cognitive_enhancement.

See USASOC Public Affairs. U.S. Army Special Operations Command rolls out new strategy. *U.S. Army* [online]. October 17, 2019 [cit. 2020-04-19]. Dostupné z: https://www.army.mil/article/228605/us_army_special_operations_command_rolls_out_new_strategy.

on a comprehensive and a time-consuming effort of the cognitive development of the personnel.

Lastly, providing situational awareness at the operational level will also be shaped, in a very specific way, by operations conducted in cyberspace. In addition to developing the technical capacities of the headquarters and the skills of "cyber personnel" to interpret the situation in this space intelligibly, it is necessary to ensure that "non-cyber personnel" have a general understanding of the cyber activities which will allow them to comprehend the situation in cyberspace in the context of overall, joint situational awareness to support well-informed decision-making in operations.

Author: ***MAJ Marek Fiebich, M.A.,*** *born in 1983. Graduated from the University of Defence in Brno (2008), the Metropolitan University Prague (2010) and the University of Leicester, UK (2016). From 2008 to 2013, he served at different land forces units within military intelligence and operations. In 2010, he was deployed to ISAF, Afghanistan, as a military intelligence officer. From 2013 to 2016, he served at the Multinational Joint Headquarters Ulm, Germany, as a combined joint operations centre officer. After his return in 2016, he was appointed to the Land Forces Command Operations Directorate. From 2018, he serves at the Department of Military Strategic Studies of the Centre for Security and Military Strategic Studies in Brno. He deals with operational art and operational environment.*

How to cite: FIEBICH Marek. Situational Awareness and Current Information Environment. *Vojenské rozhledy*. 2020, 29 (3), 025-040. ISSN 1210-3292 (print), 2336-2995 (online). Available at: www.vojenskerozhledy.cz

 DOI: 10.3849/2336-2995.29.2020.03.041-056

Peer-reviewed

Leaderless Resistance: Development, Countering and Research of Insurgent Concept

Odpor bez vůdce: vývoj, potlačování a výzkum povstaleckého konceptu

Miroslav Mareš

Abstract: The paper deals with an insurgent strategic concept "leaderless resistance". It was elaborated by US intelligence officer Colonel Ulius Louis Amoss. It is used by various insurgent actors and it is researched within the context of insurgency and counterinsurgency and interconnected issues (extremism, terrorism etc). The author of this contribution deals with the development tendencies and with the strengths and weaknesses of this strategy (including the derived concepts as "leaderless Jihad" etc.). Its adaptation in the era of modern political and hybrid warfare is explained. Challenges for successful countering from the point of view of security architecture (intelligence and law enforcement agencies, army, non-.state actors) are discussed.

Abstrakt: Článek se zabývá povstaleckým strategickým konceptem „odporu bez vůdce". Byl vytvořen americkým zpravodajským důstojníkem plukovníkem Uliusem Louisem Amossem. Je užíván různými aktéry a je zkoumán v kontextu povstalectví a proti-povstalectví a souvisejících problémů (extremismus, terorismus apod.). Autor tohoto příspěvku se zabývá vývojovými tendencemi a silnými a slabými aspekty této strategie (včetně odvozených konceptů, jako je „džihád bez vůdce" apod.). Je vysvětlena jeho adaptace na moderní politickou a hybridní válku. Diskutovány jsou výzvy pro úspěšné potírání z hlediska bezpečnostní architektury (zpravodajství a agentury vymáhající právo, armáda, nestátní aktéři).

Keywords: Resistance; Counter-insurgency; Extremism; Terrorism; Intelligence.

Klíčová slova: Odboj; proti-povstalectví; extremismus; terorismus; zpravodajství.

INTRODUCTION

Historical and contemporary insurgencies and their countering pose a significant challenge to military forces, law enforcement agencies and intelligence services. Insurgent strategies and tactics are also objects of expert discussions and academic research. Theory and practice can be in a close interconnection, as the development of the concept "leaderless resistance" shows. A short essay written originally by US intelligence officer Ulius Louis Amoss in the early 1950 s was later able to affect several important insurgent thinkers from various extremist scenes and it has a strong impact also in contemporary world. Underdeveloped seems to be research of its recent impact on the military sphere.

The goals of this article are to explain the origins, spread and contemporary use of "leaderless resistance", to analyze its specific interconnection with the military sphere (including its overlap with modern political and hybrid warfare) and to discuss challenges of countering this phenomenon. With respect to these goals, the research questions are: 1) how "leaderless resistance" affected insurgent and terrorist strategies, 2) how can "leaderless resistance" be interconnected with the military sphere and 3) how this strategy can be successfully eliminated. A strategic analysis within the context of research of insurgency and terrorism as well as approaches of intelligence studies will be used[1]. East Central European perspective is emphasized in the article, because the impact of "leaderless resistance" was not systematically researched in this area[2] (despite the fact that the origins of the concept have strong ties to East Central Europe – see below).

1 ANALYTICAL FRAMEWORK: A NETWORK PERSPECTIVE, (NON)HIERARCHY AND CELLS

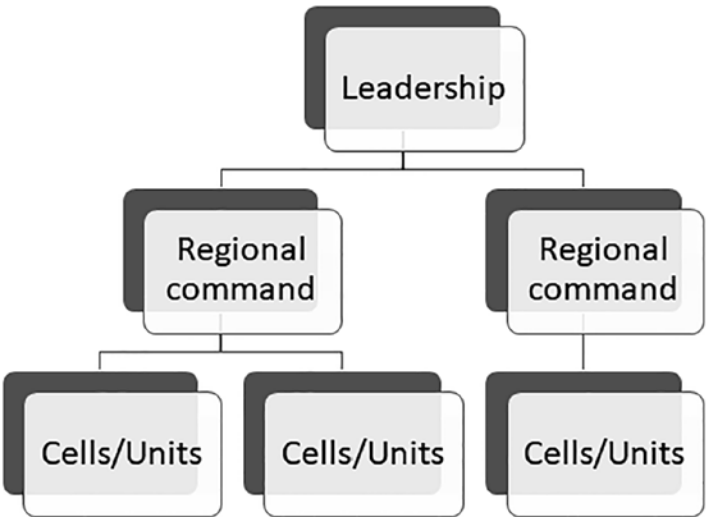
The concept of "leaderless resistance" is based on a free structure of actors involved. Due to this fact, the best approach how to understand its position within the spectrum

1 GOMPER, David C., Paul K. DAVIS, Stuart E. JOHNSON a Duncan LONG. *Analysis of Strategy and Strategies of Analysis*. RAND Corporation, 2008. ISBN 13: 9780833045034.

2 Some specific issues related to extreme right „lone wolves" were discussed in MAREŠ, Miroslav a Richard STOJAR. Extreme right perpetrators. FREDHOLM, Michael. *Understanding Lone Actor Terrorism.: Past experience, future outlook, and response strategies.* London: Routledge, 2016, s. 66-86. ISBN 9781138309142. The diploma thesis written by Pavel Drlík offers an interesting case study of the "National Resistance". DRLÍK, Pavel. *Případová studie aktéra "Netwar"*. Brno, 2009. Dostupné také z: https://is.muni.cz/th/ocvin/Pripadova_studie_aktera_netwar.pdf. Bakalářská práce. Masarykova univerzita. Vedoucí práce Martin Bastl.

of insurgent strategies (including terrorist strategies[3]) should be based on a structural analysis of subversive entities. Such approach offers a network analysis, elaborated by Richard Matthew and George Shambaugh. They divided terrorist structures into two main categories: 1) the traditional hierarchical model with a commander and subordinated units 2) modern "netwar" model consisting of free non-hierarchical network of involved units[4]. The hierarchical model can include more commando-levels (a pyramidal model) or the leaders can coordinate cells and these cells do not have contacts among them (centralized coordinated model). Within the "network" structure we can distinguish between interconnected linear network of cells (they coordinate directly and immediately their activities) and a diffused model (cells without direct contacts among them, they are coordinated only by common goals, not by direct communication and coordination). In a very simplified way the foundations of these models are outlined in the following graphics.

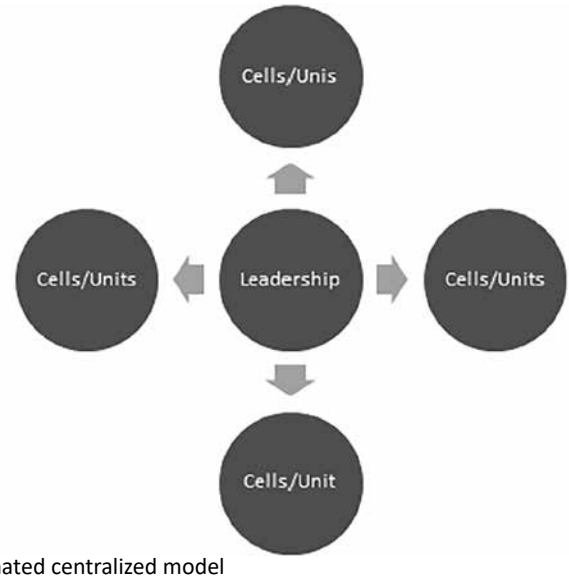
Basic models of insurgent structures



Scheme 1: Pyramidal hierarchical model

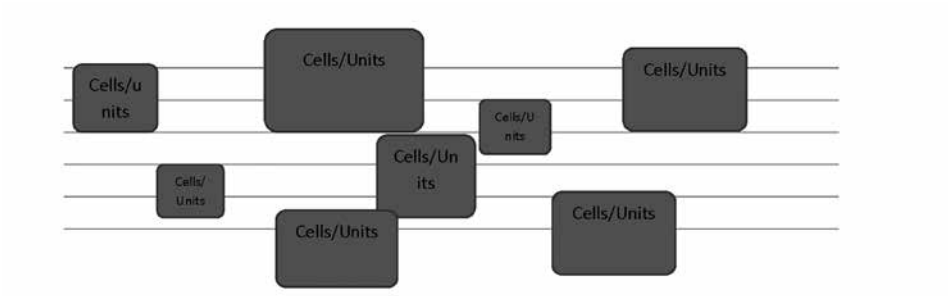
3 Due to the fact that contemporary conceptualizations of insurgencies and terrorism are in many cases closely interconnected, in this article subversive terrorism will be subsumed under a broader spectrum of insurgent strategies. This approach is typical of Israeli expert Ariel Merari. See MERARI, Ariel. Terrorism as a strategy of insurgency. *Terrorism and Political Violence*. 1993, 5(4), 213-251. DOI: 10.1080/09546559308427227. ISSN 0954-6553. Dostupné také z: http://www.tandfonline.com/doi/abs/10.1080/09546559308427227

4 MATTHEW, Richard a George SHAMBAUGH. The Limits of Terrorism: A Network Perspective1. *International Studies Review*. 2005, **7**(4), 617-627. DOI: 10.1111/j.1468-2486.2005.00536.x. ISSN 1521-9488. Dostupné také z: https://academic.oup.com/isr/article-lookup/doi/10.1111/j.1468-2486.2005.00536.x.



Scheme 2: Coordinated centralized model

Scheme 3: Linear model



Scheme 4: Diffused model

In the diffused model some units/cells can play much a more important role than the others and their importance can step by step create informal and later formal leadership in an insurgent movement. It is important to emphasize that the dynamics of networks plays an important role in their analysis as well as in their countering. According to Matthew and Shambaugh: "if network-based terrorist groups are successful in creating a more hierarchical structure, the increased organization and higher levels of coordination will likely generate new preferences and new vulnerabilities that make these hierarchical terrorist networks easier to target and neutralize"[5]

Each insurgent movement faces several dilemmas. Ethan Frisch identified the following ones:

1. Action versus secrecy (requirement to carry out attacks on the one hand and to be caught on the other hand);
2. Growth versus control (a growing number of members, controlled areas and actions lead to loss of efficient control over the insurgent movement);
3. Recruitment versus retention (how to force the recruited members to fulfil their commitments and to keep them in the insurgent organization);
4. Success versus longevity (insurgent organizations should achieve at least short-term goals and to survive to achieve long-term goals);
5. Resources versus constituencies (insurgents groups need support and sources from the population and if they use direct violence against people, they cause "constituent alienation")[6]. Free network of cells can be a rational choice in the first phase of insurgencies, later it can transform into more deeply structured and/or hierarchical forms. In such cases the concept of proto-insurgency can be useful for an analysis. David Byman defines proto-insurgency as „a small, violent group that seeks to gain the size necessary to more effectively achieve its goals and use tools such as political mobilization and guerrilla warfare as well as terrorism"[7]. If the insurgent movement maintains the free cell or the linear model in a long-term perspective, it can be subsumed under the concept of the 4th generation of warfare[8] and also under new concepts of warfare (as will be more deeply discussed later in the „military" chapter of this article).

---

5 MATTHEW, Richard a George SHAMBAUGH. 2005, 626.

6 FRISCH, Ethan. Insurgencies are Organizations Too: Organizational Structure and the Effectiveness of Insurgent Strategy. *Peace & Conflict Review*. 2011, 6(1), 17-41. ISSN 1659-3995. Dostupné také z: http://www.review.upeace.org/images/pcr6. 1. pdf

7 BYMAN, Daniel. *Understanding Proto-Insurgencies*. Santa Monica: RAND Corporation, 2007. ISBN 978-0833041364. Dostupné také z: https://www.rand.org/content/dam/rand/pubs/occasional_papers/2007/RAND_OP178.pdf

8 Fourth generation of warfare is characterized by the fact that „in response to the overwhelming capability of the modern conventional military forces, weaker opponents began resorting alternative ways of waging wars, as insurgency, "terrorism" and other forms of "asymmetric" conflict." PERLA, Peter P., Albert A. NOFI a Michael C. MARKOWICZ. *Wargaming Fourth Generation Warfare (U).* [online]. Alexandria: CNA Corporation, 2006 [cit. 2020-06-28]. Dostupné z: https://www.cna.org/CNA_files/PDF/D0014752.a2.pdf

2 ORIGINS OF THE CONCEPT: FAILURE OF WESTERN SECRET OPERATIONS IN THE COMMUNIST BLOC

"Leaderless resistance" is recently presented as an example of the diffused model used by non-state actors, however, it was created with more sophisticated - "state-linked" - goals and with the potential to change into different forms of insurgency. Its origins must be understood within the context of the beginning of the Cold War (and its possible outbreak into the „hot" Third World War"). The author of the original concept was Ulius Louis Amoss[9]. He published his essay called "Leaderless Resistance. New Tactics for an Old War " in 1953 for US intelligence community for the first time. After his death it was reprinted for broader public on 17 April 1962[10].

The main message of the paper is unsatisfaction with the Western approach towards anti-communist resistance movements in Eastern Europe and with many failures of secret agents from exile organizations that cooperated with Western intelligence services. He stated the West was losing the Cold War, because: "The enemy has adopted new tactics, tactics that make the classic underground system obsolete, tactics that doom great secret organizations because they can no longer remain secret."[11]

The scope of primarily Amoss's criticism was relatively narrow. It aimed at the fact that communist agents penetrated into exile political organizations. This fact caused the above mentioned disclosure of whole insurgent networks in the countries of the Communist Bloc. He also evaluated overestimation of the role of money negatively, which was supplied by Western special services to the hands of resistance organizations and these were willing to act only due to this financial support. Lack of leaders characterized resistance in the communist countries and the exile organizations were not able to generate "new Titos" (in the sense of strong insurgent commanders after the model Josip Broz Tito during the Second World war)[12].

Polish political émigré and their controversial links caused Amoss' *biggest concern. He* emphasized the destruction of the Polish underground organization "Association Freedom and Independence" (Zrzeszenie Wolność i Niezawisłość - WiN"). As Amoss wrote, its

9 Colonel Ulius Louis Amoss was a US intelligence officer of Greek origin. He was born in 1895. During the Second World War he joined the Office of Strategic Services (OSS¨) and led its office in Kairo (which was responsible for operations in Northern Africa and Southern Europe). Since 1947 he worked for the Central Intelligence Agency (CIA) and in 1948 he established the allegedly commercial International Services of Information (INFORM), however, it was a CIA cover organisation. He died in 1961. SIMKIN, John. Ulius Louis Amoss. In: *Spartacus Educational* [online]. N.: Spartacus Educational, 1997 [cit. 2020-06-28]. Dostupné z: https://spartacus-educational.com/JFKamossU.htm

10 AMOSS, Ulius Louis. Leaderless Resistance. New Tactics for an Old War. *Inform*. 1962, N.(6205), 1-4. (archive of the Wisconsin Historical Society).

11 AMOSS, Ulius Louis. 1962, 1.

12 AMOSS, Ulius Louis. 1962, 1-3.

leader was uncovered and forced to cooperate with the Polish secret police[13]. Another case was related to parachutists trained at an American intelligence school in Western Germany, who were arrested after communist agents in exile organizations informed their commanders in Warsaw[14]. Trials with Western agents in Poland in 1952-1953 initiated Amoss' reasoning to change the previous approach of US intelligence towards anti-communist resistance in Eastern Europe.

He struggled for segregation of political action (exile government, exile and underground political parties etc.) from intelligence and subversive activity. "Political émigré organizations must never be entrusted with tasks of a military intelligence or subversive nature. Subversive activity must be entrusted only to elite groups, small in size, strictly isolated from one another."[15]

3 "LEADERLESS RESISTANCE" 1. 0. : SPONTANEOUS FREELY ORGANIZED ANTI-COMMUNIST MOVEMENT WITH WESTERN SUPPORT

American intelligence should construct its own intelligence network, independent on émigré political institutions. Political emigrants should not be involved in training of intelligence and subversive activities. An exposed (even partially) underground organization, whether American or émigré, must be considered as lost[16]. Amoss also stated: "Individuals who proved successful in underground work under the Germans are not to be considered automatically qualified for work under Soviet occupation. Current psychological, moral and technical factors are vastly different, and so are the loyalties"[17].

The above mentioned ideas are rooted in intelligence work with own agents. Amoss' main contribution to the theory of insurgency is presented in the last part of his paper.

13 In fact, the WiN was penetrated by agents of the Polish communist secret service called Department of Security (Urząd bezpieczeństwa – UB). They were able to take over control of the leading structure of the WiN. In 1948-1952, the Polish UB played with the CIA a spy game which caused elimination of hundreds anti-communist activists. Polish secret service used the name „Operacja Cezary" for designation of this game. FRAZIK, Wojciech. Operacja "Cezary". Prowokacyjna v komenda WiN. *Biuletyn Instytutu Pamięci Narodowej*. 2008, 8(1-2 (84-85), 167-170. ISSN 1641-9561.

14 AMOSS, Ulius Louis. 1962, 1-2.

15 AMOSS, Ulius Louis. 1962, 2.

16 AMOSS, Ulius Louis. 1962, 2.

17 AMOSS, Ulius Louis. 1962, 2.

He labelled[18] the concept of large underground systems "with its cells everywhere and its couriers swarming from center to center" [19] as passed. As a "sweeping the Soviet orbit" he declared "leaderless resistance", as a spontaneous movement without traditional political representation. This movement should be supported by Western intelligence services.

The core of Amoss' *message is in the following sentences: "*In the event of war, obviously the West would like the satellite armies to "come to over". This can be achieved only if we are able to create among the rank and file of these armies the proper climate and a genuine desire to do so. No organization is capable of accomplishing this thing. No one's orders would be obeyed. But the rank and file would come over if their morale was properly influenced. For this we do not need "leaders"; we need leading ideas. These ideas would produce leaders. The masses would produce them and the ideas would be their inspiration"[20].

If we analyze these words, we can see the author's struggle to support a spontaneous movement which follows common ideas and these ideas are able to mobilize to various acts of resistance. The role of US intelligence is to offer popular ideas to oppressed people and to support various parts of the freely organized resistance movement. Real activities can generate new leaders who can take control over broader parts of the movement. With these new leaders Western intelligence should cooperate. "Leaderless resistance" can be also only the starting phase of the resistance movement which can receive new leaders. If the new leaders are uncovered, thanks to the spontaneity and diffusion of the movement, they can be substituted. Amoss predicted: "It could be the time when Bolshevism would pull in its lines, sullenly giving up one country after another – and with no danger of general war"[21].

We can see that the concept elaborated by Amoss (he labelled it as "tactics") includes foreign state support through intelligence service to a spontaneous movement, which is not linked to emigrant structures, it is originally non-hierarchically organized and which tries to achieve common popular goals. This movement can change its substance and it will generate new leaders. Interaction of governmental intelligence activities and a leaderless resistant movement in foreign countries are typical of Amoss' original concept.

---

18 Despite the fact that Amoss did not quote any authors or works linked to this traditional system, might to be that his criticism reacts to the publication written by Ferdinand Otto Miksche. The Czechoslovak emigrant was inspired by the WW II experience and he proposed hierarchical structures with specialized branches as an optimal architecture of an underground movement in his book, which was first published in 1947 (it was re-edited several times and became popular at the turn of the 1940 s/1950 s). MIKSCHE, Ferdinand Otto. *Secret Forces.: The Technique of Underground Movements*. 2. London: Faber and Faber Limited, 1951. ISBN N., p. 113.

19 AMOSS, Ulius Louis. 1962, 3.

20 AMOSS, Ulius Louis. 1962, 3.

21 AMOSS, Ulius Louis. 1962, 4.

4 REBIRTH OF "LEADERLESS RESISTANCE" AND ITS SPREAD

In the era of the publication of the original version of Amoss' paper, it had only a limited impact. According to US expert Chip Berlet, it was propagated in leaflets airdropped over Cuba in 1961, which were prepared by anti-Castro Cuban exile activists with ties to the CIA. Establishing of "phantom cells" (Celulas Fantasmas) was demanded[22]. "Leaderless resistance" was allegedly discussed also as a model of insurgency in the case of the communist occupation of the United States of America[23]. The white supremacist scene was later responsible for the "2. 0. version" of "leaderless resistance" and for its spread. In 1983, Louis Beam[24] published in the internal newsletter of the Ku Klux Klan a paper called "Leaderless Resistance", in which he presented and developed Amoss' *ideas*, adapted for the purposes of white supremacist movement[25]. Beam discussed this concept within the US far right-wing militant scene[26] and in 1992 his paper was revised and reprinted in the far-right journal "The Seditionist"[27]. This version was broadly widespread, firs in the United States and later world-wide. It strongly influenced the racist and neo-Nazi scene in many countries.

Beam proposed, similarly as Amoss, establishing of a non-pyramidal resistance movement which will be able to resist against infiltration of enemie's secret agents. In contrast to Amoss, the enemy was not the communist rule, but, federal institutions of the United States of America. The white supremacist scene should be able to generate common

22 BERLET, Chip. Leaderless Resistance Publishing History. *Chip Berlet's Blogsite: Research for Progress* [online]. http://www.researchforprogress.us/topic/: Chip Berlet, 2017 [cit. 2020-06-28]. Dostupné z: http://www.researchforprogress.us/topic/39014/leaderless-resistance-publishing-history/

23 MCALLISTER, Bradley a Alex P. SCHMID. Theories of Terrorism. SCHMID, Alex P. *Routledge Handbook of Terrorism Research*. London: Routledge, 2011, s. 201-271. ISBN 9780415411578.

24 Louis Beam was born in 1946. He served as a machine-gunner on helicopter in Vietnam and he was awarded the Distinguished Flying Cross. After return to the USA he started to be active in the militant white racist scene, among others in the Ku Klux Klan and in the organization Aryan Nations. He published his own journal The Seditionist. He is considered an important person in the intellectual and strategic background of the white supremacist scene in the 1980 s and 1990 s. SOUTHERN POVERTY LAW CENTRE. Louis Beam. *Southern Poverty Law Centre* [online]. Montgomery: Southern Poverty Law Centre, 2020 [cit. 2020-06-28]. Dostupné z: https://www.splcenter.org/fighting-hate/extremist-files/individual/louis-beam

25 BEAM, Louis. Leaderless Resistance. *Inter Klan Newsletter & Survival Alert*. 1983, N.(N.), 12-13. ISSN N. Dostupné také z: https://simson.net/ref/leaderless/1983.inter-klan_newsletter.pdf Beam was active in the Ku Klux Klan, however, he had broader ambitions to mobilize masses of white supremacists. Due to this fact he published a paper about non-hierarchical strategy in the journal published by a strong hierarchical pyramidal organization. Later he left the KKK and also the KKK split into various factions. According to Kathleen Blee and Mehr Latif, a number of local Klans moved more underground and they cooperated with racist skinheads and neo-Nazis. BLEE, Kathleen a Mehr LATIF. Ku Klux Klan. Vigilantism against blacks, immigrants and other minorities. BJØRGO, Tore a Miroslav MAREŠ. *Vigilantism against Migrants and Minorities*. London: Routledge, 2019, s. 31-42. ISBN 9781138493926.

26 Leader of the organisation White Aryan Resistance (W.A.R.) Tom Metzger was an important partner in these discussions

27 BEAM, Louis. Leaderless Resistance. *The Seditionist*. 1992, N(12), 1-4. Dostupné také z: http://www.louisbeam.com/leaderless.htm

ideas and propaganda for phantom cells of the resistance movement. It means that some "strategic circles" of the white supremacist scene have to play a similar role as the US intelligence in the original concept from the 1950 s.

Beam stated: "Members of phantom cells or individuals will tend to react to objective events in the same way through usual tactics of resistance. Organs of information distribution such as newspapers, leaflets, computers, etc., which are widely available to all, keep each person & informed of events, allowing for a planned response that will take many variations. No one need issue an order to anyone. Those idealist truly committed to the cause of freedom will act when they feel the time is ripe, or will take their cue from others who precede them.[28]"

These ideas were in the 1990 s and 2000 s able to find response in the militant right-wing extremist spectrum in Western countries. A broad spectrum of violent actions committed by various actors (members of youth subcultures as racist skinheads, frustrated military veterans or idiosyncratic racists) required a reasonable strategic concept to improve the propagandist impact and efficiency of militant activities. "Leaderless resistance" was broadly accepted, at least as one of possible ways of the "fight against system".

Its spread was accompanied also by publications of other authors than Louis Beam. For example, in the novel "Hunter" written by Andrew Macdonald[29] (pseudonym for William Pierce[30]), in the publication "Leaderless Resistance: Where There's a Will There's a Way "of British National Anarchist activist Troy Southgate[31] or in the guideline "The Field Manual" written by Max Hammer (pseudonym of the Norwegian neo-Nazi activist Erik Nielsen) for purposes of the transnational organization Blood & Honour (he recommend the use of "leaderless resistance" only in some countries)[32].

In the Czech Republic, "leaderless resistance" was propagated in the neo-Nazi spectrum in the second half of the 2000 s[33]. Mostly the neo-Nazi organizations National Resistance (Národní odpor - NO) and Autonomous Nationalists (AN)[34] were inspired by them. They had the possibility to use also the Czech translation of the novel "Hunter"[35]. In 2015, the Czech translation of the original paper by Louis Beam was published in far

28 BEAM, Louis. 1992

29 MACDONALD, Andrew. *The Hunter*. 2. Hillsboro: National Vanguard Books, 1998. ISBN 9780937944097.

30 William Luther Pierce (1933-2002) was leader of the neo-Nazi organisation National Alliance.

31 MACKLIN, Graham D. Co-opting the counter culture: Troy Southgate and the National Revolutionary Faction. *Patterns of Prejudice*. 2005, 39(3), 301-326. DOI: 0.1080/00313220500198292. ISSN 14617331.

32 HAMMER, Max. *The Field Manual*. N: Blood & Honour, 2000. ISBN N. Author's archive.

33 BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. Čeští neonacisté se zviditelňují. *Bezpečnostní informační služba* [online]. Praha: Bezpečnostní informační služba, 2007 [cit. 2020-06-30]. Dostupné z: https://www.bis.cz/aktuality/cesti-neonaciste-se-zviditelnuji-85429626.html

34 MAREŠ, Miroslav. Hrozba politického extremismu z hlediska ozbrojených sil České republiky. *Vojenské rozhledy*. 2009, 18(50)(2), 138-151. ISSN ISSN 1210-3292.

35 It was published by the publisher Kontingent Press. It included preface in which the publisher explained that the Czech edition was motivated by educational and anti-Racist aims. KONTINGENT PRESS. Předmluva. *Lovec*. Praha: Kontingent Press, 2008, s. 5-6. ISBN 978-80-254-3105-4.

right circles[36]. The Czech scene transmitted the ideas of "leaderless resistance" to Slovak right-wing extremists[37].

5 REAL IMPACT OF "LEADERLESS RESISTANCE"

However, despite the broad widespread of the idea of "leaderless resistance" its impact on real activities was for a long time limited. As an action inspired by this concept was mentioned mostly the Oklahoma city bombing on 19 April 1995. Two right-wing extremist perpetrators – Timothy McVeigh and Terry Nichols – attacked a federal building and killed 168 victims[38]. According to expert Daniel Koehler, the German right-wing terrorist group National Socialist Underground (Nationalsozialitsicher Untergrund), which operated in 1999-2011, might have been influenced by Louis Beam's "leaderless resistance" ideas[39].

But the use of "leaderless resistance" did not seem to be very efficient until the mid of the 2010 s. A series of right-wing extremist lone-wolf attacks in Western countries in the second half of the second decade of the 21st century (mostly in the year 2019 - New Zealand, USA, Germany) renewed academic debates about the concept. Some authors see in these attacks confirmation of the success of "leaderless resistance".[40]. During the time of the Corona-Crisis experts warn that the right-wing extremist scene in the USA uses the concept of "leaderless resistance" to accelerate violent protests against anti-pandemic restrictions and to support terrorist attacks (connected with racial-specific victims of the

36 LOUIS, Beam. Odpor bez vůdce. *Délský potápěč* [online]. Praha: Délský potápěč, 2015 [cit. 2020-06-30]. Dostupné z: https://deliandiver.org/2015/07/louis-beam-odpor-bez-vudce.html. The same publisher translated also a text critical towards „leaderless resistance" in which the author calls for a movement with a strong leader. MORGAN, John. Odpor s vůdcem aneb dilema dnešní pravice. *Délský potápěč* [online]. Praha: Délský potápěč, 2015 [cit. 2020-06-30]. Dostupné z: https://deliandiver.org/2015/03/odpor-s-vudcem-aneb-dilema-dnesni-pravice.html

37 JANÍČEK, Tomáš. *Súčasné krajne pravicové násilie na Slovensku*. Brno, 2015. Diplomová práce. Fakulta sociálních studií Masarykovy univerzity. Vedoucí práce Miroslav Mareš.

38 MARTIN, Gus. *Understanding Terrorism. Challenges, Perspectives and Issues*. 4. London: Sage, 2012. ISBN 978-1452205823.

39 KÖEHLER, Daniel. The German 'National Socialist Underground (NSU)' and Anglo-American Networks. The Internationalisation of Far-Right Terror. JACKSON, Paul a Anton SHEKHOVTSOV. *The Post-War Anglo-American Far Right: A Special Relationship of Hate*. New York: Palgrave Macmillan, 2014, s. 122-141. ISBN 978-1-137-39621-1.

40 Leonard Weinberg stated: „The evident inability of the FBI and other law enforcement agencies to identify potential perpetrators, much less anticipate their attacks, provides support for Louis Beam's decades-old argument". WEINBERG, Leonard. Lone Wolf Attacks Prove Louis Beam Was Right About "Leaderless Resistance". *Fair Observer* [online]. Mountain View: Fair Observer, 2019 [cit. 2020-06-30]. Dostupné z: https://www.fairobserver.com/global-terrorism-news/lone-wolf-attacks-louis-beam-leaderless-resistance-domestic-terrosrim-us-news-88710/

COVID-19 and with the federal character of measures) with the goal to attract more people to see its propagandist platforms (various chats in Telegram or Gab)[41].

Recent trend can confirm the impact of original Beam's ideas, however, it is not clear if all perpetrators really act with the intention that they are part of a resistance movement[42]. Declared inspiration by other lone wolves (Anders Breivik, Brenton Tarrant etc.) does not seem to be sufficient for labelling their attacks as "leaderless resistance". However, it is definitely a dangerous trend with a potential to mobilize further supporters.

The concept of "leaderless resistance" is broader than only lone-wolf terrorism[43]. It should serve to a mass wave of subversive activities. Recent academic tendency to connect it only with lone-wolf terrorism is too narrow and it ignores the ideological and strategical dimension (among others production of leading ideas by strategic thinkers within the movement).

"Leaderless resistance" is not limited to the right-wing extremist scene. Similar concepts were developed also by other extremist streams. American expert Marc Sageman sees clear similarities between Beam's ideas and the main line of the publication "The Call to Global Islamic Resistance", written by Hakim (known as Abu Musab al-Suri or Mustapha Setmariam Nasr) from 2004. Sageman speaks in this context about "leaderless Jihad"[44]. Another expert, Paul Joosse, identified convergency between the structures of environmental extremists and "leaderless resistance"[45]. It is difficult to prove that Islamists or environmental extremists read Beam's paper, but due to many overlaps it is not excluded.

6 "LEADERLESS RESISTANCE", MILITARY SPHERE AND HYBRID THREATS

If we turn back to the roots of Amos' and Beam's concepts of strong resistance movements which should be able to generate new leaders and more sophisticated forms of insurgent warfare, we do not see such success of "leaderless resistance" up to now. The

41 WALLNER, Claudia a Jessica WHITE. The Far-Right and Coronavirus: Extreme Voices Amplified by the Global Crisis. *Royal United Services Institut* [online]. London: Royal United Services Institut, 2020 [cit. 2020-06-30]. Dostupné z: https://rusi.org/commentary/far-right-and-coronavirus-extreme-voices-amplified-global-crisis

42 KOEHLER, Daniel. *Right-Wing Terrorism in the 21st Century: The 'National Socialist Underground' and the history of terror from the Far-Right in Germany*. London: Routledge, 2017. ISBN 978-1138123281.

43 See the comprehensive strategic analysis (including propagandist aspects) in TOMASIEWICZ, Jarosław. Strategia oporu niekierowanego w wojnie asymetrycznej. *Przegląd Geopolityczny*. 2009, 1(1), 161-190. ISSN 2080-8836. Dostupné také z: https://przeglad.org/wp-content/uploads/2015/01/Tomasiewicz_Jaroslaw_PG_t.1.pdf.

44 SAGEMAN, Marc. *Leaderless Jihad Terror Networks in the Twenty-First Century*. Philadelphia: University of Pennsylvania Press, 2008. ISBN 9788170493532.

45 JOOSSE, Paul. Leaderless Resistance and Ideological Inclusion: The Case of the Earth Liberation Front. *Terrorism and Political Violence*. 2007, 19(3), 351-368. DOI: 10.1080/09546550701424042. ISSN 0954-6553.

fact is that only acts of lone-wolf terrorists and small cells without capability to establish a strong and widespread militant movement remained. On the other hand, the security environment has changed in comparison with the Cold war and perception of warfare includes its new forms. In the new forms (or generations of warfare) the effectiveness of "leaderless resistance" can be improved.

Maintaining of the militant milieu and permanent mobilization of supporters (including the use of the internet) are basic conditions for building subversive capacities within the context of the 4th generation warfare, which is based on asymmetric approaches. Expert George Michel even sees "leaderless resistance" as an adapting phenomenon to the Fifth-generation of warfare due to its growing connection with the use of modern technologies and transnationalisation. An unrestricted battlefield is typical of "leaderless resistance" as well as of the 5thGW[46].

Despite the fact that military efficiency of "leaderless resistance" was relatively low up to now, we can find significant overlaps of its actors with the military sphere. The military background had several important authors or perpetrators related to "leaderless resistance". Louis Beam and Timothy McVeigh were both military veterans (Beam from the Vietnam war and Macveigh from the Gulf war). Frustrated soldiers or veterans can be due to their skills important members of small "phantom cells" or perpetrators of individual attacks.

In contrast, military staff can also be a target of attacks committed within the context of "leaderless resistance". They are perceived as part of the "system". Perpetrators can be other soldiers or people from non-military environment. It is important to mention that many contemporary individual terrorists consider themselves "soldiers" and they sometimes wear obscure uniforms during their actions or they link their acts to war conflicts[47]. It can cause also their interest to confront "real soldiers".

In broader context "leaderless resistance" can be utilized within the context of contemporary hybrid warfare. Spontaneous violent free network can cause chaos and it can facilitate operations of special forces and well directed paramilitary groups during the "hot phase" of the hybrid war. During the long-term hybrid campaigns, respectively within the context of political warfare[48], stabile "leaderless resistance" movement can be used as a tool to weaken and discredit the enemy. Support of such movements by foreign intelligence returns us to the origins of Amoss' concept.

46 MICHAEL, George. *Lone Wolf Terror and the Rise of Leaderless Resistance*. Nashville: Vanderbilt University Press, 2011. ISBN 9780826518576.

47 HARTLEB, Florian. *Lone Wolves: The New Terrorism of Right-Wing Single Actors*. Cham: Springer, 2020. ISBN 9783030361525.

48 GALEOTTI, Mark. *Russian political war: moving beyond the hybrid*. London: Routledge, 2019. ISBN 978-113-8335-950.

7 COUNTERING "LEADERLESS RESISTANCE"

"Leaderless resistance" is a flexible and adaptable phenomenon with a broad spectrum of varieties. Its countering poses a huge challenge due to its free and spontaneous character, including a propagandist threatening message which is connected with the spread of information about each act which can be affiliated with this concept[49]. Basic recommendation to counter "leaderless resistance" is to react to prevent it, after the outbreak to react to its fluid substance and to stop its spread and transformation into a strong efficient insurgent movement.

Countering "leaderless resistance" is a task for comprehensive security architecture which is able to react to the above mentioned varieties and development phases (from propaganda across lone-wolf and small-cell terrorism and diffused mass acts of subversion to transformation into more sophisticated insurgency). It requires innovative and autonomous approaches of individual institutions, however, also strong leadership. Leaderless counterterrorism and leaderless counterinsurgency are not welcomed, even if the enemy acts leaderlessly.

Regarding the specific features of "leaderless resistance", the following measures can be recommended:

1) Use of efficient counter-narratives. Success of "leaderless resistance" is based on commonly shared ideas. Their elimination is a task for the whole responsible political representation and society. Specific counter-narratives can be prepared by expert teams affiliated with governmental bodies;

2) Identification of lone-wolfs and small cells. Recently the crucial task is to improve methods to identify possible initiating persons and "foot soldiers" of leaderless resistance. As Florian Hartleb stated about perpetrators: "whenever a person states they are a "military detachment" in a combative mentality, openly expresses sympathy for using weapons, identifies himself with former actors of murderous deeds and murderous violent deeds as well as appears to be inspired by a missionary-like compulsion"[50].

3) Efficient intelligence work in resistance milieu, which requires coordination of activities platforms for sharing information between criminal intelligence, foreign intelligence and military intelligence (due to the above mentioned overlaps with the military scene). Growing use of the internet and possible use of cyber-attacks by "leaderless resistance" should lead to involvement of institutions from cyber-security branch;

4) Law enforcement and justice treatment of "leaderless resistance" as a strategic concept. Juridical bodies should take into account that allegedly isolated acts are in fact part of a broader strategic concept;

---

49 Paul Joosse even describes „leaderless resistance" as „a rhetorical construct, a meaning-conferring "ideology of effervescence" that lifts the spirits of both movement progenitors who advocate the strategy as well as incipient lone wolves who consider responding to their exhortations." JOOSSE, Paul. Leaderless Resistance and the Loneliness of Lone Wolves: Exploring the Rhetorical Dynamics of Lone Actor Violence. *Terrorism and Political Violence*. 2017, 29(1), 52-78. DOI: 10.1080/09546553.2014.987866. ISSN 0954-6553.

50 HARTLEB, Florian 2020.

5) Appropriate military reactions in case of a serious outbreak of "leaderless resistance". In case of mass subversive activities of "phantom cells" with military equipment (including attacks at military deposits) to use efficient swarming tactics aimed to elimination of the most active cells and use of the concept of "area of responsibility" for control of insurgent territories[51];

6) Paradoxically, the diffused and unorganized character of the resistance can be supported by counter-insurgent forces in the case when the threat of its transformation into a well-organized movement is growing. However, such approach must be temporarily limited and it should serve only to re-structuring and improvement of counter-insurgency.

CONCLUSION

If we examine the weak and strong points of the concept (which is sometimes called tactics and sometimes it is called strategy), we can see the mobilization potential as an "output-advantage." Many individuals can intensify their personal engagement in insurgent activities if they have the feeling that they are part of the mass "comprehensive strategy". An advantage for insurgents is also the fact that the holders of power are not fully able to identify all small cells and individuals. They can surprise with varieties of attacks. A weak government or occupation power can be pushed to capitulate only due to this mass scope of attacks. On the other side, the transition into efficient "war machine" is the biggest weakness in the case that the enemy is able to withstand uncoordinated attacks and step by step eliminate its insurgent enemies who are not able to organize a well organized and weaponized underground army for a "real battle". In future insurgencies the capability to maintain the function of the internet and electronic communication as such or to destroy modern communication technologies will be very important (and in such case to find a model for coordination of resistant activities without a leader).

"Leaderless resistance" is a vital subversive concept, despite the fact that its foundations were formulated in the early 1950 s. Its original character as a tactics, which should be supported by US intelligence, was later transformed into broader strategic concepts used by extremists (including a part of the Czech extremist scene). The rise of new interest into "leaderless resistance" is caused due to a wave of lone-wolf terrorism in last years and topically also due to adaption of some extremists to the Corona-crisis. It can be misused also by drivers of various hybrid campaigns and within the context of political warfare. In the new situation "leaderless resistance" can be more dangerous than before. It requires also deep knowledge of the concept and efficient planning of counter-strategies in civilian, law-enforcement, intelligence and military branches.

51 FREUDENBERG, Dirk. *Theorie des Irregulären: Partisanen, Guerillas und Terroristen im modernen Kleinkrieg*. Wiesbaden: VS-Verlag für Sozialwissenschaften, 2008. ISBN 978-3531157375.

This paper was written under the research project OPTIZ "Optimization of Intelligence Activities and Intelligence Institutions in the Changing Environment" (OPTIZ9070204510), funded by the Ministry of Defence of the Czech Republic ("Development of the Armed Forces of the Czech Republic" defence research programme).

Author: ***prof. Miroslav Mareš, PhD.,*** *born in 1974. He is the guarantor of security and strategic studies at the Department of Political Science of the Faculty of Social Studies of Masaryk University in Brno. He focuses on the research of extremism and terrorism in the Central Europe. He is a member of the European Expert Network on Terrorism Issues. He has worked with the OSCE and participated in the counter-extremism and the counter-terrorism activities of the European Union. He is an author or co-author of more than two hundred publications (among other with Astrid Bötticher they wrote the book Theorien, Extremism – Konzepte, Restoring, issued in 2012, in Munich).*

How to cite: MAREŠ Miroslav. Leaderless resistance: Development, Countering and Research of Insurgent Concept. *Vojenské rozhledy*. 2020, 29 (3), 041-056. ISSN 1210-3292 (print), 2336-2995 (online). Available at: www.vojenskerozhledy.cz

 DOI: 10.3849/2336-2995.29.2020.03.057-071

Recenzovaný článek

Je Turecko připraveno na válku se Sýrií?

Is Turkey Ready for a War with Syria?

Vladimír Bízik, Zdeněk Kříž

Abstrakt: Tento článek odpovídá na otázku, zda je Turecko připraveno vstoupit do otevřeného vojenského konfliktu se Sýrií Bašára al-Asada. Text vychází z adaptace Clausewitzova předpokladu, že pro vítězné vedení války musí stát disponovat třemi zdroji: vlastními bojovými silami, podporou obyvatelstva a podporou spojenců. Turecko vykazuje slabiny ve vojenské doméně, zejména v oblasti letectva a protivzdušné obrany a není jisté, že by bylo schopné ovládnout vzdušný prostor v konfliktní oblasti. Turecké obyvatelstvo si vleklý zahraniční konflikt dlouhodobě nepřeje. Země je navzdory mnoha neshodám pevně zakotvena v NATO a její strategické zájmy se neliší od zájmů svých strategických spojenců. Turecko si rovněž nemůže dovolit dostat se do přímého konfliktu s Ruskem. Text uzavírá, že Turecko si vstup do otevřeného ozbrojeného konfliktu nemůže dovolit politicky ani vojensky.

Abstract: This article examines whether Turkey is ready for a full-scale military conflict with Bashar Al-Assad's Syria. It draws from an adaptation of Clausewitz's concept of three resources that a state must possess to be able to win a war: the fighting forces proper, popular support, and its allies. Turkey is at a significant disadvantage when it comes to its air force and air defense capabilities. Should a major confrontation erupt, Turkey would not be guaranteed to be able to control the relevant air space. Turkish citizens do not favor seeing their country in a foreign quagmire. Despite myriad differences, Turkey it is still deeply embedded within NATO, and its strategic interests do not differ from those of its strategic allies. Turkey also cannot afford to risk an open military conflict with Russia. The article concludes that Turkey is politically and militarily not capable of fighting a full-scale war in Syria.

Klíčová slova: Sýrie; Rusko; Erdoğan; Putin; Asad; Clausewitz; letectvo; podpora obyvatelstva.

Key words: Syria; Russia; Erdoğan; Putin; Assad; Clausewitz; Air Force, Public Support.

ÚVOD A KONCEPTUÁLNÍ RÁMEC

Připravenost Turecka na vedení války je v kontextu eskalace konfliktu v Sýrii na přelomu února a března 2020 nesporně relevantním tématem. Koncept připravenosti země na vedení války je implicitně obsažen v klíčových dílech vojenských teoretiků. Obsahuje jej již nadčasové dílo Carla von Clausewitze *O válce*, kde autor zmiňuje síly, kterými musí stát disponovat, aby mohl vstoupit do války a vyhrát ji. Clausewitz uvádí: „Tyto síly jsou; *vlastní, bezprostřední bojové síly*, *země* se svým povrchem a obyvatelstvem, a *spojenci*."[1] Důležitý je poznatek, že válku nevede jen stát, ale celá společnost jako taková.[2] Jak si všímá Colin Gray, v moderním kontextu demokratických států je naprosto zásadní role veřejného mínění.[3] Je zejména důležité, aby obyvatelstvo země považovalo předmět sporu, o který se má válka vést, za niterně svůj. Jak rozpoznal již Sun-c', země je připravena na válku, pokud jsou vojáci státu ochotni v ní bojovat a umírat a obyvatelstvo přinášet oběti.[4]

Po nastínění kontextu motivace jednotlivých aktérů syrské krize ve druhé kapitole bude pozornost věnována rozboru turecké armády (kapitola 3). Postojům turecké společnosti ke krizi v Sýrii se bude věnovat kapitola 4. Studium Clausewitze a vojenské historie ukazuje, že zajistit si spolehlivé spojence pro případ války, kteří poskytnou dodatečné vojenské kapacity, ekonomickou pomoc nebo alespoň podporu politickou, je klíčovým faktorem v připravenosti země na válku. Proto je třeba věnovat pozornost vztahům Turecka se svými spojenci a partnery, což činí kapitola 5.

Článek dochází k závěru, že eskalace ozbrojeného konfliktu s Asadovou Sýrií ze strany Erdoğanova Turecka by byla iracionální. Žádnou ze tří sil, které Clausewitz považuje za klíčové pro vítěznou válku Turecko v dostatečné míře nedisponuje. Turecké ozbrojené síly, zejména letectvo, nejsou ve stavu, který by přinesl rychlé vítězství, pokud by syrské vládní síly podpořilo Rusko. Obyvatelstvo Turecka není přímému vojenskému zapojení také jednoznačně nakloněno. V neposlední řadě, Turecko nemá podporu spojenců pro své angažmá v konfliktu. Pokud by se Turecko v Sýrii dostalo do otevřené vleklé války, byl by to důsledek iracionálního rozhodnutí a takováto situace by mohla ohrozit mocenské pozice Erdoğana a oslabit Turecko jako celek.

1 CLAUSEWITZ, Carl von. *O válce.* Překladatel Zbyněk SEKAL. Praha: Academia, 2008, s. 28.

2 GRAY, Colin S. *Fighting Talk: Forty Maxims on War, Peace, and Strategy Paperback*. Westport, CT: Praeger Security International, 2007, s. 24–27.

3 GRAY, Colin S. *War, Peace, and International Relations: An Introduction to Strategic History*. London: Routledge, 2008, s. 8.

4 HANDEL, Michael I. *Masters of War: Classical Strategic Thought* [online]. Hoboken: Taylor and Francis, 2012, s. 90 [cit. 09. 07. 2020]. Dostupné z: http://public.eblib.com/choice/publicfullrecord.aspx?p=254399

1 KONTEXT KONFLIKTU A MOTIVACE AKTÉRŮ

Motivace Turecka pro angažmá v konfliktu je mnohovrstvá. Bezprostřední příčinou tureckého jednání jsou bezpečnostní důsledky konfliktu v podobě zhruba 3,7 miliónu uprchlíků, kteří našli útočiště v Turecku. Náklady na jejich podporu se odhadují na zhruba 20 mld. euro.[5] Nedávná syrská ofenziva v Idlibu (2019/2020) vytvořila dalších 700 000-900 000 uprchlíků, o kterých lze důvodně přepokládat, že budou hledat útočiště v Turecku.[6] Pro syrský režim jde jednu z posledních významných oblastí, které nezískal zpět pod vlastní kontrolu. Druhu vrstvou je nezájem Turecka na tom, aby se v Sýrii vytvořily podmínky pro vznik jakéhokoli útvaru, který by mohl posloužit jako zárodek budoucího kurdského státu. A za třetí, v hloubi motivace režimu Recepa Tayyipa Erdoğana může hrát roli i touha získat zpět maximum z «dědictví» Osmanské říše, kam Sýrie dlouhá staletí patřila.[7] Synergickým efektem těchto motivací je fakt, že Turecko není v současnosti nijak zainteresováno na přežití Asadova režimu.[8]

Ruská motivace spočívá v dlouhodobé podpoře svého spojence poskytujícího vojenské základny v regionu, jež sahá daleko do období studené války. Podpora Asada umožňuje vytvářet Vladimírovi Putinovi na domácí scéně před ruskou veřejností dojem, že Rusko je nadále globální velmoc se schopností projektovat moc. Dále je pro Rusko rozhodně výhodnější vést boj s radikálními islámskými skupinami na syrské než na ruské půdě. V neposlední řadě slouží Sýrie jako testovací polygon pro ruské zbraňové systémy.

Pokud chceme porozumět kontextu eskalace na přelomu února a března 2020, je třeba uvést, Turecko varovalo Sýrii před snahou získat zpět pod svou kontrolu Idlib. V průběhu syrské ofenzívy v oblasti se Turky podporovaní povstalci pokoušeli sestřelit ruské a syrské bojové letouny. Pravděpodobně jako odvetu zaútočila syrská nebo ruská (případně obojí) bojová letadla na velitelské stanoviště v Idlibu a turecký konvoj.[9] Po smrti 34 tureckých vojáků 27. února 2020, kdy hrozilo, že se syrskému režimu podaří ovládnout provincii Idlib, zahájilo Turecko na začátku března 2020 v regionu energický protiútok. Ten vzal syrským silám a Rusku naději, že provincii v dohledné době ovládnou, pokud bude Turecko ochotné bojovat. Proto proběhlo 5. března 2020 jednání v Moskvě mezi

5 SÖNMEZ, Mustafa. Mystery surrounds Turkey's $ 40 billion refugee bill. In: *Al-Monitor* [online]. 2. 11. 2019 [cit. 16. 04. 2020]. Dostupné z: https://www.al-monitor.com/pulse/originals/2019/10/turkey-syria-40-billion-refugee-bill-calls-for-explanation.html

6 GALL, Carlotta. Turkey Launches Deadly Airstrikes Against Syrian Forces. In: *The New York Times* [online]. 3. 2. 2020 [cit. 16. 04. 2020]. Dostupné z: https://www.nytimes.com/2020/02/03/world/middleeast/turkey-syria-idlib.html

7 DANFORTH, Nick. Turkey's New Maps Are Reclaiming the Ottoman Empire. In: *Foreign Policy* [online]. 23. 10. 2016 [cit. 16. 04. 2020]. Dostupné z: https://foreignpolicy.com/2016/10/23/turkeys-religious-nationalists-want-ottoman-borders-iraq-erdogan/

8 HUGHES, Lindsay. *Russia and Turkey in Syria: The Erosion of the Friendship? (Strategic Analysis Paper)*. Future Directions International, 2020.

9 TISDALL, Simon. Erdoğan is reaping what he sowed: Turkey is on the brink of disaster in Syria. In: *The Guardian* [online]. 2. 3. 2020 [cit. 16. 04. 2020]. Dostupné z: https://www.theguardian.com/commentisfree/2020/mar/02/erdogan-turkey-syria-assad

Putinem a Erdoğanem, na jehož základě bylo v provincii Idlib uzavřeno další příměří. Protože jak Rusko, tak Turecko dlouhodobě chápou koncept příměří především jako období operační přestávky mezi bojovou činností, není vyloučeno, že dříve či později bude nějakou stranou konfliktu (případně oběma) příměří porušeno a válka se znovu rozhoří v plné intenzitě. Ostatně obyvatelé Idlibu dle dostupných dat příliš nevěří tomu, že by příměří opravdu vydrželo.[10]

2 STAV TURECKÉ ARMÁDY

Turecká armáda dlouho hrála ve společnosti mnohem významnější roli, než je v demokracii obvyklé, neboť byla podle ústavy garantem sekularismu v Turecku a strážcem prozápadní orientace země. V zemi provedla čtyři vojenské převraty (1960, 1971, 1980 a 1997), které se vymezovaly proti nárůstu moci politického islámu.[11] Proto také Erdoğan od svého příchodu k moci usiloval o omezení jejího vlivu ve společnosti, což se mu zdařilo již před pokusem o vojenský převrat roku 2016. Omezeny byly pravomoci Národní bezpečnostní rady a jak ústava, tak dílčí zákony byly revidovány takovým způsobem, aby nebylo možné dovodit aktivní roli armády ve věcech uspořádání státu.[12] V rámci série soudních procesů s údajnou tajnou skupinou „Ergenekon“ byly části vedení armády zpacifikovány[13] a poníženy.[14] V roce 2013 bylo odsouzeno k dlouhým až doživotním trestům 275 důstojníků včetně bývalého náčelníka generálního štábu İlkera Başbuğa. To vše se událo za nebývalé podpory obyvatelstva, které to mohlo vnímat jako dlouho očekávanou demokratizaci, demilitarizaci a normalizaci civilně-vojenských vztahů v zemi.[15]

Neúspěšný vojenský převrat potom poskytl skvělou příležitost dokonat toto dílo. Bezprostřední reakcí Erdoğana byla rozsáhlá čistka v armádě, což není v takové situaci nijak neobvyklé. Vazba byla uvalena na 7 500 vojáků, včetně 118 generálů a admirálů.[16] Z ozbrojených sil bylo nakonec vyhozeno 40 % všech admirálů a generálů[17] a z politických

10 PITEL, Laura, Henry FOY a Chloe CORNISH. Idlib residents put little faith in Russian-Turkish peace deal. In: *Financial Times* [online]. 8. 3. 2020 [cit. 16. 04. 2020]. Dostupné z: https://www.ft.com/content/83ed1fd2-6131-11ea-b3f3-fe4680ea68b5

11 EDROOS, Faisal a Ahmad EL AMRAOUI. Why Turkey's military is not what it used to be. In: *Al Jazeera* [online]. 5. 6. 2018 [cit. 16. 04. 2020]. Dostupné z: https://www.aljazeera.com/indepth/features/turkey-military-180527105359421.html

12 ŞAHIN, Hakan. Turkey's Play with Its Military. *Mediterranean Quarterly*. 2018, roč. 29, č. 4, s. 33–37.

13 DANĚK, Pavel a Zdeněk KŘÍŽ. Politický vliv turecké armády. *Politologická revue* [edo]. 2011, roč. 17, č. 2, s. 48.

14 SINGH, Chaitram a John HICKMAN. Soldiers as Saviors of the State: The Cases of Turkey and Pakistan Contrasted. *Journal of Third World Studies*. 2013, roč. 30, č. 1.

15 ŞAHIN, Hakan. *Turkey's Play with Its Military*, s. 36.

16 KIRBY, Paul. Who's the target of Turkey's purge? In: *BBC News* [online]. 20. 7. 2016 [cit. 16. 04. 2020]. Dostupné z: https://www.bbc.com/news/world-europe-36835340

17 EDROOS, Faisal a Ahmad EL AMRAOUI. *Why Turkey's military is not what it used to be*.

důvodů propuštěno více než 22 000 důstojníků, vojáků a kadetů.[18] Dle tureckých údajů z ledna 2019 mělo být v souvislosti s vojenským převratem k doživotí odsouzeno 58 generálů a 629 vyšších důstojníků.[19] Všechna tato data potvrzují, že turecké zbrojené síly prošly zásadní čistkou, zejména na úrovni generálů, admirálů a vyšších důstojníků.

Důležitou systémovou změnou je podřízení generálního štábu ministerstvu obrany, což umožňuje politické reprezentaci přímo kontrolovat důstojnický sbor.[20] V armádě výrazně oslabila vrstva na Západě vzdělaných a prozápadních důstojníků a posílila vrstva konzervativních nacionalistů, kteří mnohem kritičtěji než jejich předchůdci nahlížejí na prozápadní směřování země. Výběrová kritéria přijímacích řízení do vojenských akademií upřednostňují kandidáty ze sociálních vrstev, které jsou voličskými baštami strany AKP.[21] Z vojenského úhlu pohledu je důležité, že v důsledku čistek se do velení na vyšších funkcích dostali mladší a služebně méně zkušení důstojníci.[22]

V roce 2019 prodělala turecká armáda další zásadní transformaci, jejíž součástí byla redukce povinné vojenské služby z 12 měsíců na 6 a posílení jejího dobrovolného jádra. Cílem jsou menší, avšak kvalitně vycvičené a vysoce mobilní ozbrojené síly schopné nasazení v širokém spektru operací se schopností projekce moci mimo teritorium Turecka.[23] Turecká armáda má rozsáhlé zkušenosti s prováděním protipovstaleckých operací, zejména proti PKK, ve kterých byly v minulosti používáni i vojáci základní prezenční služby. Přesto již několik let jsou aktivní vojenské operace v Sýrii a Iráku prováděny výlučně vojenskými profesionály.[24]

Dostupná data však nenasvědčují, že by čistky po pokusu o převrat roku 2016 významně omezily bojové možnosti tureckých pozemních sil. Lars Haugom argumentuje tím, že čistky zasáhly především vyšší velení tureckých vojenských složek. Výkony tureckých pozemních sil v operacích po roku 2016 nejsou dle jeho analýzy jednoznačnou katastrofou.[25]

Schopnosti tureckých sil demonstroval i průběh eskalace v Idlibu (operace *Jarní štít*) na přelomu února a března 2020. Masivní a úspěšné použití speciálních sil, dělostřelectva a desítek dronů domácí výroby zastihlo syrské síly a jejich ruské „poradce a kontraktory“ nepřipravené. Turecké vojenské akce způsobily protivníkovi značně škody. Turecké ministerstvo obrany si nárokuje zničení dvou syrských bojových letadel, osmi vrtulníků,

---

18 *Thematic Country of Origin Information Report Turkey: Military service* [online]. The Hague: Ministerie van Buitenlandse Zaken, 2019, s. 5. Dostupné z: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/ambtsberichten/2019/07/11/thematisch-ambtsbericht-dienstplicht-turkije-juli-2019/EN+Tab+Turkije+dienstplicht+4+juli+2019+zonder+vertrouwelijke+bronnen.pdf

19 *Ibid.*

20 HAUGOM, Lars. An Uncertain Future for the Turkish Armed Forces. In: *The Turkey Analyst* [online]. 26. 9. 2017 [cit. 16. 04. 2020]. Dostupné z: http://turkeyanalyst.org/publications/turkey-analyst-articles/item/588-an-uncertain-future-for-the-turkish-armed-forces.html

21 ŞAHIN, Hakan. *Turkey's Play with Its Military*, s. 46.

22 HAUGOM, Lars. *An Uncertain Future for the Turkish Armed Forces*.

23 Turkey. In: *CIA World Factbook* [online] [cit. 16. 04. 2020]. Dostupné z: https://www.cia.gov/library/publications/the-world-factbook/geos/tu.html

24 *Thematic Country of Origin Information Report Turkey: Military service*, s. 13.

25 HAUGOM, Lars. *An Uncertain Future for the Turkish Armed Forces*.

135 tanků, 77 obrněných bojových vozidel a 2 500 vojáků.[26] Jakkoli není možné tato čísla ověřit z nezávislých zdrojů, Rusko by s Tureckem nezasedlo za jednací stůl v Moskvě, kdyby se domnívalo, že krize v Idlibu *má pro něj snadné vojenské řešení. V neposlední řadě je zřejmé, že syrských cílů v* Idlibu dosud dosaženo nebylo. Proto je vysoce pravděpodobné, že turecké údaje budou v mezích všeobecné „mlhy nad bojištěm" řádově správné a schopnosti tureckých pozemních sil by se neměly podceňovat. Pokud Rusko koncem února 2020 sázelo na to, že Turecko blafuje a syrsko-ruské síly nenapadne, velmi se přepočítalo.[27]

Zatímco operační schopnosti pozemních sil a poměr sil v oblasti nemusí Turecku bránit eskalaci v Idlibu, zásadním problémem je stav turecké protivzdušné obrany. Protiletadlové raketové komplety Turecka, přestože prochází permanentní modernizací, nejsou nejmodernější a turecké autority si toho jsou velmi dobře vědomy. Spojené státy nebyly ochotné Turecku prodat systémy Patriot, a proto Erdoğan hledal jiné možnosti. Mezi lety 2013–2015 byly neúspěšné snahy obstarat si obdobné systémy v Číně.[28]

Výše uvedený problém je o to akutnější, že v nedobrém stavu je i turecké letectvo, které bylo čistkami zasaženo daleko nejvíce. Lars Haugom v roce 2017 uvádí, že v důsledku čistek klesl poměr pilotů k bojovým letadlům na 0,7, což je hluboce pod číslem 1,5, které je považováno za nezbytné minimum.[29] To je velmi alarmující situace, protože turecká protivzdušná obrana byla vždy založena primárně na silném stíhacím letectvu, jak je v NATO obvyklé a protiletadlové raketové systémy země-vzduch sloužily spíše jako jeho doplněk. Pokud byl v roce 2017 výše uvedený poměr 0,7, lze očekávat, že začátkem zlepšování tohoto stavu by mohl být nejdříve rok 2020, s dosažením přijatelného stavu někdy po roce 2022. Letošní vydání *The Military Balance* londýnské IISS však uzavírá, že nedostatek zkušeného personálu pořád negativně ovlivňuje operační efektivitu a úroveň výcviku letectva.[30]

S nedobrým stavem tureckého letectva úzce souvisí až zoufalá snaha Turecka rychle posílit svoji PVO protiletadlovými raketovými systémy země-vzduch dalekého dosahu. Řešením mají být dodávky ruských S-400 do Turecka, který je považován za velice schopný A2/AD systém.[31] Politické náklady tohoto obchodu budou diskutovány níže. Vojenské zisky jsou ale zatím nulové. Kontrakt byl podepsán v prosinci 2017, dodávky komponentů

26 AKAR, Hulusi. Bakan Akar: Bahar Kalkanı Harekâtı Planlandığı Şekilde Başarıyla Devam Ediyor. In: *Türkiye Cumhuriyeti Millî Savunma Bakanlığı* [online]. 2. 3. 2020 [cit. 16. 04. 2020]. Dostupné z: https://www.msb.gov.tr/SlaytHaber/232020-33761

27 SPICER, Jonathan a Khalil ASHAWI. President Erdogan's options narrow as Russia presses Syrian crisis to Turkey's doorstep. In: *Reuters* [online]. 27. 2. 2020 [cit. 16. 04. 2020]. Dostupné z: https://www.reuters.com/article/us-syria-security-crisis-erdogan-analysi-idUSKCN20L2I0

28 KARADENIZ, Tulay a Michael MARTINA. Turkey confirms cancellation of $3.4 billion missile defence project awarded to China. In: *Reuters* [online]. 18. 11. 2015 [cit. 16. 04. 2020]. Dostupné z: https://www.reuters.com/article/us-turkey-china-missile-idUSKCN0T61OV20151118

29 HAUGOM, Lars. *An Uncertain Future for the Turkish Armed Forces*.

30 THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES (IISS). *The Military Balance 2020*. London: Routledge, 2020, s. 153.

31 KASAPOĞLU, Can. *Turkey's S-400 Dilemma*. Istanbul: The Centre for Economics and Foreign Policy Studies (EDAM), 2017, s. 1–3.

začaly v létě 2019. To ale neznamená, že v dohledné době bude systém uveden do operační způsobilosti.[32] Nejde pouze o fyzické dodání všech klíčových komponentů systému, což je podmínka nutná, avšak nikoli dostatečná. Stejně důležité je zajistit výcvik obsluh a integraci tohoto pro Turecko nového zbraňového systému do turecké protivzdušné obrany, což nebude jednoduché. I pokud by Rusko skutečně dodalo v první půlce roku 2020 včas všechny klíčové komponenty, je téměř jisté, že S-400 nebude ještě nejméně několik měsíců bojeschopný. Vzhledem k odlišným strategickým zájmům obou států v Sýrii není možné ani vyloučit, že Rusko pozdrží dodání klíčových komponentů S-400, výcvik obsluh nebo obojí a systém komplet S-400 nebude v dohledné době operačně nasaditelný.

Celkově dostupná data ukazují, že hlavní slabinou současné turecké armády je jednoznačně protivzdušná obrana. Pokud by mělo dojít ke konfrontaci velkého rozsahu za účasti regulérních tureckých sil se Syřany a jejich *proxies* podporovanými Ruskem v provincii Idlib, případně v celé severní Sýrii, není vůbec jisté, že by Turecko bylo schopné ovládnout vzdušný prostor. Za takové situace by ani převaha tureckých pozemních sil nemusela stačit k udržení nárazníkového pásma Turecka v oblasti. Je zde také varianta kalkulující s vyřazením ruských leteckých kapacit překvapivým úderem na ruská a syrská letiště v Sýrii ať již pomocí speciálních sil a dronů nebo tradičnějšími metodami. I při nejistém úspěchu by tato možnost mohla vést k eskalaci konfliktu s Ruskem, což není v tureckém zájmu.

3 PODPORA OBYVATELSTVA PRO TURECKÉ VOJENSKÉ ANGAŽMÁ V SÝRII

Nálada turecké veřejnosti vůči uprchlíkům ze Sýrie se v minulé dekádě radikálně proměnila. Počáteční vlna jisté podpory a solidarity s trpícími je dle dostupných dat pryč. Přítomnost uprchlíků zesílila sociální problémy v Turecku, které existují bez ohledu na vývoj konfliktu v Sýrii. Ty jsou dále posilovány ekonomickou krizí, do které se Turecko začalo propadat před začátkem globální pandemie na počátku roku 2020. Tento vývoj reflektovaly již místní volby v roce 2019, ve kterých byla použita karta negativních důsledků uprchlické vlny ze Sýrie pro tureckou společnost.[33] V únoru 2020 se 70,5 % Turků domnívalo, že syrští uprchlíci poškozují tureckou ekonomiku, 76,6 %, že by neměli získat

32 GÜMRÜKÇÜ, Tuvan a Can SEZER. Turkey says delivery of second Russian S-400 batch may be delayed - Reuters. In: *Reuters* [online]. 4. 11. 2019 [cit. 17. 04. 2020]. Dostupné z: https://www.reuters.com/article/us-russia-turkey-defense/turkey-says-delivery-of-second-russian-s-400-batch-may-be-delayed-idUSKBN1XE0U1

33 YINANÇ, Barçın. The outcome of local elections might unleash anti-Syrian rhetoric. In: *Hürriyet Daily News* [online]. 2. 7. 2019 [cit. 16. 04. 2020]. Dostupné z: http://www.hurriyetdailynews.com/opinion/barcin-yinanc/the-outcome-of-local-elections-might-unleash-anti-syrian-rhetoric-144610; KINIKLIOĞLU, Suat. Syrian refugees in Turkey: changing attitudes and fortunes. *Stiftung Wissenschaft und Politik* [online]. German Institute for International and Security Affairs, 2020, č. SWP Comment 2020/C 05 [cit. 16. 04. 2020]. Dostupné z: https://www.swp-berlin.org/10.18449/2020C05/

turecké občanství a 60 % dotázaných očekává, že uprchlíci se po válce vrátí domů.[34] Dostupná data ale nenasvědčují tomu, že by turecká veřejnost vítala vojenské akce, které by byly komunikovány jako snaha zabránit vzniku další syrské uprchlické vlny do Turecka.

Před zahájením tureckých bojových operací proti syrským silám a jejich ruským „poradcům" a kontraktorům v Idlibu a okolí pouze 30,7 % procent Turků hodnotilo tureckou vojenskou přítomnost v oblasti jako nutnost, 48,8 % s touto tezí nesouhlasí a 20,5 % na to nemá názor. Data k tomuto průzkumu byla sbírána mezi 15.–21. únorem 2020. Stejný průzkum také uvádí, že se způsobem, jakým Erdoğan vykonává mandát, souhlasí 41,1% obyvatel, zatímco nesouhlasí 51,17 %.[35] Jedním z možných vysvětlení může být, že 82 % Turků se nedomnívá, že by měli se Syřany příliš mnoho společných kulturních charakteristik.[36]

Po smrti 34 tureckých vojáků po útoku rusko-syrských jednotek v severozápadní Sýrii se veřejné mínění poněkud změnilo. Z průzkumu provedeného 29. února a 1. března vyplývá, že přes 65 % Turků si přeje, aby operace v Sýrii pokračovaly, jelikož nestabilita přicházející ze Sýrie je existenční hrozbou pro Turecko (63 %) a vytvoření kurdského „teroristického státu" by ohrozilo integritu Turecké republiky (60 %).[37] Strach z kurdského ohrožení turecké národní jednoty je stálicí ležící v samotném srdci tureckého národního povědomí, a již nás nemůže překvapit.[38] Přibližně dvojnásobný nárůst v podpoře pro operaci v Sýrii je sice dramatický, ale pochopitelný: po smrti vojáků je přirozenou reakcí společnosti „semknout se kolem vlajky". Až se trauma ze ztráty na životech vytratí z kolektivního povědomí, lze očekávat, že turecké obyvatelstvo začnou trápit opět jiné problémy a podpora pro vojenský avanturismus záhy klesne na přibližně původní čísla. To lze vidět již na dalším průzkumu provedeném v dubnu 2020, v němž 28,7 % respondentů uvádí syrskou občanskou válku jako naléhavý problém turecké zahraniční politiky. Je to nárůst oproti 26 % v roce 2019, nikoli ale tak výrazný ve světle této podstatné eskalace.[39]

Z toho lze vyvodit, že válka v Sýrii je „tureckou věcí" pouze to té míry, do jaké se bezprostředně svými důsledky týká Turecka. Jakoukoli vyšší motivaci pro dlouhodobé angažmá v Sýrii turecká společnost postrádá. Taková konstelace ale není příliš příznivá pro to, aby Erdoğan zvyšoval svoje sázky v tomto konfliktu.

---

34 Türkiye'nin Nabzı - Ayın 5 Rakamı / Şubat 2020. In: *MetroPoll Stratejik ve Sosyal Araştırmalar* [online]. 2. 2020 [cit. 16. 04. 2020]. Dostupné z: http://www.metropoll.com.tr/arastirmalar/sosyal-arastirma-12/1839

35 Only 31 percent of Turks approve of Turkish military's presence in Idlib. In: *Duvar English* [online]. 5. 3. 2020 [cit. 16. 04. 2020]. Dostupné z: https://www.duvarenglish.com/politics/2020/03/05/31-percent-of-turks-approve-of-turkish-militarys-presence-in-idlib/

36 KINIKLIOĞLU, Suat. *Syrian refugees in Turkey*.

37 A & G ARAŞTIRMA. Adil Gür İdlib anketiyle bomba gibi düştü! Şehit verilmesinden kim sorumlu. In: *İnternet Haber* [online]. 2. 3. 2020 [cit. 16. 04. 2020]. Dostupné z: https://www.internethaber.com/adil-gur-idlib-anketiyle-bomba-gibi-dustu-sehit-verilmesinden-kim-sorumlu-foto-galerisi-2085738.htm

38 POULTON, Hugh. *Top Hat, Grey Wolf, and Crescent: Turkish Nationalism and the Turkish Republic*. Washington Square, N.Y.: New York University Press, 1997, s. 246–251.

39 AYDIN, Mustafa. Türk Dış Politikası Kamuoyu Algıları Araştırması, 17 Haziran 2020. In: *Kadir Has Üniversitesi* [online]. 17. 6. 2020 [cit. 30. 06. 2020]. Dostupné z: https://www.khas.edu.tr/sites/khas.edu.tr/files/inline-files/DPA2020_BASIN%5B1%5D.pdf

4 VZTAHY TURECKA SE SPOJENCI

Na první pohled by se mohlo zdát, že vzhledem k tureckému členství v NATO od roku 1952 se může Turecko opřít o dostatečnou spojeneckou podporu. Při bližším pohledu ale zjistíme, že členství v NATO příliš nepřispívá turecké schopnosti k vojenskému řešení krize v Idlibu. Příčiny jsou v zásadě dvě. První je charakter NATO jako organizace kolektivní obrany, která nijak nepokrývá případný útok na turecké síly v severní Sýrii. Jedná se o konstantu, která je tvůrcům turecké zahraniční politiky známa. Druhou příčinou malé relevance NATO pro posazení tureckých zájmů v severní Sýrii je ale aktivní Erdoğanova politika posledních let, která velmi intenzivně a velmi úspěšně pracuje na destrukci bezpečnostních vztahů s tureckými spojenci, zejména však s USA.[40]

Percepce Turecka jako spolehlivého člena NATO se zásadně změnila po reakci Erdoğana na pokus o vojenský puč roku 2016. Západ pokus o vojenský převrat odsoudil. Erdoğanova vnitřní politika se ale mezi členy NATO nesetkala s příliš velkým pochopením, neboť je chápána jako ohrožení demokracie v Turecku.[41] Aktuální vývoj potvrzuje tezi, že Erdoğan otevřeně buduje v Turecku režim osobní moci, který se postupně rozchází s kemalistickým sekulárním dědictvím a prozápadní zahraničně-politickou orientací.[42] V rámci rozsáhlé čistky v turecké společnosti zdůvodněné vojenským pučem bylo propuštěno více než 130 000 zaměstnanců veřejné správy, uvězněno více než 80 000 lidí a činnost muselo ukončit více než 1 500 nevládních organizací.[43] Tím ale výčet sporných témat nekončí.

Turecké rozhodnutí nakoupit ruské systémy S-400 vyvolalo mezi členy NATO rozčarování. Generální tajemník Stoltenberg sice vystoupil velmi vstřícně vůči Turecku a uvedl, že na turecké participaci v integrovaném systému protivzdušné obrany nic nemění, alespoň tedy pokud nebude chtít Turecko do systému zapojit ruský S-400.[44] Jeho pozici ale rozhodně nelze interpretovat jako souhlas s tureckou politikou.

Po zahájení turecké ofenzívy proti kurdským silám v severní Sýrii v říjnu 2019 některé členské státy NATO kritizovaly tureckou kampaň. Evropská unie ji neváhala označit za

---

40 DALAY, Galip a E. Fuat KEYMAN. *Turkish-U.S. Strategic Decoupling Through the Prism of Syria* [online]. 2019 [cit. 16. 04. 2020]. Dostupné z: https://www.brookings.edu/opinions/turkish-u-s-strategic-decoupling-through-the-prism-of-syria/

41 SLOAT, Amanda. *The West's Turkey Conundrum* [online]. Washington, D.C: Brookings - Robert Bosch Foundation, 2018. Dostupné z: https://www.brookings.edu/wp-content/uploads/2018/02/fp_20180212_west_turkey_conundrum.pdf

42 DANFORTH, Nick. *The Outlook for Turkish Democracy: 2023 and Beyond* [online]. Washington, D.C: THe Washington Institute of Near East Policy, 2020. Dostupné z: https://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyNote77-Danforth.pdf

43 Turkey 2018 Human Rights Report. In: *United States Department of State* [online]. 2018. Dostupné z: https://www.state.gov/wp-content/uploads/2019/03/TURKEY-2018-HUMAN-RIGHTS-REPORT.pdf

44 WADHAMS, Nick. NATO Chief Says Turkey Remains Important Ally Despite S-400 Deal. In: *Bloomberg* [online]. 18. 7. 2019 [cit. 16. 04. 2020]. Dostupné z: https://www.bloomberg.com/news/articles/2019-07-18/nato-chief-says-turkey-remains-important-ally-despite-s-400-deal

operaci, která přímo ohrožuje bezpečnost v regionu.[45] Někteří členové NATO v reakci na tento krok uvalili embargo na dovoz zbraní do Turecka. Jde zejména o Itálii, Francii a Německo.[46] Itálie na podzim 2019 stáhla svoje síly z ochrany vzdušného prostoru jižního Turecka a pokračuje pouze nasazení sil Španělska.[47]

Zdrojem vnímání Turecka jako problémového spojence ze stran členů NATO je jeho politika v migrační krizi. V roce 2016 bylo mezi Evropskou unií a Tureckem s velmi významným přispěním německé diplomacie dohodnuto, že Turecko se postará o uprchlíky na svém teritoriu, nebude je pouštět dále do Evropy a výměnou obdrží na pokrytí jich potřeb finanční kompenzaci 6 mld. euro.[48] Tureckou pozici v NATO rozhodně neposílilo, že Erdoğan se rozhodl na pozadí eskalace krize v Sýrii použít téma uprchlíků jako nástroj nátlaku na EU, a tedy i na NATO. Zejména eskalace latentního napětí s Řeckem, jež má historické kořeny a není způsobeno Erdoğanovou politikou, naplňování cílů turecké zahraniční politiky rozhodně nepomáhá. Řecko v NATO může vetovat jakýkoli návrh na poskytnutí pomoci Turecku a také tak činí.[49]

Po eskalaci konfliktu v provincii Idlib požadoval Erdoğan od NATO, Evropské unie a Spojených států konkrétní podporu v podobě vyhlášení bezletové zóny nad oblastí.[50] Takovou podporu ale Turecko nezískalo. Severoatlantická aliance pouze odsoudila útok na turecké

---

45 North East Syria: Council adopts conclusions. In: *European Council / Council of the European Union* [online]. 14. 10. 2019 [cit. 16. 04. 2020]. Dostupné z: http://www.consilium.europa.eu/en/press/press-releases/2019/10/14/council-conclusions-on-north-east-syria/

46 Foreign Affairs Council, 14 October 2019. In: *European Council / Council of the European Union* [online]. 14. 10. 2019 [cit. 16. 04. 2020]. Dostupné z: http://www.consilium.europa.eu/en/meetings/fac/2019/10/14/ "; EMMOTT, Robin. EU Governments Limit Arms Sales to Turkey but Avoid Embargo. *Reuters* [online]. 2019 [cit. 16. 04. 2020]. Dostupné z: https://www.reuters.com/article/us-syria-security-eu-france-idUSKBN1WT0M4

47 BELKIN, Paul. NATO: Key Issues Following the 2019 Leaders' Meeting. In: *Congressional Research Service* [online]. 2019. Dostupné z: https://fas.org/sgp/crs/row/R46066.pdf; Patriots at Incirlik Base can remain for 6 months more in 2020, Spanish defense minister says. In: *Daily Sabah* [online]. 25. 10. 2019 [cit. 16. 04. 2020]. Dostupné z: https://www.dailysabah.com/defense/2019/10/25/patriots-at-incirlik-base-can-remain-for-6-months-more-in-2020-spanish-defense-minister-saysthe Spanish… ","container-title":"Daily Sabah","language":"en","note":"source: www.dailysabah.com\nsection: Business","title":"Patriots at Incirlik Base can remain for 6 months more in 2020, Spanish defense minister says","URL":"https://www.dailysabah.com/defense/2019/10/25/patriots-at-incirlik-base-can-remain-for-6-months-more-in-2020-spanish-defense-minister-says","accessed":{„date-parts":[[„2020",4,16]]},"issued":{„date-parts":[[„2019",10,25]]}}}}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}

48 EU-Turkey statement, 18 March 2016. In: *European Council / Council of the European Union* [online]. 18. 3. 2016 [cit. 16. 04. 2020]. Dostupné z: http://www.consilium.europa.eu/en/press/press-releases/2016/03/18/eu-turkey-statement/; The EU Facility for Refugees in Turkey. In: *European Comission* [online]. 6. 12. 2016 [cit. 16. 04. 2020]. Dostupné z: https://ec.europa.eu/neighbourhood-enlargement/news_corner/migration_en

49 *Idlib: Greece veto of NATO statement* [online]. 2020 [cit. 16. 04. 2020]. Dostupné z: https://europediplomatic.com/2020/02/29/idlib-greece-veto-of-nato-statement/

50 THEUSSEN, Amelie a Dominika KUNERTOVA. Why Turkey can't expect military support from NATO over attacks in Syria. In: *The Conversation* [online]. 6. 2. 2020 [cit. 16. 04. 2020]. Dostupné z: http://theconversation.com/why-turkey-cant-expect-military-support-from-nato-over-attacks-in-syria-132838

síly, vyjádřila plnou solidaritu s Tureckem bez stanovení konkrétních opatření a vyhověla Turecku v případě konzultací dané situace na základě článku 4 Washingtonské smlouvy.[51]

Ačkoli se Erdoğanovo Turecko v mnohém rozchází se svými západními spojenci a NATO, očekávat faktické, natož formální vystoupení Turecka z aliance zůstává i po desetiletích nenaplněnou věštbou. Regionální dynamika a povaha stávajícího tureckého režimu znamenají částečný odklon od shody v krátkodobých zájmech Turecka a zbytku NATO. Na druhé straně, zatím nenastal rozchod ve strategických a dlouhodobých zájmech. To lze pozorovat na příkladu snad největší roztržky mezi Tureckem a jeho aliančními spojenci, na tureckém rozhodnutí o koupi ruských systémů S-400. V květnu 2019 Erdoğan, znám svým nevybíravým slovníkem vůči svým západním partnerům, prohlásil, že nákupem systémů Ankara v žádném případě nehledá „alternativu" ke svému spojenectví se Západem.[52] K aktivaci nakoupených systémů S-400 mělo dojít v dubnu 2020, z důvodu probíhající pandemie však Turecko koncem měsíce oznámilo, že se nasazení odkládá. To sice neznamená úplné upuštění od plánů, přesto to ale může dát Turecku a jeho západním partnerům čas pro urovnaní sporu, zejména se Spojenými státy americkými.[53]

Nesmíme opomenout ani bilaterální turecko-americké vztahy, které se za poslední léta výrazně zhoršily. Z úhlu pohledu Erdoğanova Turecka je problematické, že Spojené státy podpořily svržení protureckých sunitských islamistů v Egyptě a napomohly svrhnout Kaddáfího režim v Libyi, se kterým Turecko udržovalo intenzivní hospodářské styky. Vztahy se Spojenými státy zhoršovalo i obviňování bývalého Erdoğanova souputníka, islamistického klerika Fethullaha Gülena ze zosnování převratu, aniž by Erdoğanův režim byl schopný je podložit hodnověrnými důkazy.[54] Než se dal do pohybu proces stahování ze Sýrie ve druhé polovině Trumpovy administrativy, Spojené státy podporovaly Syrské demokratické síly jako svého strategického spojence v boji proti *Daiš* a v zadržování vlivu

---

51 Press point by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at Turkey's request for Article 4 consultations on the situation in Syria. In: *NATO* [online]. 28. 2. 2020 [cit. 16. 04. 2020]. Dostupné z: http://www.nato.int/cps/en/natohq/opinions_173931.htm"container-title":"NATO","language":"en","note":"source: www.nato.int","title":"Press point by NATO Secretary General Jens Stoltenberg following the North Atlantic Council meeting at Turkey's request for Article 4 consultations on the situation in Syria","URL":"http://www.nato.int/cps/en/natohq/opinions_173931.htm","accessed":{„date-parts":[[„2020",4,16]]},"issued":{„date-parts":[[„2020",2,28]]}}}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}; Statement by the Secretary General after Article 4 consultations. In: *NATO* [online]. 28. 2. 2020 [cit. 16. 04. 2020]. Dostupné z: http://www.nato.int/cps/en/natohq/opinions_173939.htmfollowing a request by Turkey to hold consultations under Article 4 of NATO's founding Washington Treaty on the situation in Syria.","container-title":"NATO","language":"en","note":"source: www.nato.int","title":"Statement by the Secretary General after Article 4 consultations","URL":"http://www.nato.int/cps/en/natohq/opinions_173939.htm","accessed":{„date-parts":[[„2020",4,16]]},"issued":{„date-parts":[[„2020",2,28]]}}}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}

52 BALCI, Ali. A Three-level Analysis of Turkey's Crisis with the U.S.-led Order. *Insight Turkey* [online]. 2019, roč. 21, č. 4, s. 21–22 [cit. 09. 04. 2020]. Dostupné z: https://www.insightturkey.com/commentary/a-three-level-analysis-of-turkeys-crisis-with-the-us-led-order

53 CUPOLO, Diego. Delayed S-400 Activation could offer chance for Turkey-US ties to warm. In: *Al-Monitor* [online]. 21. 4. 2020 [cit. 21. 04. 2020]. Dostupné z: http://www.al-monitor.com/pulse/originals/2020/04/s-400-delay-us-turkey-window-opportunity.html

54 ERDEM, Bora. US-Turkey Relations in the Light of Turkey's Freedom of Press. *Global Media Journal*. 2018, roč. 16, č. 30.

Ruska a Íránu. Tuto politiku započala Obamova administrativa a dlouhou dobu v ní nepolevovala ani administrativa Donalda Trumpa. Významnou částí Syrských demokratických sil jsou kurdské milice, jež Turecko vnímá, zejména pro propojení se Stranou kurdských pracujících (PKK), jako zásadní hrozbu pro svou integritu.[55] Jelikož kurdská otázka je citlivá nejenom pro politické elity, ale i veřejnost, není divu, že antiamerické sentimenty byly v posledních letech na historickém maximu. Spojené státy jsou dnes dle průzkumů veřejného mínění vnímány jako největší hrozba pro Turecko.[56]

Zhoršení vztahů se projevilo i v tom, že byla započata debata o redukci americké vojenské přítomnosti na základně v Incirliku.[57] Na tureckou ofenzivu proti kurdským silám v severní Sýrii z října 2019 reagovala Trumpova administrativa vyhlášením sankcí na některé členy turecké vlády.[58] V tu dobu byly vzájemné vztahy již poškozeny kauzou S-400, která nakonec vedla k vyřazení Turecka z programu F-35, v jehož rámci mělo Turecko získat 100 kusů a mělo se i podílet na jeho produkci.[59] Trumpova administrativa, která slíbila voličům snížit americké angažmá ve světě, není příliš ochotná Turecku v Sýrii jakkoli pomáhat a hlouběji zabředat do konfliktu, který je z hlediska životních amerických národních zájmů nevýznamný.[60]

Disharmonii v zájmech spojenců v Sýrii lze shrnout následovně: Ankara vnímá kurdské milice jako největší hrozbu, Asada jako hrozbu sekundární a *Daiš* jako terciární. Washington považuje za největší hrozbu *Daiš*, pak Írán a až na vzdáleném posledním místě Asada.[61]

---

55 OĞUZLU, H. Tarık. Turkish Foreign Policy in a Changing World Order. *All Azimuth: A Journal of Foreign Policy and Peace* [online]. 2018, s. 135 [cit. 13. 04. 2020]. Dostupné z: http://dergipark.org.tr/en/download/article-file/920715

56 AYDIN, Mustafa. *Türk Dış Politikası Kamuoyu Algıları Araştırması, 17 Haziran 2020*.

57 LUBOLD, Gordon, Felicia SCHWARTZ a Nancy A. YOUSSEF. U.S. Pares Back Use of Turkish Base Amid Strains With Ankara. In: *Wall Street Journal* [online]. 11. 3. 2018 [cit. 16. 04. 2020]. Dostupné z: https://www.wsj.com/articles/u-s-pares-back-use-of-turkish-base-amid-strains-with-ankara-1520766121

58 TRUMP, Donald J. Executive Order on Blocking Property and Suspending Entry of Certain Persons Contributing to the Situation in Syria. In: *The White House* [online]. 14. 10. 2019 [cit. 16. 04. 2020]. Dostupné z: https://www.whitehouse.gov/presidential-actions/executive-order-blocking-property-suspending-entry-certain-persons-contributing-situation-syria/“plainCitation“:“TRUMP, Donald J. Executive Order on Blocking Property and Suspending Entry of Certain Persons Contributing to the Situation in Syria. In: The White House [online]. 14. 10. 2019 [cit. 16. 04. 2020]. Dostupné z: https://www.whitehouse.gov/presidential-actions/executive-order-blocking-property-suspending-entry-certain-persons-contributing-situation-syria/“,“noteIndex“:58},“citationItems“:[{„id“:1528,“uris“:[„http://zotero.org/users/4884900/items/VP8948DZ“],“uri“:[„http://zotero.org/users/4884900/items/VP8948DZ“],“itemData“:{„id“:1528,“type“:“webpage“,“abstract“:“By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.

59 Multilateral (06-1231) - Memorandum of Understanding Concerning the Production, Sustainment, and Follow-On Development of the Joint Strike Fighter. In: *United States Department of State* [online]. 31. 12. 2006 [cit. 16. 04. 2020]. Dostupné z: https://www.state.gov/06-1231

60 COOK, Steven A. The War in Syria Is Turkey’s Problem, Not America’s. In: *Foreign Policy* [online]. 3. 6. 2020 [cit. 16. 04. 2020]. Dostupné z: https://foreignpolicy.com/2020/03/06/syria-turkey-us-problem-idlib-crisis/

61 ÇAĞAPTAY, Soner. *Erdogan’s Empire: Turkey and the politics of the Middle East*. London: I.B. Tauris, 2019, s. 131.

Zejména po roce 2016 Turecko sleduje politiku „více azimutů“ charakterizovanou Erdoğanovým heslem „svět je větší než pětka“ (maje na mysli pět jaderných mocností).[62] Součástí této politiky se po roce 2016 stalo sblížení s Ruskem (vzhledem k odkazu na jaderné mocnosti poněkud paradoxně), přestože v Sýrii patří Rusko mezi strategické oponenty Turecka a Sovětský svaz v minulosti učinil mnohé pro podporu PKK. Rusko rétoricky podpořilo Erdoğanovu vnitřní politiku po neúspěšném puči roku 2016[63] a zejména v kontrastu s vlažným odsouzením puče ze strany Obamovy administrativy začalo Turecko vnímat Rusko jako spolehlivého partnera, který tureckým problémům rozumí.[64] Ve spolupráci s Ruskem je budována jaderná elektrárna v Akkuyu za 20 mld. USD, plynovod TurkStream a Turecko si obstaralo ruský systém protivzdušné obrany S-400 v ceně kolem 2,5 mld. USD.[65] Z hlediska Ruska se nepochybně jednalo o diplomatický úspěch, protože se podařilo vrazit hlouběji klín mezi Turecko a jeho tradiční spojence. Rusko tento krok ani nic nestál. Za výše uvedené zboží musí Turecko tak jako tak zaplatit. O dosažení rusko-tureckého strategického partnerství ale nemůže být ani řeči, protože jejich odlišné zájmy v Sýrii, Libyi, Íránu a na Balkáně k němu nevytváří příliš velký prostor.[66] Erdoğanovi je, zdá se, souzeno naplňovat staré turecké přísloví, že „Turek nemá jiného přítele než sebe sama“.[67] Velmi úspěšně se zbavuje tureckých spojenců, aniž by získal spojence nové. Vrcholem tohoto paradoxu je, že je na západních státech ekonomicky závislý. V roce 2019 se mezi deseti nejvýznamnějšími státy pro turecký export nacházely pouze tři nezápadní země: Irák na 3. místě (9 mld. USD tureckého exportu), na 9. místě Izrael (4,4. mld. USD)

---

62 ARAL, Berdal. “The World is Bigger than Five”: A Salutary Manifesto of Turkey’s New International Outlook. *Insight Turkey* [online]. 2019, roč. 21, č. 4 [cit. 09. 04. 2020]. Dostupné z: https://www.insightturkey.com/article/the-world-is-bigger-than-five-a-salutary-manifesto-of-turkeys-new-international-outlookErdoğan’s charisma and his powerful sense of mission to carry the ‘periphery’ into the center as well as Turkey’s ascendancy to a rising power that has prompted it to advocate multipolarity in the international system. This article argues that the motto “the world is bigger than five” has a number of connotations: a strong support for a just and peaceful international order; a plea against permanent membership and the accompanying veto mechanism; a call for reforming the UN to render the UNSC more representative, transparent and accountable; and an outcry against imperialistic interventions.”,”container-title”:”Insight Turkey”,”ISSN”:”1302177X, 25647717”,”issue”:”4”,”journalAbbreviation”:”IT”,”language”:”en”,”source”:”DOI.org (Crossref

63 Turkey thanks Putin for unconditional support over coup attempt - Turkey News. In: *Hürriyet Daily News* [online]. 25. 7. 2016 [cit. 16. 04. 2020]. Dostupné z: http://www.hurriyetdailynews.com/turkey-thanks-putin-for-unconditional-support-over-coup-attempt---102062

64 AKTÜRK, Şener. Relations between Russia and Turkey Before, During, and After the Failed Coup of 2016. *Insight Turkey* [online]. 2019, roč. 21, č. 4, s. 105 [cit. 09. 04. 2020]. Dostupné z: https://www.insightturkey.com/article/relations-between-russia-and-turkey-before-during-and-after-the-failed-coup-of-2016

65 MEYER, Henry a Fırat KOZOK. Putin Swallows Irritation at Erdogan as Syria Strains Ties - Bloomberg. In: *Bloomberg* [online]. 6. 2. 2020 [cit. 16. 04. 2020]. Dostupné z: https://www.bloomberg.com/news/articles/2020-02-06/putin-swallows-irritation-at-erdogan-as-syria-clash-strains-ties

66 TOL, Gönül a Ömer TAŞPINAR. Turkey’s Russian Roulette. In: MEZRAN, Karim a Arturo VARVELLI, eds. *The MENA Region: A Great Power Competition* [online]. Milano: ISPI and Atlantic Council, 2019, s. 121–123 [cit. 16. 04. 2020]. Dostupné z: https://www.ledizioni.it/download/25762/

67 ILYAS, Ahmet a Murat SILINIR. Strategic Role of Nationalism in Nation-State Building Process: Comparative Historical and Instrumental Analysis of Italy, Germany and Turkey in the Context of Nationalism. *European Journal of Social Sciences*. 2016, roč. 51, č. 4, s. 262.

a na 10. místě Rusko (3,9 mld. USD). Do Ruska šlo pouze 2,3 % tureckého exportu, což z něj rozhodně nečiní klíčové exportní teritorium pro turecké hospodářství.[68]

ZÁVĚR

Erdoğan se svojí zahraniční politikou vmanévroval v Sýrii do strategické slepé uličky a turecká strategická pozice v Sýrii není příliš příznivá. Turecko nemá spojence, kteří by jej v této kauze podpořili. Rozsáhlejší operace v Sýrii a zatlačení na Damašek by narazilo na odpor jak Ruska, tak Západu.[69] Obyvatelstvo není příznivě nakloněno dalšímu tureckému angažmá. Ozbrojené síly Turecka se vyrovnávají s čistkami a reformou a jeho protivzdušná obrana má daleko do optimální kondice. Otevřená eskalace se syrskými a ruskými silami by mohla být pro Turecko poměrně nebezpečná jak vojensky, tak politicky.

Na straně druhé ale musíme vzít v potaz, že Turecko má v Sýrii ve srovnání s Ruskem velmi podstatnou výhodou, kterou je geografie. Pokud by se rozhodlo eskalovat, může Rusku velmi významně ztížit přístup do regionu a zkomplikovat logistikou podporu ruských a syrských sil. Dokud Turecko nenapadne ruské teritorium a není žádný vojenský ani politický důvod, proč by tak mělo činit, bude pro Rusko velmi komplikované rozhodnout se pro přímý vojenský útok proti Turecku. Pokud totiž Rusko napadne turecké síly a vojenské základny na území Turecka, riskuje velmi významně, že se otevře debata o aktivaci článku 5 Washingtonské smlouvy. Ano, Rusko má jaderné zbraně a může jimi hrozit. Není ale jediným aktérem v syrské hře, který je jadernou mocností. Dále je třeba vzít v potaz, že pokud bude Putinovo Rusko příliš mařit sledování tureckých bezpečnostních zájmů v Sýrii, může to zhatit dosažení mnohem lákavějšího ruského strategického cíle, totiž dokončit odklon Turecka od Spojených států a Západu obecně.[70]Přesto není Erdoğanova pozice, do které se sám vmanévroval, záviděníhodná. Chybný krok by jej mohl stát vše, co se mu za minulé dekády podařilo při změnách v turecké společnosti dosáhnout.

Z těchto důvodů lze uzavřít, že Turecko na válku v Sýrii není připraveno a kalkulace ve prospěch rozpoutání otevřeného vojenského konfliktu by byla ze všech úhlů iracionální. Jestli se prezident Erdoğan bude chovat racionálně, nelze v dohledné době očekávat válku mezi Tureckem a Asadovou Sýrií, alespoň dokud nedojde k vývoji, který by zásadně změnil kalkulace aktérů.

68 WORKMAN, Daniel. Turkey's Top Trading Partners. In: *World's Top Exports* [online]. 1. 2. 2020 [cit. 16. 04. 2020]. Dostupné z: http://www.worldstopexports.com/turkeys-top-import-partners/

69 HALE, William. Turkey, America, Russia and the Syrian Civil War. *Insight Turkey* [online]. 2019, roč. 21, č. 4, s. 38 [cit. 09. 04. 2020]. Dostupné z: https://www.insightturkey.com/commentary/turkey-the-us-russia-and-the-syrian-civil-war

70 ÇAĞAPTAY, Soner. Turkey's Options for Pressuring Russia in Idlib Are Limited. In: *The Washington Institute* [online]. 11. 2. 2020 [cit. 16. 04. 2020]. Dostupné z: https://www.washingtoninstitute.org/policy-analysis/view/turkeys-options-for-pressuring-russia-in-idlib-are-limited

Tento článek byl vypracován v rámci řešení grantového projektu „Metodika predikce, včasného varování a prevence hrozeb plynoucích z regionálních ozbrojených konfliktů pro vnitřní bezpečnost ČR" (VI20172020094, Ministerstvo vnitra České republiky).

Autoři: ***Mgr. et Mgr. Vladimír Bízik****, narozen 1989. Vystudoval magisterský obor Právo a právní věda na Právnické fakultě (2012) a magisterský obor Mezinárodní vztahy na Fakultě sociálních studií (2016) Masarykovy univerzity v Brně. Také studoval na Marmara University a Bilgi University v tureckém Istanbulu; a na kyperské University of Nicosia. Pracoval na Mezinárodním politologickém institutu Masarykovy univerzity a v neziskových organizacích Liga lidských práv a Think-tank Evropské hodnoty. Nyní působí na Fakultě sociálních studií Masarykovy univerzity jako doktorand v oboru Mezinárodní vztahy a evropská politika. Zabývá se problematikou pacifikace státních společností, teoriemi mezinárodních vztahů a zeměmi Blízkého východu.*

prof. PhDr. Zdeněk Kříž, Ph.D.*, narozen 1972. Vystudoval politologii a historii na FF MU. V letech 2010 a 2011 byl členem odborného týmu ministra obrany pro zpracování Bílé knihy o obraně České republiky 2011. V současnosti působí jako vedoucí Katedry mezinárodních vztahů a evropských studií Fakulta sociálních studií Masarykovy univerzity v Brně. Specializuje se na dějiny mezinárodních vztahů, mezinárodní bezpečnostní organizace, bezpečnostní politiku Německa a České republiky, civilní řízení a demokratickou kontrolu armády a na historii válečných konfliktů. Je autorem a spoluautorem řady monografií a článku na tato a příbuzná témata.*

Jak citovat: BÍZIK, Vladimír, and Zdeněk KŘÍŽ. Je Turecko připraveno na válku se Sýrií? *Vojenské rozhledy*. 2020, 29 (3), 057-071. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz

Informace

Příčiny vzniku a začlenění kybernetických sil a informačních operací do Armády České republiky

Reasons of formation and integration of cyber forces and information operations into the Army of the Czech Republic

Martin Havlík

Abstrakt: Cílem tohoto informativního článku je komplexně popsat příčiny vzniku a začlenění kybernetických sil a informačních operací do struktury Armády České republiky, včetně dalších významných konotací. Záměrem není prezentovat nové vědecké poznatky, ale poukázat na smysl existence kybernetických sil a informačních operací, jako nutné separátní složky Armády České republiky schopné reakce na dynamický vývoj bezpečnostního prostředí a neutichající rozvoj moderních technologií. Obsah a hlavní argumenty tohoto článku reflektují přechod od klasické formy válčení k platformě nové, reprezentované zejména kybernetickým prostorem a hybridní kombinací široké škály nástrojů moci s důrazem na informační operace.

Abstract: The goal of this informative article is to comprehensively describe the causes of the formation and integration of cyber forces and information operations into the structure of the Army of the Czech Republic, including other significant connotations. The intention is not to present new scientific findings, but to point out the meaning of the existence of cybernetics and information operations as a necessary separate component of the Army of the Czech Republic capable of responding to the dynamic development of the security environment and the continuous development of modern technologies. The content and main arguments of this article reflect the transition from the classical form of warfare to the new platform, represented mainly by cyber space and a hybrid combination of a wide range of power tools with an emphasis on information operations.

Klíčová slova: Bezpečnost; operace; moderní technologie; multidoménový boj.

Keywords: Security; Operation; Modern Technology; Multi-Domain Battle.

ÚVOD

Informativní článek zaměřený na integraci kybernetických sil a informačních operací do struktury Armády České republiky (AČR) je určen pro vojenské publikum v rámci České republiky, českou odbornou bezpečnostní komunitu i širokou veřejnost jakožto nástroj osvěty a potřeby reflektovat význam kybernetického prostředí v současném světě. Řešená problematika koresponduje s aktuálním rámcem výstavby a rozvoje schopností AČR, který je doktrinálně ukotven v příslušných koncepčních dokumentech AČR a rezortu ministerstva obrany České republiky.

V úvodu je nutné si uvědomit, že samotné výsledky, přínos a efektivitu popisované integrace nových kyberneticky orientovaných schopností do AČR bude možné expertně posoudit až s odstupem několika let či dekád. Metodologický přístup k tomuto článku je interpretativního typu, který je pro výklad a objasnění tématu užitečnější, než například teorie a výzkumný přístup explanační.

Na úvod je vhodné zmínit také limitující podmínky a základní východiska, jež reálně omezují hloubku interpretovaných faktů a argumentů. Jde především o celkový rozsah a předem definovaný strukturální rámec informativního článku, které omezují obsahovou zevrubnost, včetně hloubky provedených rozborů vztahujících se k hlavním argumentům a ukazatelům. Mimo uvedené omezení je nutné brát v potaz citlivost samotného tématu ve vztahu k unikátním vojenským schopnostem a ochraně souvisejících utajovaných informací.

Deskripce jednotlivých kapitol kopíruje z pohledu autora záměrně realistické vymezení bezpečnosti, které obecně zdůrazňuje, že si jednotliví státní aktéři musí zajistit svou bezpečnost vlastními silami (tedy schopnostmi, případně i kumulací moci), kdy dochází logicky k nárůstu vyzbrojování, posilování a modernizaci armády (a dalších bezpečnostních subjektů) a uzavírání případných dohod s dalšími aktéry (ve smyslu bilaterálních či multilaterálních dohod[1]). Celý obsahový kontext článku reflektuje vlastní lokaci autora, kdy pohled na zkoumanou problematiku je typu „insider“.[2]

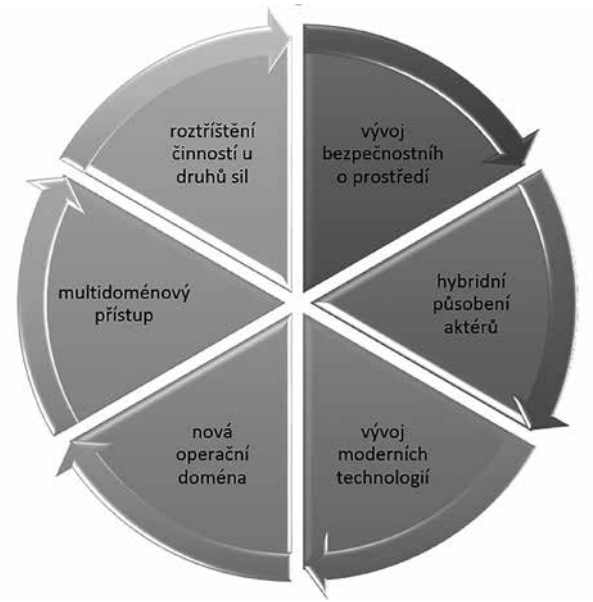
1 PŘÍČINY VZNIKU KYBERNETICKÝCH SIL A INFORMAČNÍCH OPERACÍ V AČR

Vznik kybernetických sil a informačních operací byl v uplynulých letech iniciován a determinován několika významnými faktory (konkrétně viz následující obrázek), které

1 Například spolupráce v rámci OSN (Organizace spojených národů), NATO (North Atlantic Treaty Organization), EU (European Union) či V4 (Visegrádská čtyřka).

2 Pohled typu „insider“ lze obecně chápat tak, že se autor článku (studie, kvalifikační práce apod.) pohybuje přímo v dané oblasti zájmu, případně v konkrétním regionu, jde-li například o specifickou regionální analýzu zaměřenou na vybraného státního aktéra.

mají majoritně nadnárodní globální rozměr (až na roztříštěnost či decentralizaci kybernetických a informačních činností u jednotlivých druhů sil v rámci AČR). Mimo uvedené je vhodné zdůraznit, že některými schopnostmi ze spektra informačních operací v kybernetickém prostoru AČR vůbec nedisponovala. V této kapitole bude dále jednotlivým faktorům (těm nejvýznamnějším) věnována bližší pozornost s cílem osvětlení vážnosti a implikací, které následně vedly ke vzniku kybernetických sil a informačních operací, jakožto nedílné a samostatné součásti AČR.



Obrázek č. 1: Hlavní příčiny vzniku kybernetických sil a informačních operací v AČR

1.1 Změna a dynamický vývoj bezpečnostního prostředí (strategického i operačního), a to nejen v kontextu aktuální situace v Evropě, Africe či na Blízkém a středním východě ve vztahu k migrační krizi a související hrozbě teroristických útoků

Strategické prostředí zahrnuje mezinárodní vztahy a je charakterizované celosvětově, a to většinou na základě bezpečnostních hrozeb (mezinárodní terorismus, neschopnost vlád spravovat území vedoucí až ke zhroucení státu, šíření zbraní hromadného ničení, mezinárodní organizovaný zločin, místní či regionální etnické a teritoriální konflikty, humanitární krize jako důsledek ozbrojených konfliktů, nevratné změny životního prostředí, přírodní katastrofy, průmyslové havárie a pandemie). Strategické prostředí je nadále charakterizováno vysokou dynamikou změn, rostoucí různorodostí aktérů a stále složitější

provázaností bezpečnostních trendů a faktorů. Hrozby, rizika a jejich zdroje jsou mnohdy obtížně lokalizovatelné a nyní mají převážně nestátní a nadnárodní charakter.[3],[4]

Operační prostředí je tvořeno souborem činitelů, okolností a vlivů, jež určuji konkrétní podmínky, ve kterých bude prostřednictvím vojenské operace dosahováno stanovených cílů. Patří sem mimo jiné terén, klimatické a povětrnostní podmínky, charakter státu, sociální demografie, regionální a mezinárodní vztahy, vojenské schopnosti všech stran konfliktu, informační situace, technologie, externí (nevojenské, nevládní) organizace zúčastněné v prostoru operace, národní zájmy všech zúčastněných stran, čas, ekonomika v dané oblasti a další vlivy. Operační prostředí, ve kterém jsou nebo budou ozbrojené síly nasazeny, ovlivňuje způsob vedení operací na všech stupních velení a řízení. Pochopení operačního prostředí a jeho součástí v politické, ekonomické, vojenské, sociální, bezpečnostní a informační oblasti a stavu infrastruktury je klíčovým faktorem pro dosažení cílů operace. Informační procesy, včetně zpravodajského zabezpečení či kybernetické ochrany, musí být schopny identifikovat hrozby vůči záměrům dosažení stanovených cílů a bezpečnosti vlastních sil ve všech fázích operace bez ohledu na to, v jak složitém prostředí budou vojenské síly operovat.[5],[6]

Výše uvedené vymezení strategického a operačního prostředí a zejména jejich nedávný vývoj generovaly potřebu reagovat na změny ve způsobech prosazování zájmů státních i nestátních aktérů. V této souvislosti se napříč českou bezpečnostní komunitou stále více akcentovala otázka významu či dopadu kybernetických útoků. Mimo armádní oblast, kde se kybernetické problematice v omezené míře věnovalo Centrum CIRC[7] pod AKIS (Agentura komunikačních a informačních systémů), se uvnitř rezortu obrany ČR problematikou kybernetické bezpečnosti, obrany a ochrany začaly intenzivněji zabývat také Vojenské zpravodajství a Odbor bezpečnosti Ministerstva obrany. Dílčími schopnostmi vést informační operace pak disponovaly Speciální síly a také 103. centrum CIMIC/PSYOPS v podřízenosti Pozemních sil AČR.

1.2 Nárůst hybridního působení, aktivit a hrozeb státních i nestátních aktérů s využitím kybernetického prostoru a informačních nástrojů

V kontextu vývoje bezpečnostního prostředí je vhodné dodat, že v současné době existuje pro společnost (v globálním i regionálním pohledu) mnoho odlišných a aktuálních hrozeb, u nichž je nejistá pravděpodobnost a velmi nízká předvídatelnost. Jakákoliv

3 MINISTERSTVO OBRANY ČR. Odbor komunikace a propagace MO. *Bílá kniha o obraně.* Praha, Ministerstvo obrany ČR, 2011. ISBN 978-80-7278-564-3. Str. 168.

4 KOVÁŘ, František, KRCHOVÁ, Hana. *Strategický management.* 1. vydání. Praha: Vysoká škola ekonomie a managementu, 2006. ISBN 978-80-86730-29-5. Str. 178.

5 JANÁČ, Karel. *Zpravodajství z lidských zdrojů na operačním a taktickém stupni v podmínkách AČR.* 2011, Vyškov: Správa doktrín ŘeVD.

6 *Doktrína AČR v mnohonárodních operacích.* 2008, 1. vyd. Vyškov: Správa doktrín ŘeVD. Str. 144.

7 CIRC (Computer Incident Response Capability) reprezentuje schopnost reakce na počítačové incidenty.

forma odstrašování není v současné době již plně relevantní a příslušné vojenské strategie musí být proto sestaveny tak, aby byly připraveny na nejistotu a šok. Tyto skutečnosti mají velmi významný dopad také na hodnocení a predikci vývoje bezpečnostní situace v celosvětovém měřítku, a to z pohledu akademických, politických, vojenských či zpravodajských subjektů.[8] Nejvíce je v posledních pěti letech skloňován význam takzvaného hybridního působení a hybridních hrozeb státních i nestátních (případně také proxy-státních) aktérů, jež preferují použití nekonvenčních nástrojů moci s velmi zásadním a stále intenzivnějším využíváním kybernetického prostoru. V této souvislosti lze kybernetické prostředí efektivně využít k prosazení nejrůznějších zájmů. V oblasti obrany je proto zapotřebí alternativně rozvíjet bezpečnostní, obranné a ochranné mechanismy a procesy, které by byly schopny detekovat, identifikovat, analyzovat, ochránit či zabezpečit vlastní kybernetický prostor a k němu afilovanou kritickou infrastrukturu (a všechny související referenční objekty či chceme-li aktiva). Je proto logické, že ani AČR nemohla v této souvislosti zůstat stranou a nereagovat na evidentní bezpečnostní hrozby a výzvy.

1.3 Neustálý vývoj a s ním spojená široká implementace moderních technologií (včetně umělé inteligence, IoT – Internet of Things, nanotechnologií či autonomních robotických systémů apod.) v komerční sféře i vojenském segmentu potenciálních protivníků

Pokud budeme chtít reflektovat dlouhodobé, střednědobé i aktuální (krátkodobé) požadavky vládních autorit zakomponované v bezpečnostní i zahraniční politice s ohledem na působení proti potencionálním hrozbám, bude potřeba, aby jednotlivé subjekty podílející se na obraně proti hrozbám včasně a nepřetržitě reagovaly na okolní prostředí, jež se velmi dynamicky mění. Na základě těchto předpokladů je důležité, aby se, jak jednotlivé složky ozbrojených sil, tak i dalších státních subjekty (včetně zpravodajských institucí) a integrovaného záchranného systému kontinuálně přizpůsobovaly novým trendům a metodám s využitím nejmodernějších technologií.

Trvalým úkolem Armády České republiky je připravovat se k obraně země a bránit ji proti vnějšímu napadení a zároveň se připravovat k zapojení do obrany v rámci systému kolektivní obrany NATO. Armáda musí disponovat schopnostmi pro naplnění politicko-vojenských ambicí České republiky[9] a dalších úkolů a závazků. Předpokládaný vývoj bezpečnostního prostředí a záměr použití armády vyžaduje, aby byly rovnoměrně rozvíjeny všechny požadované schopnosti (včetně kybernetické ochrany a aktivního informačního působení v kybernetickém prostoru). Zde nepopiratelnou roli hrají i kybernetické síly a široké spektrum souvisejících informačních operací.

8 HAVLÍK, Martin. *Fenomén Big Data jako trend ovlivňující technické zpravodajské disciplíny.* Brno - Vojenské rozhledy, 2014, roč. 23 (55), č. 4. ISSN 1210-3292. Str. 124 – 132.

9 Usnesení vlády ČR ze dne 26. září 2012 č. 699 o Obranné strategii České republiky.

V souvislosti s masivním rozvojem moderních technologií v posledních letech narůstá také intenzita, počet a nebezpečnost samotných útoků na informační a komunikační infrastrukturu (obecně kritickou infrastrukturu). Do popředí se ve vojenské oblasti dostávají zejména prostředky pasivního monitoringu a sledování kybernetického prostoru, které poskytují nové výhody v získávání, analýze a distribuci tolik potřebných informací (často také zpravodajských informací) o prostoru zpravodajského zájmu z multidoménového pohledu. Je přínosné reflektovat to, že jak softwarové, tak i hardwarové prostředky by měly být vyvíjeny na modulárním základě z důvodu jejich efektivnějšího využití a všestranné výhodnosti při jejich budoucí modernizaci. Se zefektivňováním organizačních struktur úkolových uskupení v operacích lze očekávat další těsnější logické propojení zpravodajství, elektronického boje a informačních operací, a to zejména na operačním a taktickém stupni.

1.4 Akceptace kybernetického prostoru jako další (vedle pozemní, vzdušné, námořní a vesmírné[10]) operační domény NATO, a to konkrétně na summitu NATO ve Varšavě v roce 2016

Od konce Studené války do dnešních dnů je patrný vývoj v oblasti dimenzí (viz následující obrázek) ozbrojených konfliktů a také s tím souvisejících operací, který souvisí s přechodem od fyzické podoby válčiště k platformě mnohem více imaginární reprezentované zejména kybernetickým prostorem.

Obrázek č. 2: Uznané operační domény NATO od konce roku 2019

10 Vesmírná doména byla v rámci NATO akceptována až no konci roku 2019.

Přes uvedené skutečnosti však nelze tvrdit, že se jednotlivé strany současných a zcela jistě také budoucích konfliktů budou výhradně soustředit na válku v kybernetickém prostoru, ale budou využívat kombinaci všech pěti dimenzí. V oblasti vojenských (zejména zpravodajsky orientovaných) aktivit světových velmocí zaměřených na pronikání do strategických subjektů kritické infrastruktury (například průnik USA a Izraele do iránských zařízení pro obohacování uranu), získávání strategicky významných informací v oblasti průmyslové špionáže (zejména v případě Čínské lidové republiky), bude prostor kybernetický majoritním působištěm budoucích konfliktů a také širokého spektra bezpečnostních operací. Pokud budeme reflektovat současné trendy v oblasti vývoje a zaměření operací, lze poukázat na následující parametry, které strukturálně nejvíce charakterizují operace budoucnosti. Jedná se o:

- komplexní operace vedené ve všech pěti dimenzích (doménách);
- důraz na informační operace vedené v kybernetickém prostoru;
- komplexní rozměr operací v celém spektru možných konfliktů;
- vedení více souběžných operací na mnoha různých místech v globálním pohledu;
- vzrůstající operační tempo budoucích operací.[11]

1.5 Potřeba komplexního propojení všech operačních domén a multidoménový (multi-domain) přístup k efektivnímu plánování a vedení operací

V případě kybernetického prostoru jde vůbec o první doménu, která není jednoznačně ohraničena a široce se prolíná všemi ostatními operačními doménami (více viz následující obrázek). Naopak můžeme tvrdit, že kybernetický prostor zastřešuje a pokrývá všechny ostatní operační domény (i když například v případě vesmíru tomu tak není komplexně).[12] Efektivní působení v kybernetické doméně z pohledu AČR není zcela pochopitelně možné zabezpečit jinak, než záměrnou výstavbou nových, separátních a speciálně zaměřených prvků ve struktuře AČR disponujících adekvátními prostředky a schopnostmi.

Poměrně nový multidoménový přístup vyspělých armád musí reagovat na bezpečnostní výzvy a zejména na strukturu schopností a přístupy potenciálních protivníků. Je tedy žádoucí, aby armády „západní“ společnosti byly schopné společným úsilím zvítězit v případné budoucí multidoménové válce, která bude reprezentována kombinací konvenčních zbraní (využívajících moderní technologie), elektronického boje, informačních operací v kybernetickém prostoru a také působení ve vesmíru. Multidoménové operace budoucnosti budou mnohem komplikovanější a náročnější ve vztahu k nasazeným silám a prostředkům. Cílem bude nadále minimalizovat rizika vlastního

11 HAVLÍK, Martin. *Vývoj operačního prostředí v kontextu budoucích konfliktů a směřování zpravodajské podpory*. Bezpečnostní teorie a praxe. 2015, č. 4. ISSN 1801-8211.

12 Vždy je nutné reflektovat prostor pokrytí jednotlivých domén dostupnými kybernetickými prostředky.

ohrožení a posilovat efektivitu při plnění náročných operačních požadavků. Zde (jakožto součást multidoménového boje) bude nezanedbatelnou (v budoucnu naopak klíčovou) roli hrát právě kybernetický prostor a informační operace v něm vedené.

Obrázek č. 3: Provázání kybernetické domény s ostatními operačními doménami

Některé zdroje uvádějí, že se díky pokroku především v síťových technologií budou postupně potírat rozdíly mezi jednotlivými operačními doménami v případě zmiňovaného multidoménového boje. Činnost v jedné doméně tedy obecně výrazně ovlivní situaci v další doméně. Letouny, pozemní protivzdušná obrana, prostředky aktivního kybernetického boje, vesmírné senzory a další vojenské systémy budou v multidoménovém boji vytvářet síťově propojený bojový systém, který v reálném čase povede koordinovanou bojovou činnost. Vojáci budou postupně čelit hrozbám ve všech doménách války, operacím v komplexních prostředích, hybridním strategiím a případně také zbraním hromadného ničení.[13],[14]

Americký TRADOC (Training and Doctrine Command) v poměrně zdařilém přehledovém dokumentu[15] definoval v této souvislosti celkem 12 stěžejních okruhů (vývojových trendů), které budou determinovat budoucí podobu, pojetí a rozměr moderní války.

Jedná se o:

---

13 AN – Armádní Noviny. *Bojiště budoucnosti 2050 podle americké armády.* [online]. 2017 [cit. 2020-03-20]. Dostupné z: https://www.armadninoviny.cz/bojiste-2050-americka-armada-se-pripravuje-pro-bojiste.html

14 AN – Armádní Noviny. *Americké tanky budoucnosti: Klíčem je mobilita a údržba.* [online]. 2019 [cit. 2020-03-20]. Dostupné z: https://www.armadninoviny.cz/americke-tanky-budoucnosti-mobilita-a-udrzba.html

15 US TRADOC. *The Operational Environment and the Changing Character of Future Warfare.* [online]. 2017 [cit. 2020-03-20]. Dostupné z: https://community.apan.org/wg/tradoc-g2/mad-scientist/m/visualizing-multi-domain-battle-2030-2050/200203

- BigData (velkoobjemová data);
- výroba energie a její ukládání (skladování);
- kybernetický prostor a vesmír;
- Collective Intelligence (inteligentní propojení sociálních sítí a zařízení);
- technologie, inženýrství a výroba;
- klimatické změny a konkurenční boj o suroviny;
- Artificial Intelligence (umělá inteligence);
- propojení člověka a počítačů;
- demografie a urbanizace;
- změny v ekonomické rovnováze;
- zvyšování úrovně lidské výkonnosti;
- robotika.

Všechny výše uvedené okruhy trendů budou (jak již bylo nastíněno výše) stále intenzivněji ovlivňovat způsob vedení války i jejich budoucí výsledky. Je proto nutné z pohledu bezpečnostního aparátu ČR (včetně samotné AČR) reflektovat tyto trendy a přizpůsobit nově budované schopnosti takto směřovanému vývoji.

1.6 Roztříštění existujících vojenských činností kybernetického a informačního charakteru ve struktuře jednotlivých druhů vojsk bez jednotného systematického řízení a rozvoje

Decentrální a nesystémové roztříštění elementů i jednotlivců zabývajících se problematikou informačních operací a dalšími činnostmi v kybernetickém prostoru ve struktuře ostatních druhů sil i vojsk bez jednotného velení a řízení podpořilo iniciaci vzniku samostatného organizačního celku, který do budoucna komplexně pojme celou související problematiku kybernetické domény. Toto bylo dále umocněno tím, že některé dílčí schopnosti informačního charakteru (zejména vedení informačních operací v kybernetickém prostoru) nebyly v rámci AČR pokryty vůbec. S ohledem na uvedené bylo proto hlavní úsilí v rámci výstavby kybernetických sil a informačních operací u AČR zaměřeno na sjednocení existujících činností v kybernetickém prostoru a informačním prostředí. Příslušná koncepce výstavby a rozvoje schopností kybernetických sil a informačních operací v AČR však i nadále počítá s tím, že jednotliví specialisté kybernetické problematiky budou působit u útvarů ostatních druhů sil a budou primárně poradním orgánem velitele pro oblast působení v kybernetickém prostoru. Mimo to budou také odpovídat za spolupráci s odborně nadřízenými útvary.

2 MISE, VIZE, HODNOTY A STRATEGIE KYBERNETICKÝCH SIL A INFORMAČNÍCH OPERACÍ

Mise a vize organizací se velmi často ve společnosti zaměňují, uživatelé je nedokáží striktně odlišit a někdy dokonce dochází k tomu, že tyto pojmy někteří jedinci (někdy i samotní zaměstnanci) považují dokonce za synonyma bez obsahového rozdílu. Je potřeba zdůraznit, že tomu tak není a jedná o různé termíny, jejichž vymezení je zcela odlišné. Jediné co lze v případě vize a mise organizace unifikovat je to, že obsah obou těchto významných termínů (vztažených ke konkrétní organizaci) je potřeba široce komunikovat a sdílet, a to jak směrem k vlastním příslušníkům, tak i dalším „stakeholders“ (všem zainteresovaným stranám). Prezentace a sdělení by pak měly být srozumitelné, aby ji všichni jednoznačně pochopili a zejména, aby všichni společně postupovali k jejich naplnění. Takováto vysvětlující kampaň pak zcela jistě pomůže šířeji pochopit to, co daná organizace dělá a všichni zainteresovaní následně podpoří její působení.

2.1 Mise

Mise organizace by měla vycházet z formulací vrcholového vedení, aby co nejlépe reflektovalo podstatu a stanovené cíle organizace. Obecně je mise definována tak, aby byla srozumitelná a poměrně snadno zapamatovatelná všemi zainteresovanými stranami a subjekty. Mise velmi často vychází ze samotného účelu a předmětu (či chceme-li smyslu) existence dané organizace a je v čase poměrně stálá, tedy neměnná.

Smyslem existence kybernetických sil a informačních operací je vybudování samostatného druhu sil ve struktuře AČR, který bude schopen integrovat kybernetické a informační schopnosti do vedení společných a komplexních multidoménových operací AČR.

2.2 Vize

Vize v manažerském pojetí ve vztahu k organizacím obecně vymezuje a popisuje to, čeho chce daná organizace v dlouhodobém horizontu dosáhnout a jaké cíle v této souvislosti naplnit. Vize může obecně existovat (a často tomu s ohledem na duševní vlastnictví a příslušná „know-how“ tak je) pouze v myšlenkách a hlavách zakladatelů, případně sdílena mezi velmi úzkou skupinou vedení předmětné organizace (někdy také i v rámci celé organizace), anebo může být naopak veřejně dostupná a prezentovaná. V případě citlivých oblastí zájmu je někdy přímo žádoucí, aby široká veřejnost nevěděla konkrétně, čeho chce přesně daná organizace v dlouhodobém horizontu dosáhnout. Ve všech případech by však samotná vize měla být dostatečně ambiciózní a měla by umožňovat vlastní modifikaci s ohledem na dosahování stanovených cílů, vývoj okolního prostředí a případné požadavky nadřízených subjektů.

V případě kybernetických sil a informačních operací jako integrální součásti AČR je vize zaměřena na následující oblasti:

- kybernetické síly a informační operace AČR budou schopny působit a mít vliv v informačním prostředí a kybernetické doméně;
- kybernetické síly a informační operace AČR budou schopny chránit své i resortní síly a prostředky (včetně informačních systémů a další infrastruktury), získávat informace a ve spolupráci s Vojenským zpravodajstvím vést kybernetické operace;
- působení v kybernetické doméně a související informační operace budou plně integrovány do vedení společných operací s cílem propojit stávající taktické schopnosti, vytvořit a rozvinout chybějící síly a prostředky ve všech fázích konfliktu, a to konkrétně:
    - zajištěním plánování v kybernetické doméně;
    - zajištěním koordinace informačních operací;
    - zajištěním koordinace civilně-vojenské interakce[16];
- kybernetické síly a informační operace AČR budou schopny poskytovat široké spektrum informací do sdíleného operačního obrazu ve všech fázích konfliktu.

2.3 Hodnoty

Úkolem kybernetických sil a informačních operací jako integrální součásti AČR je podpořit multidoménový přístup k vedení společných operací a přímo se do tohoto společného úsilí zapojit, kdy nejširší spektrum zainteresovaných subjektů jednoznačně chápe a podporuje význam kybernetického prostoru (jakožto nové operační domény) a vedení souvisejících informačních operací k prosazování zájmů České republiky v oblasti obrany.

Klíčovým hybatelem je jednoznačně kontinuálně se vzdělávající lidský personál s nedogmatickou (otevřenou) myslí, který vytváří stěžejní základ pro působení v nové operační doméně (kybernetickém prostoru) a je proaktivně a flexibilně schopný absorbovat nové informace k výkonu všech potřebných činností.

2.4 Strategie

Strategie kybernetických sil a informačních operací není s ohledem na citlivost tématu veřejná. Rámcově jsou strategické postupy a také důležité časové milníky rozvoje vymezeny v existujících koncepčních dokumentech AČR, kde stěžejním je samotná *Koncepce výstavby a rozvoje schopností kybernetických sil a informačních operací v AČR.*[17]

16 Často označováno anglickým termínem Civil-Military Interaction ~ CMI.

17 Vychází dále také z Bezpečnostní strategie ČR, Obranné strategie ČR, Dlouhodobého výhledu pro obranu 2035, Doktríny AČR, Auditu národní bezpečnosti a Cílů výstavby schopností 2017 (CT 2017).

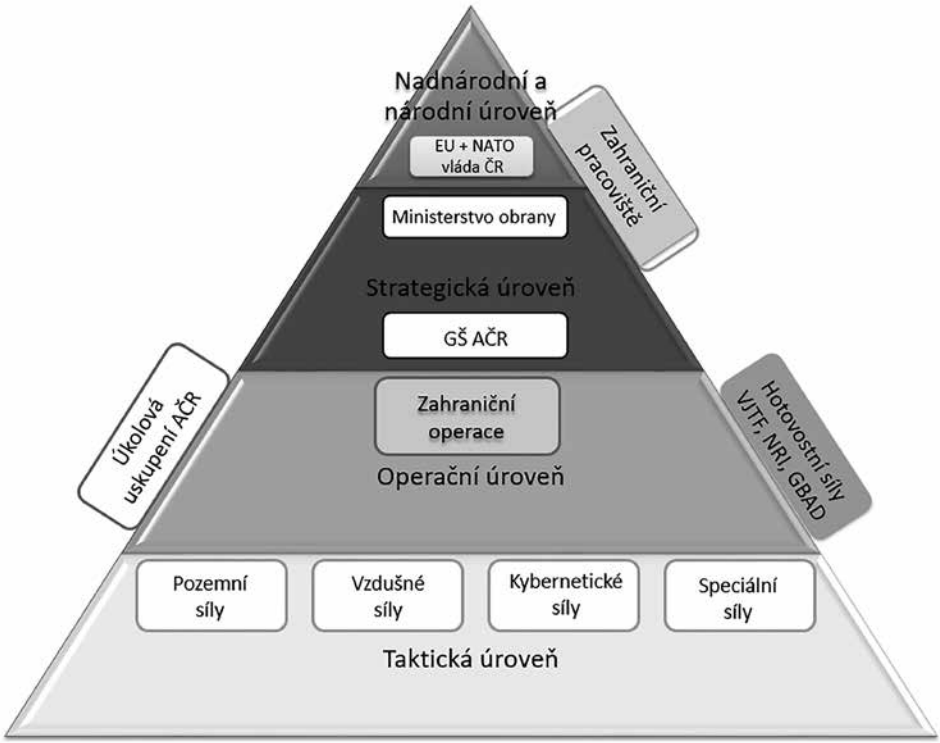
Koncepce výstavby a rozvoje schopností kybernetických sil a informačních operací v AČR je strategickým dokumentem pro výstavbu schopností kybernetických sil a informačních operací. Shrnuje současný stav a definuje úkoly a opatření nezbytná k dosažení požadovaných schopností s cílovým stavem k roku 2030. Tento zmíněný dokument logicky navazuje a blíže determinuje nadřízenou armádní koncepci KVAČR (Koncepce výstavby AČR) a je součástí soustavy koncepčních dokumentů rezortu ministerstva obrany (ustanovena jako koncepce 3. řádu).

3 INTEGRACE KYBERNETICKÝCH SIL A INFORMAČNÍCH OPERACÍ DO AČR

Zámysl vzniku kybernetických sil a informačních operací je datován k přelomu let 2017 a 2018, a to v kontextu výsledků a závěru summitu NATO v Polsku (viz rozšíření počtu operačních domén o kybernetický prostor uvedený v předcházející kapitole) a potřebě reflektovat existenci a význam kybernetického operačního prostoru. Myšlenka vybudování separátního organizačního celku ve struktuře AČR, který se bude předmětnou problematikou zevrubněji zabývat, byla následně podpořena vznikem operačně-organizačního jádra pro výstavbu, a to k 1. lednu 2019 s následným vznikem a zahájením činnosti Velitelství kybernetických sil a informačních operací (VeKySIO) k 1. červenci 2019 se sídlem v Brně. V další fázi rozvoje a budování schopností bylo do podřízenosti VeKySIO transformováno 103. centrum CIMIC/PSYOPS a přejmenováno na Skupinu kybernetických sil a informačních operací (SkKySIO), a to konkrétně k 1. lednu 2020.

Dislokace VeKySIO v Brně byla systematicky prosazena s ohledem na přítomnost Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) a dalších institucí zabývajících se kybernetickou problematikou (akademická pracoviště Masarykovy univerzity, Vysokého učení technického či Univerzity obrany, sídlo armádního centra CIRC, komerční subjekty apod.).

V kontextu dalších rozsáhlých změn v organizační struktuře AČR a s přechodem na staronový trojstupňový systém velení a řízení k 1. lednu 2020 došlo k integraci kybernetických sil a informačních operací (KySIO) na taktickou úroveň vedle pozemních sil, vzdušných sil a speciálních sil. Blíže demonstruje začlenění KySIO do struktury AČR následující schéma.



Obrázek č. 4: Integrace kybernetických sil do struktury AČR/MO[18]

V kontextu integrace kybernetických a informačních operací do struktury AČR a v rámci navazující spolupráce a zejména komunikace se zahraničními subjekty je vhodné unifikovat také používané překlady organizačních součástí kybernetických sil a informačních operací. Oficiálně schválené zkratky a překlady názvů jsou následující:

- *Velitelství kybernetických sil a informačních operací (VeKySIO) => Cyber and Information Warfare Command (CIWC);*
- *Skupina kybernetických sil a informačních operací (SkKySIO) => Cyber and Information Warfare Group (CIWG).*

S ohledem na vše uvedené je proto doporučeno, aby byly v komunikaci s jinými organizačními celky v rámci rezortu ministerstva obrany a v komunikaci se zahraničními partnery používány schválené jednotné názvy, překlady a zkratky.

18 Ve schématu použité zkratky: AČR – Armáda České republiky, ČR – Česká republika, EU – Evropská unie, GBAD – Ground Base Air Defence, GŠ – Generální štáb, NATO – North Atlantic Treaty Organization, NRI – NATO Readiness Initiative, VJTF – Very High Readiness Joint Task Force.

ZÁVĚR

V budoucích operacích je nutné si uvědomovat, že půjde v první řadě o ovládnutí informačního prostoru, prozkoumání a zmapování bojiště, udržení vlastních komunikačních kanálů a přerušení komunikačních tras protivníka. Primární úlohu budou hrát nevojenské hybridní (komplexní) aktivity na jedné straně s kinetickými operacemi ozbrojených jednotek na straně druhé, na se něž primárně zaměřuje západní vojenské myšlení. Je nutné brát v potaz, že na fyzický boj má dojít až úplně naposled, a to za vhodně vymodelovaných a dodržených podmínek. Ideálně však tehdy, když protivník už de facto v informační sféře i politicky prohrál – tedy my jsme získali značnou informační převahu a kontrolu nad jeho vlastním informačním prostorem.

V dnešním globalizovaném světě se bezpečnostní aparát neobejde bez nasazení technických prostředků umožňujících vedení informačních operací či shromažďování informací v kybernetické doméně i celkovém bezpečnostním prostředí. Monitorování komunikací a činnosti v informačním prostředí jsou rozhodujícími instrumenty, které jsou využívány pro identifikaci hrozícího nebezpečí, teprve poté následují obranná opatření, která mají toto nebezpečí minimalizovat. Nasazení moderních technologií v kybernetickém prostoru je proto nezbytné pro udržení vysoké úrovně bezpečnosti státu a nemá nic společného s velmi často mediálně proklamovaným masovým sledováním občanů.

Agresivita regionálních velmocí, soupeření o suroviny, hybridní působení, masivní migrační vlny (související s vývojem na Blízkém východě, Asii či Africe) nebo pandemie jsou hlavními hrozbami pro Českou republiku i Evropu. Dynamický rozvoj vědy a moderních technologií s sebou přináší vyšší dostupnost vyspělých technologií. Dostupnost informačních, nano a biotechnologií a snadnější výroba či automatizace budou přispívat k růstu schopností potenciálních protivníků a jejich zbraňových systémů, jejichž primární ovládání bude realizováno prostřednictvím kybernetického prostoru. V komerční sféře i celé společnosti nadále poroste závislost na informačních technologiích. S tímto budou logicky souviset i kybernetické útoky, které mohou zásadně ohrozit funkčnost státu ve všech jeho dimenzích, včetně ozbrojených sil. Řada států i nestátních entit cíleně proto buduje schopnosti kybernetického útoku na elektronické systémy státních i nestátních institucí a kritickou informační infrastrukturu.[19] Proto je nutné, aby se také Česká republika a její bezpečnostní, ochranné a obranné segmenty také zaměřily na rozvoj a budování schopností čelit kybernetickým hrozbám a efektivně působit v kybernetickém prostoru s cílem zajištění vlastních zájmů. Zde právě hraje významnou roli také výše popisované nově vzniklé kybernetické síly a informační operace, které se v nedávné době staly neodmyslitelnou integrální součástí AČR a rozšířily a doplnily tak systémovou mozaiku národního působení v kybernetickém prostoru.

19 MINISTERSTVO OBRANY ČR. *Dlouhodobý výhled pro obranu 2030.* Praha: Ministerstvo obrany ČR, 2015. 14 s.

Autor: ***Mgr. Ing. Martin HAVLÍK, Ph.D., MBA, MSc.*** *Pracovník Ministerstva obrany České republiky. Specializuje se na zpravodajskou problematiku, zejména pak na oblast technických zpravodajských disciplín, informačních a kybernetických operací jakožto nedílné součásti hybridního působení státních i nestátních aktérů. Mimo uvedené se dlouhodobě zaměřuje na analýzy bezpečnostních hrozeb a rizik v oblastech konfliktů (především v Asii) s dopadem na obranu a bezpečnost České republiky.*

Jak citovat: HAVLÍK Martin. Příčiny vzniku a začlenění kybernetických sil a informačních operací do Armády České republiky. *Vojenské rozhledy.* 2020, 29 (3), 072-086. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz.

Informace

Společná bezpečnostní a obranná politika EU v kostce – část první

EU's Common Security and Defence Policy in a Nutshell – Part One

Vilém Kolín

Abstrakt: Společná bezpečnostní a obranná politika (CSDP), na jejímž základě EU buduje svoji obrannou identitu, je širokospektrální. Zaměřuje se nejen na obrannou složku CSDP, ale i na související oblasti jako obranný průmysl a trh, obranný výzkum a vývoj, a s tím korespondující legislativu a různé politické a finanční nástroje na jejich podporu. To na straně jedné brání snadnému ohraničení problematiky evropské obrany. Na straně druhé to odráží robustnost přístupu EU k evropské obraně a ochotu mobilizovat všechny dostupné zdroje. Článek přibližuje genezi evropské obrany, jejich hlavních milníků, aktérů, souvisejících procesů, pravidel, a klíčových nástrojů, které jsou dnes z podstatné části soustředěny pod hlavičkou CSDP. Aktuální otázky evropské obrany včetně scénářů jejího možného budoucího vývoje mají v textu také své místo, stejně jako příspěvek České republiky.

Abstract: The Common Security and Defence Policy (CSDP), on the basis of which the EU builds its defence identity, has a broad spectrum. It focuses not only on the defence component of the CSDP, but also on associated areas such as defence industry and market, defence research and development, and supports them with related legislation and various policy and financial instruments. On the one hand, this prevents the issue of European defence from being easily confined. On the other hand, this reflects the robustness of the EU's approach to European defence and its willingness to mobilize all available resources. The article describes the evolution of European defence, its major milestones and actors, related processes and rules, and the key tools that are now largely concentrated under the umbrella of the CSDP. Current issues of European defence, including scenarios of its possible future development, are also addressed, as well as the contribution of the Czech Republic.

Klíčová slova: EU; SBOP; PESCO; EDA; Lisabonská smlouva; obranná politika; obranný průmysl.

Key words: EU; CSDP; PESCO; EDA; Lisbon Treaty; Defence Policy; Defence Industry.

ÚVOD: V ČEM JE PŘÍSTUP EVROPSKÉ UNIE K OBRANĚ JINÝ? [1]

Evropská unie *(European Union – EU)* je mnohotvárným a pestrým seskupením, které nabízí svým členům řadu ekonomických a politických výhod včetně jednotného trhu, jednotné měny, společné obchodní a zemědělské politiky, finančních nástrojů na podporu výzkumu a inovací, nebo malých a středních podniků. Jednou z mnoha aktivit, které EU rozvíjí, je i Společná bezpečnostní a obranná politika *(Common Security and Defence Policy – CSDP)*, na jejímž základě EU buduje svoji obrannou identitu – alianci. Na rozdíl od Severoatlantické aliance *(North Atlantic Treaty Organisation – NATO)*, která je založena na jediném účelu, a sice kolektivní obraně svých členů, je záběr EU širokospektrální. Zaměřuje se nejen na obrannou složku CSDP, ale i na související oblasti jako obranný průmysl a trh, obranný výzkum a vývoj, a s tím korespondující legislativu a různé politické a finanční nástroje na jejich podporu. To na straně jedné brání snadnému ohraničení problematiky evropské obrany. Na straně druhé to odráží robustnost přístupu EU k evropské obraně a ochotu mobilizovat všechny dostupné zdroje. A to včetně těch, které byly zřízeny k jinému účelu, než je evropská obrana, jako pravidla pro zadávání zakázek v oblasti obrany a bezpečnosti převzaté z podobné civilní úpravy, nebo pravidla pro čerpání financí na projekty v oblasti bezpečnosti a obrany ze Strukturálních fondů, které byly původně zřízené za jiným účelem, a sice vyrovnání sociální nerovnosti mezi regiony jednotlivých členských států EU.

Cílem tohoto článku, který je s ohledem na svoji délku rozdělen do dvou částí vydaných v tomto a následujícím čísle časopisu, je v prvním z nich popsat genezi evropské obrany, jejich hlavních milníků, aktérů, souvisejících procesů, pravidel, a klíčových nástrojů, jež jsou dnes z podstatné části soustředěny pod hlavičkou CSDP. Prostředkem k tomuto cíli je převážně popisný, avšak snadno uchopitelný, text, jehož smyslem je čtenáři blíže přiblížit fungování tohoto relativně složitého ekosystému. Aktuální otázky evropské obrany včetně scénářů jejího možného budoucího vývoje mají v textu také své místo a tvoří druhou část článku, stejně jako kapitola věnovaná zapojení a příspěvku České republiky.

1 JAK EVROPSKÁ OBRANA VZNIKLA?

Geneze zrodu evropské obrany nebyla jednoduchá ani přímočará a jako taková kopírovala logiku vzniku evropského integračního procesu, který po dvou zničujících válkách měl do Evropy vrátit mír a stabilitu. Jak v té době napsal Robert Schuman, francouzský ministr zahraničí a jeden z duchovních otců myšlenky evropské jednoty: „Evropa se nevytvoří najednou, nebo podle jednoho plánu. Uskuteční se naplňováním konkrétních cílů, vytvářejíc nejprve skutečnou solidaritu!“[2] Tato slova, patrně nejznámější, ze

1 Názory a doporučení obsažené v tomto článku jsou výlučně autora.

2 Schumanova deklarace, 9. května 1950 [online]. [cit. 6. 7. 2019] Dostupné z https://europa.eu/european-union/about-eu/symbols/europe-day/schuman-declaration_cs.

Schumanovy deklarace, dala v roce 1952 vzniknout Evropskému společenství uhlí a oceli (*European Coal and Steel Community – ECSC*), které odstartovalo evropský integrační proces vedoucí ke vzniku EU. Avšak ne vše se dařilo uskutečnit podle plánu. V roce 1954 Francie odmítla návrh na zřízení Evropského obranného společenství (*European Defence Community – EDC*), které by fungovalo na základě společné evropské armády, řízené jedním evropským ministerstvem obrany, jednotným rozpočtem a společným akvizičním programem.[3] Krach návrhu EDC obrátil pozornost k NATO, které vzniklo o pár let dříve. Současně zpomalil realizaci myšlenky evropské obrany takřka o padesát let, nemluvě o vytvoření nadnárodních struktur včetně evropské armády, která je i dnes, po téměř sedmdesáti letech od zrodu této myšlenky, stále v nedohlednu.

Klíčovým momentem pro oživení myšlenky evropské obrany byl rozpad Jugoslávie a následné konflikty v 90. letech minulého století.[4] Absence institucionálního rámce a nástrojů EU pro spolupráci v obraně a bezpečnosti pro řešení podobných krizí naplno odhalila slabiny evropského integračního projektu a jasně ukázala na neschopnost Evropanů vyřešit evropský konflikt „evropskými prostředky“. Vzniklé vakuum vyplnily Spojené státy, které s využitím NATO zásadně přispěly k ukončení válek na Balkáně. EU sice nehrála klíčovou roli v ukončení konfliktu. Nicméně to se napříště mělo změnit. Podobně jako trýznivá zkušenost druhé světové války vedla k oživení myšlenky evropské integrace, odstartovala tato válečná zkušenost novou éru v budování evropské obrany. Tento proces pak během čtvrtstoletí vykrystalizoval v nové ambice, nové instituce a nástroje, a posunul EU blíže k vytvoření odpovídající schopnosti pro zvládání podobných krizí.

2 JAK SE EVROPSKÁ OBRANA USTANOVILA?

Přání disponovat autonomní evropskou vojenskou silou (nezávislou na Spojených státech) je patrné již v Maastrichtské smlouvě z roku 1993, která v rámci pilířového uspořádání EU dává v rámci druhého (mezivládního) pilíře vzniknout Společné zahraniční a bezpečnostní politice (*Common Foreign and Security Policy – CFSP*).[5] Současně jasně hovoří o tom, že CFSP bude zahrnovat všechny otázky týkající se bezpečnosti EU „včetně budoucího vymezení společné obranné politiky, která by časem mohla vést ke společné obraně“[6]. Deklarace britského ministerského předsedy Tony Blaira a francouzského prezidenta Jacquese Chiracka, která zazněla ze Saint Malo v roce 1998 na pozadí stupňující se krize v Kosovu, jenž se NATO zakrátko rozhodlo vyřešit leteckými údery

3 FIDLER, Jiří a PLECHANOVOVÁ, Běla. *Kapitoly z dějin mezinárodních vztahů 1941-1995*. Praha: Institut pro středoevropskou kulturu a politiku, 1997. S. 110. ISBN 80-85241-79-X.

4 REHRL, Jochen, ed. *Handbook on CSDP*. Sv. 1. 3. vyd. Vídeň: Armed Forces Printing Centre, 2017. S. 17. ISBN 978-92-95201-05-7.

5 Smlouva o Evropské unii (EU) - tzv. Maastrichtská smlouva (7. února 1992, platí od 1. listopadu 1993) (92/C 191/01). Hlava V, Ustanovení o Společné zahraniční a bezpečnostní politice [online]. [cit. 13. 7. 2019]. Dostupné z https://www.euroskop.cz/8917/sekce/zakladajici-smlouvy.

6 Ibid. Článek J.4.

proti Jugoslávii, šla ještě o krok dále. Dva tehdy nejdůležitější zastánci myšlenky posilování evropské obrany v ní formulovali návrh na vytvoření důvěryhodné vojenské síly EU k řešení mezinárodních krizí tam, kde NATO není zapojeno.[7]

Deklarace ze Saint Malo byla důležitým mezníkem v realizaci evropské obrany, kdy na straně jedné stanovila její novou ambici a na straně druhé vytvořila její hlavní rámec.[8] Institucionální změny, které následovaly, pak daly myšlence evropské obrany konkrétní podobu. Amsterdamská smlouva z roku 1999 vytvořila pozici Vysokého zmocněnce pro CFSP zastávanou generálním tajemníkem Evropské rady.[9] Smlouva z Nice z roku 2003 formalizovala Evropskou bezpečnostní a obrannou politiku (*European Security and Defence Policy – ESDP*) a vtělila ji do institucionální struktury EU.[10] V návaznosti na vytvoření Politického a bezpečnostního výboru (*Political and Security Committee – PSC*), Vojenského výboru EU (*EU Military Committee*) a Vojenského štábu (*EU Military Staff*), pak ještě svěřila PSC politickou kontrolu a strategické řízení nad operacemi pro řešení krizí.[11] Ve stejném roce byla přijata Evropská bezpečnostní strategie (*European Security Strategy*), první dokument tohoto typu v historii EU, definující bezpečnostní hrozby, zájmy a ambice EU, zejména pak snahu učinit z EU globálního aktéra.[12] O rok později byla k podpoře obranné spolupráce a vojenské integraci členských států založena Evropská obranná agentura (*European Defence Agency – EDA*).[13] V neposlední řadě v roce 2009 vstoupila v platnost Lisabonská smlouva, která dala vzniknout novým nástrojům a nové institucionální struktuře evropské obrany, jež zůstávají v platnosti do současnosti.[14]

---

7 Joint Declaration issued at the British-French Summit, 4. prosince 1998 [online]. [cit. 13. 7. 2019] Dostupné z https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf.

8 Ref. 4. S. 17.

9 Smlouva o Evropské unii. Konsolidovaná verze – ve znění Amsterodamské smlouvy (2. říjen 1997), Hlava V, Ustanovení o Společné zahraniční a bezpečnostní politice, Článek 18; a Článek 26. [online]. [cit. 13. 7. 2019]. Dostupné z https://www.euroskop.cz/8917/sekce/zakladajici-smlouvy.

10 Treaty of Nice amending the Treaty on European Union, the Treaties Establishing the European Communities and certain related acts (2001/C 80/01), Official Journal of the European Communities, 10. března 2001, Declaration adopted by the Conference, Declaration on the European security and defence policy [online]. [cit. 13. 7. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12001C%2FTXT.

11 Ibid. Article 25.

12 A secure Europe in a better world - European security strategy, Brusel, 12. prosince 2003 [online]. [cit. 13. 7. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ar00004.

13 Council Joint Action 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency, Official Journal of the European Union, 17. července 2004 [online]. [cit. 13. 7. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2004.245. 01. 0017.01.ENG & toc=OJ:L:2004:245:FULL.

14 Lisabonská smlouva pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství (2007/C 306/01), Úřední věstník Evropské unie, 17. prosince 2007 [online]. [cit. 13. 7. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:12007L/TXT.

Přijetí Lisabonské smlouvy bylo důležitým mezníkem v budování evropské obrany, neboť ze všech předchozích reformních smluv nejsilněji akcentovala obranný aspekt. Zároveň vytvořila řadu nových institucí a současně reorganizovala staré s cílem zefektivnit fungování ESDP jako celku. Dále přenesla na členské státy nové závazky a poskytla jim nové mechanismy spolupráce, čímž je posunula zase o krok dále ve spolupráci v obranných otázkách. Mezi nejvýznamnější změny patří přejmenování ESDP na CSDP, jenž se nově stává nedílnou součástí CFSP, zajišťující EU „operativní schopnost, která se opírá o civilní a vojenské prostředky", jež v případě potřeby EU „může použít pro mise vedené mimo území Unie k udržení míru, předcházení konfliktům a posílení mezinárodní bezpečnosti".[15] S cílem naplnit ambici a vytvořit předpoklady pro fungování EU jako globálního aktéra, akcentované již ve výše zmíněné Evropské bezpečnostní strategii, a současně personifikovat nově ustavenou CSDP, Lisabonská smlouva vytvořila pozici Vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku (*The High Representative of the Union for Foreign Affairs and Security Policy – HR/VP*), který je současně místopředsedou Evropské komise.[16] Vysokému představiteli asistuje nově vytvořený diplomatický sbor EU, Evropská služba vnější akce (*European External Action Service – EEAS*), jejíž součástí se stal také EUMS.[17] Lisabonská smlouva vytvořila i nový jednací formát Rady pro zahraniční věci (*Foreign Affairs Council – FAC*), kterému Vysoký představitel předsedá.[18] Dříve ustavené EDA se v textu Lisabonské smlouvy dostalo plného uznání i nových úkolů.[19] Jedním z nich je dohled nad implementací nově vytvořeného mechanismu Stále strukturované spolupráce (*Permanent Structured Cooperation – PESCO*) určené pro státy, jejichž vojenské schopnosti splňují přísnější kritéria a jsou ochotni v jejich zlepšování přijmout ještě tvrdší závazky s ohledem na vedení těch nejnáročnějších misí.[20] Vedle PESCO přinesla Lisabonská smlouva i ustanovení o vzájemné pomoci v případě ozbrojeného napadení; doložku solidarity pro případ, kdy některý členský stát se stal cílem teroristického útoku nebo obětí přírodní nebo člověkem způsobené pohromy; a také rozšířené ustanovení o posílené spolupráci zahrnující nově i CSDP.[21] Lisabonská smlouva také formalizovala a dále rozvedla tzv. Petersberské úkoly, v jejichž rámci může EU „použít civilní a vojenské prostředky," poskytované jednotlivými státy pro „společné akce v oblasti odzbrojení, humanitární a záchranné mise, poradní a pomocné mise ve vojenské oblasti, mise pro předcházení konfliktům a udržení míru, mise bojových sil k řešení

15 Ibid. Hlava III, Ustanovení o orgánech, Společná bezpečnostní a obranná politika, Oddíl 2, Ustanovení o společné bezpečnostní a obranné politice, Článek 28a, odstavec 1.

16 Ibid. Ustanovení o orgánech, Článek 9e.

17 Ibid. Ustanovení o orgánech, Společná bezpečnostní a obranná politika, Kapitola 2, Zvláštní ustanovení o společné zahraniční a bezpečnostní politice, Oddíl 1, Společná ustanovení, Článek 13a.

18 Ibid. Ustanovení o orgánech, Článek 9c; a Článek 9e.

19 Ibid. Ustanovení o orgánech, Společná bezpečnostní a obranná politika, Oddíl 2, Ustanovení o společné bezpečnostní a obranné politice, Článek 28a, odstavec 3; a Článek 28d, odstavec 1.

20 Ibid. Článek 28a, odstavec 6; a Článek 28e.

21 Ibid. Článek 28a, odstavec 7; Doložka solidarity, Hlava VII, Doložka solidarity, Článek 188r; a Posílená spolupráce, Článek 280d.

krizí, včetně misí pro prosazování míru a stabilizačních operací po ukončení konfliktů."[22] Konečně v rozhodovacím procesu v rámci CSDP Lisabonská smlouva potvrdila princip jednomyslnosti. Hlasování kvalifikovanou většinou se omezilo na dílčí mechanismy, jakým je například PESCO nebo jmenování Vysokého představitele.[23]

3 PROČ BUDOVÁNÍ EVROPSKÉ OBRANY V POSLEDNÍCH LETECH AKCELERUJE?

Snaha EU urychlit vytvoření evropské obrany je především reakcí na měnící se globální prostředí. Spojené státy v podobě Trumpovy administrativy dávají Evropanům jasně najevo, že obrana Evropy je primárně jejich záležitostí a že se Spojené státy nemusí v evropských záležitostech v případě krize nebo válečného konfliktu již napříště angažovat.[24] Z toho plynoucí postupné oslabovaní transatlantické vazby v rámci NATO, neukončená občanská válka na Ukrajině a snahy Putinova Ruska s využitím hybridních způsobů boje o obnovení studenoválečných pozic, teroristické útoky Islámského státu na evropské půdě, a konečně neoslabující migrační vlny, jsou jen některé z faktorů, které u Evropanů vyvolávají pocit ohrožení a stupňují tlak na změnu přístupu k obranné dimenzi EU.[25] Odchod Velké Británie z EU, která po řadu let byla hlavním odpůrcem myšlenky posilování evropské obrany, tento tlak jen umocňuje a současně vytváří vhodnou příležitost pro akceleraci celého procesu.[26] Nicméně výchozí podmínky Evropanů nejsou dobré. EU je jako celek po Spojených státech druhá na světě z hlediska výše výdajů na obranu, ale dosahuje jen 15% jejich vojenské efektivity.[27] Míra obranné spolupráce mezi členskými státy je nízká (více než 80% výdajů na investice a 90% výdajů na obranný výzkum se realizuje výlučně na národní úrovni) a členské státy nekoordinují plánování a pořízení nových zbraňových systémů, čímž přetrvává vysoká míra roztříštěnosti a duplicity (v Evropě je 178 různých zbraňových systémů oproti 30 ve Spojených státech).[28] Členské státy také nedostatečně investují do obranného výzkumu a vývoje, což ohrožuje technologický náskok a operační převahu zbraňových systémů nové generace (poměr souvisejících investic EU,

22 Ibid. Článek 28b, odstavec 1.

23 Ibid. Článek 28, odstavec 3; Článek 28e.

24 KOLÍN, Vilém, Česká republika a 'nová' Společná bezpečností a obranná politika EU: Čas zásadních rozhodnutí. *Vojenské rozhledy*. 2017; 26 (3), S. 69. ISSN 1210-3292.

25 Ibid. S. 69-70.

26 KOLÍN, Vilém, Stálá strukturovaná spolupráce (PESCO): nový pilíř v budování evropské obrany. *Vojenské rozhledy*. 2018; 27(4), S. 22. ISSN 1210-3292.

27 SOLANA, Javier, European Defence, one achievement at a time. *EDM: European Defence Matters*. 2019; 17, S. 7. ISSN 1977-5059.

28 Sdělení Komise Evropskému parlamentu, Radě, Evropskému Hospodářskému a sociálnímu výboru a Výboru regionů: Vznik Evropského obranného fondu, COM(2017) 295, Brusel, 7. června 2017. S. 3. [online]. [cit. 20. 7. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0295.

členských států EDA, vůči Spojeným státům je téměř 1:8),[29] a celkově na obranu vydávají málo finančních prostředků (v průměru 1,4% HDP v roce 2017 za všechny členské státy EDA ve srovnání s 3,6% HDP ve stejném roce ve Spojených státech).[30] Výsledkem je nízká interoperabilita, technologická zaostalost a neschopnost ozbrojené síly účinně nasadit. Není proto překvapení, že s ohledem na horšící se globální prostředí a svízelnou situaci Evropanů, se evropská obrana v posledních letech stala jednou z hlavních priorit EU, zejména pak Evropské komise Jean-Clauda Junckera, který ji vedl v letech 2014 až 2019.

V tomto kontextu přijala EU v roce 2016 novou Globální strategii zahraniční a bezpečnostní politiky (*Global Strategy for the European Union's Foreign And Security Policy – EUGS*) nazvanou Sdílená vize, společný postup: silnější Evropa (*Shared Vision, Common Action: A Stronger Europe*), ve které stanovila rozvoj strategické autonomie za základní cíl EU.[31] Takřka současně podepsala EU s NATO společnou deklaraci (*EU-NATO Joint Declaration*) o strategickém partnerství mezi oběma organizacemi[32] a jen o pár měsíců později byl přijat Implementační plán o bezpečnosti a obraně (*Implementation Plan on Security and Defence*), který stanovil nové ambice EU v návaznosti na dříve přijatou EUGS.[33] Ve stejné době představila Evropská komise Evropský obranný akční plán (*European Defence Action Plan – EDAP*), ve kterém navrhla vytvoření Evropského obranného fondu (*European Defence Fund – EDF*) na podporu evropského obranného výzkumu a vývoje.[34]. V roce 2017 pak členské státy rozhodly o ustavení Stále strukturované spolupráce (*Permanent Structured Cooperation – PESCO*), která z obavy o vytvoření vícerychlostní

29 Poměr vypočítán s přihlédnutím k celkovým výdajům na obranný výzkum a vývoj členských států EDA a Spojených států v roce 2016. Ty za členské státy EDA dosáhly 8,8 mld. euro a za Spojené státy 78,1 mld. dolarů. Použitý směnný kurz pro rok 2016: 1 EUR : 1,11 USD. *Defence Data 2016-2017, Key Findings and Analysis*. Brusel: European Defence Agency, 2018. S. 10. ISBN 978-92-95075-42-9; a Fact Sheet: Government Expenditures on Defense Research and Development by the United States and Other OECD Countries, Congressional Research Service, R45441, Version 2, 19. prosince 2018, S. 1 [online]. [cit. 20. 7. 2019]. Dostupné z https://crsreports.congress.gov/search/#/?termsToSearch=R45441 & orderBy=Relevance.

30 Ibid. *Defence Data 2016-2017, Key Findings and Analysis*. S. 4.; a Defence Expenditure of NATO Countries (2010-2017), NATO Communique PR/CP(2018)16, Brusel, 15. března 2018. S. 3 [online]. [cit. 20. 7. 2019]. Dostupné z https://www.nato.int/cps/en/natohq/news_152830.htm.

31 Shared Vision, Common Action: A Stronger Europe: Global Strategy for the European Union's Foreign And Security Policy, Brusel, 16. června 2016. S. 4 [online]. [cit. 20. 7. 2019]. Dostupné z https://eeas.europa.eu/regions/western-europe/17304/global-strategy-european-unions-foreign-and-security-policy_en.

32 Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Altlantic Treaty Organization, Varšava, 8. července 2016. [online]. [cit. 20. 7. 2019]. Dostupné z https://www.consilium.europa.eu/en/press/press-releases/2016/07/08/eu-nato-joint-declaration.

33 Implementation Plan on Security and Defence, 14392/16, Council of the European Union, Brusel, 14. listopadu 2016 [online]. [cit. 20. 7. 2019]. Dostupné z https://eeas.europa.eu/regions/western-europe/17304/global-strategy-european-unions-foreign-and-security-policy_en.

34 Sdělení Komise Evropskému parlamentu, Radě, Evropskému Hospodářskému a sociálnímu výboru a Výboru regionů: Evropský obranný akční plán, COM(2016) 950, Evropská komise, 30. listopadu 2016. [online]. [cit. 20. 7. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52016DC0950.

Evropy v obranné spolupráci čekala na svoje spuštění od schválení Lisabonské smlouvy.[35] Zatím posledním důležitým milníkem bylo vytvoření nového Ředitelství Evropské komise pro Obranný průmysl a vesmír (*DG Defence Industry and Space*), které se zformovalo v roce 2019 v rámci nové Evropské komise pod vedením Ursuly von der Leyen.[36]

4 JAKÉ JSOU HLAVNÍ INSTITUCE ODPOVĚDNÉ ZA EVROPSKOU OBRANU?

4.1 Evropská rada a její součásti

Obrana státu a jeho obyvatel zůstává jednou z výlučných pravomocí státu, jeho suverenitou, kterou si stát brání individuálně nebo kolektivně za pomoci ostatních států, spojenců. Není proto žádným překvapením, že hlavní institucí, jenž řeší otázky evropské obrany, je Evropská rada: kolektivní orgán, který se schází na úrovni prezidentů a předsedů vlád a formuluje obecné politické zadání a priority pro EU jako celek.[37] Jednání Evropské rady se účastní i předseda Evropské komise a Předseda Rady (*President of the European Council*), volený na období dvou a půl roku, který jednání řídí.[38] Jak již bylo zmíněno dříve, rozhodování Evropské rady v rámci CSDP je ve valné většině případů jednomyslné, konsensuální, respektující primární odpovědnost státu za otázku obrany. Evropská rada nevytváří evropskou legislativu, ale přijímá rozhodnutí a doporučení, které jsou pro členské státy politicky závazné.[39] O úroveň níže stojí již zmíněný FAC složený z ministrů zahraničí, ale zasedající i ve formátu ministrů obrany.[40] FAC spolu s Evropským parlamentem vykonává legislativní a rozpočtové funkce a předsedá mu Vysoký představitel.[41]

Denní činnost Rady podporuje Výbor stálých zástupců II (*COREPER II - Comité des représentants permanents*), kterému předsedá zástupce členské země vykonávající

35 Ref. 26. S. 21-22.

36 European Commission 2019 – 2024, Allocation of portfolios and supporting services, Brusel, 7. listopadu 2019. [online]. [cit. 9. 11. 2019]. Dostupné z https://ec.europa.eu/commission/towards-new-commission_en.

37 Obecné informace k Evropské radě a aktuálním tématům jsou dostupné na https://www.consilium.europa.eu/en/european-council/.

38 Ref. 4. S. 46.

39 Ibid.

40 Obecné informace k Radě pro zahraniční věci a aktuálním tématům jsou dostupné na https://www.consilium.europa.eu/en/council-eu/configurations/fac/.

41 Ref. 4. S. 50-51.

v danou dobu předsednictví Radě.[42] COREPER II je hlavním přípravným výborem Rady a zasedá na úrovni velvyslanců členských států při EU.[43] Vedle COREPER II existuje již zmíněné PSC, kterému předsedá zástupce EEAS.[44] PSC zasedá na úrovni velvyslanců členských státu odpovědných za CSDP a podobně jako COREPER II je přípravným výborem pro Radu, odpovědným primárně za monitorování mezinárodní situace, formulaci doporučení ohledně strategických přístupů a politických řešení, které předkládá Radě. Dále vykonává politickou kontrolu a strategické řízení nad operacemi k řešení krizí.[45] PSC spolupracuje s Politicko-vojenskou skupinou (*PMG – Politico-Military Group*), která se zabývá politickými aspekty vojenských a vojensko-civilních otázek včetně těch souvisejících s operacemi a misemi EU, a připravuje pro PSC související doporučení a monitoruje jejich implementaci.[46] PMG je také odpovědné za vztahy s třetími zeměmi včetně vztahů s NATO. PMG předsedá zástupce Vysokého představitele.[47] Vedle PMG existuje Výbor pro civilní aspekty krizového řízení (*Committee for Civilian Aspects of Crisis Management – CIVCOM*), jenž PSC poskytuje související informace.[48] Již dříve zmíněný EUMC je nejvyšším vojenským orgánem v rámci Rady a sestává se z náčelníků generálních štábů členských států, kteří jsou po většinu roku zastoupeni stálými zástupci.[49] EUMC je podobně jako PMG a CIVCOM poradním orgánem PSC, kterému poskytuje vojenský názor a doporučení.[50] Dalším důležitým orgánem je také dříve zmíněný EUMS,[51] který podléhá Vysokému představiteli a je organizačně součástí EEAS, kterou jako celek Vysoký představitel řídí.[52] EUMS pracuje pod vedením EUMC a jako integrální součást EEAS a tzv. komplexního přístupu (*Comprehensive Approach*) koordinuje vojenskou součást EEAS, zejména pak operace a mise EU a budování vojenských schopností.[53] EUMS také spra-

42 Obecné informace ke COREPER II jsou dostupné na https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/coreper-ii/.

43 Ref. 4. S. 52.

44 Obecné informace k Politickému a bezpečnostnímu výboru jsou dostupné na https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/political-security-committee/.

45 Ref. 4. S. 52-53.

46 Obecné informace k Politicko-vojenské skupině jsou dostupné na https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/politico-military-group/.

47 Ref. 4. S. 53-54.

48 Ibid. S. 54. Obecné informace k Výboru pro civilní aspekty krizového řízení jsou dostupné na https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/committee-civilian-aspects-crisis-management/.

49 Obecné informace k Vojenskému výboru a aktuálním tématům jsou dostupné na https://eeas.europa.eu/headquarters/headQuarters-homepage/5428/european-union-military-committee-eumc_en/.

50 Ref. 4. S. 53.

51 Obecné informace k Vojenskému štábu a aktuálním tématům jsou dostupné na https://eeas.europa.eu/headquarters/headquarters-homepage_en/5436/The%20European%20Union%20Military%20Staff%20(EUMS).

52 Ref. 4. S. 70.

53 Společné sdělení Evropskému parlamentu a Radě, Komplexní přístup EU vůči vnějším konfliktům a krizím, JOIN(2013) 30, Brusel, 11. prosince 2013. [online]. [cit. 27. 7. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52013JC0030; a ref. 4. S. 55, 70.

vuje Evropské operační centrum (*EU Operations Centre – OPSCEN*),[54] které bylo aktivováno FAC v roce 2012 na podporu misí CSDP.[55] V neposlední řadě je třeba zmínit Útvar schopnosti civilního plánování a provádění (*The Civilian Planning and Conduct Capability – CPCC*), který je odpovědný za civilní mise CSDP včetně jejich plánování a realizace a podobně jako EUMS je součástí EEAS.[56] CPCC funguje pod politickou kontrolou PSC a vede ho Vysoký představitel.[57] Podpora vojenských misí pak připadá na Útvar schopnosti vojenského plánování a provádění (*The Military Planning and Conduct Capability – MPCC*), který je součástí EUMS, informuje však i EUMC, a podobně jako CPCC se zodpovídá PSC.[58]

4.2 Evropská obranná agentura a ostatní agentury Rady

EDA je podobně jako Evropská rada součástí mezivládního přístupu. Veškeré aktivity Agentury jsou rozhodovány a financovány členskými státy (nikoliv z rozpočtu EU).[59] Přijatá rozhodnutí mají politickou nikoliv právní závaznost a navrhovaná doporučení slouží jako vodítko pro členské státy, nikoliv jako právně vynutitelné akty. Členy EDA jsou všechny členské státy s výjimkou Dánska, které v rámci Maastrichtské smlouvy získalo *opt-out* v otázkách evropské obrany.[60] V čele Agentury stojí Vysoký představitel. Denní chod EDA řídí Výkonný ředitel, přičemž členské státy dohlížejí na implementaci dohodnutých aktivit skrze Řídící výbor, který se pravidelně schází (zpravidla dvakrát ročně) v různých formátech podle zaměření agendy na úrovni Ministrů obrany, Národních ředitelů pro vyzbrojování, Ředitelů pro schopnosti a Ředitelů pro výzkum a vývoj.[61]

EDA byla založena v roce 2004 formou Společné akce (*Joint Action*), nástrojem vytvořeným Maastrichtskou smlouvou, s cílem podporovat Radu a členské státy v jejich úsilí o zlepšení obranných schopností EU v oblasti zvládání krizí a podpoře ESDP (dnes

54 Ibid. Ref. 4. S. 70.

55 Obecné informace k Evropskému operačnímu centru jsou dostupné na https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/5392/csdp-structure-instruments-and-agencies_en.

56 Obecné informace k Útvaru schopnosti civilního plánování a provádění jsou dostupné na https://eeas.europa.eu/topics/military-and-civilian-missions-and-operations_en/5438/The%20Civilian%20Planning%20and%20Conduct%20Capability%20(CPCC).

57 Ref. 4. S. 71.

58 Factsheet: The Military Planning and Conduct Capability (MPCC), European Union External Action Service, listopad 2018 [online]. [cit. 27. 7. 2019]. Dostupné z https://eeas.europa.eu/sites/eeas/files/mpcc_factsheet_november_2018.pdf.

59 Obecné informace k Evropské obranné agentuře a aktuálním tématům jsou dostupné na https://www.eda.europa.eu/. Viz také KOLÍN, Vilém, Evropská obranná agentura po třech letech. *Obrana a strategie*. 2007; 7(4), S. 73-85. ISSN 1214-6463; a KOLÍN, Vilém, Evropská obranná agentura v šesti letech. *Obrana a strategie*. 2010; 10(2), S. 21-44. ISSN 1214-6463.

60 Ref. 4. S. 165. Obecné informace k *opt-outs* Dánska v rámci EU jsou dostupné na https://english.eu.dk/en/denmark_eu/danishoptouts.

61 Ibid. Ref. 4. S. 164.

CSDP).[62] Jejím původním posláním bylo rozvíjet obranné schopnosti, podporovat obranný výzkum a technologie, posílit spolupráci ve vyzbrojování, a vytvářet Evropský trh s obranným materiálem (*European Defence Equipment Market – EDEM*) za současného posilování Evropské obranné technologické a průmyslové základny (*European Defence, Technological and Industrial Base – EDTIB*).[63] Třebaže působnost EDA byla dále upravena Lisabonskou smlouvou, která mimo jiné přisoudila Agentuře roli v PESCO, její hlavní poslání v budování obranných schopností zůstalo beze změny.[64] V roce 2018 měla EDA sídlící v Bruselu ve svém portfoliu 97 projektů v oblastech obranného výzkumu a rozvoje schopností, 17 dalších programů a více než 190 různorodých aktivit jdoucích od harmonizace pravidel pro urychlení přesunu vojsk přes hranice členských států, přes školení expertů v kybernetické bezpečnosti, po definici klíčových strategických aktivit.[65] Objem prostředků investovaných členskými státy do obranného výzkumu v letech 2004 až 2017 prostřednictvím EDA dosáhl objemu 1 mld. euro.[66]

V roce 2017 Řídící výbor na úrovni ministrů obrany schválil Dlouhodobou revizi (*Long Term Review – LTR*), která do značné míry redefinovala původní zaměření Agentury. Ta se dle LTR soustředí primárně na tři úkoly: stává se hlavním nástrojem EU pro plánování obranných schopností a stanovení souvisejících priorit; stejně tak jako hlavním fórem a koordinátorem životního cyklu rozvoje obranných schopností (od konceptu, přes vývoj, výrobu, po údržbu, modernizaci a nahrazení novým systémem); a funguje jako hlavní prostředník mezi členskými státy a ostatními institucemi EU.[67]

Vedle EDA, která je Agenturou Rady, existují ještě dvě další agentury spravované Radou: Evropský institut strategických studií (*European Union Institute for Security Studies – EU ISS*) sídlící v Paříži a Evropské satelitní centrum (*European Union Satellite Centre – SatCen*) se sídlem ve španělském Torrejón de Ardoz. První z nich se od doby svého vzniku v roce 2002 zaměřuje na analýzu zahraniční, bezpečnostní a obranné politiky, především pak na otázky související s CFSP a CSDP.[68] EU ISS je financován z příspěvků členských států a řízen představenstvem, kterému předsedá Vysoký představitel. PSC

---

62 Council Joint Action 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency, Official Journal of the European Union, 17. července 2004 [online]. [cit. 27. 7. 2019]. Dostupné z https://op.europa.eu/en/publication-detail/-/publication/572178ea-442e-4810-a01d-58e30c486f47/language-en.

63 Ibid. Článek 5, odstavec 3.

64 Ref. 14. Hlava III, Ustanovení o orgánech, Společná bezpečnostní a obranná politika, Oddíl 2, Ustanovení o společné bezpečnostní a obranné politice, Článek 28a; Článek 28d; a Protokol o Stálé strukturované spolupráci stanovené článkem 28a Smlouvy o Evropské Unii.

65 Factsheet: EDA at Glance, European Defence Agency, 26. dubna 2019 [online]. [cit. 3. 8. 2019]. Dostupné z https://www.eda.europa.eu/info-hub/publications/publication-details/pub/infographic-eda-at-a-glance.

66 Ref. 4. S. 165.

67 Long Term Review of the Agency – Conclusions and Recommendations: A Reinforced Agency to Enable Member States to Deliver on Defence Capabilities, European Defence Agency, 18. května 2017 [online]. [cit. 3. 8. 2019]. Dostupné z https://www.eda.europa.eu/docs/default-source/documents/ltr-conclusions-and-recommendations.pdf.

68 Obecné informace k Evropskému institutu strategických studií a aktuálním tématům jsou dostupné na https://www.iss.europa.eu/.

vykonává nad Institutem politický dohled, avšak nijak neomezuje jeho institucionální nebo akademickou svobodu.[69] Výstupem práce EU ISS jsou primárně odborné studie, komentáře a články, které se těší velké pozornosti ze strany odborné veřejnosti. Druhou ze zmíněných agentur je SatCen založený v roce 1992 s cílem poskytovat produkty a služby v oblasti družicového snímkování zemského povrchu.[70] Jeho hlavním zákazníkem jsou instituce a organizace EU jako Evropská komise, Rada a EEAS v kontextu implementace CFSP a CSDP, ale i členské státy a mezinárodní organizace. SatCen, který byl v roce 2002 přeměněn na agenturu Rady financovanou členskými státy, je podobně jako EU ISS postaven pod politický dohled PSC a Vysokého představitele.[71] Pro úplnost je v rámci institucí Rady třeba zmínit i Evropskou bezpečnostní a obrannou školu (*European Security and Defence College – ESDC*), jejíž hlavní náplní je od doby svého vzniku v roce 2005 poskytovat vzdělávání v oblasti CSDP.[72] ESDC se sídlem v Bruselu dnes v různých členských státech EU realizuje přes 40 kurzů zaměřených na různé aspekty CSDP,[73] například zvládání krizí, kybernetickou bezpečnost, hybridní hrozby nebo klimatické změny.

4.3 Evropská komise

Evropská komise není tradičním aktérem na poli budování evropské obrany. Podle Lisabonské smlouvy může v rámci CFSP podpořit iniciativu Vysokého představitele, který je zároveň místopředsedou Evropské komise, a v některých případech připravit i společný návrh.[74] Nicméně nemá v rámci CFSP právo samostatné (legislativní) iniciativy tak, jako tomu je v jiných oblastech, například v zemědělské nebo v obchodní politice.[75] Tím je zachována výlučnost mezivládního přístupu k CFSP a tím i CSDP, která je plně respektována v kontextu Evropské rady a institucí Rady popsaných výše.[76] Nicméně Evropská komise se již paralelně se vznikem EDA angažovala v tvorbě EDEM a EDTIB a postupně

69 CSDP structure, instruments, and agencies: European Union Institute for Security Studies, European Union External Action Service, 8. července 2016 [online]. [cit. 10. 8. 2019]. Dostupné z https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/5392/csdp-structure-instruments-and-agencies_en.

70 Obecné informace k Evropskému satelitnímu centru a aktuálním tématům jsou dostupné na https://www.satcen.europa.eu/.

71 CSDP structure, instruments, and agencies: European Union Satellite Centre, European Union External Action Service, 8. července 2016 [online]. [cit. 10. 8. 2019]. Dostupné z https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp/5392/csdp-structure-instruments-and-agencies_en.

72 Obecné informace k Evropské bezpečnostní a obranné škole a aktuálním tématům jsou dostupné na https://esdc.europa.eu/.

73 Ref. 4. S. 219.

74 Ref. 14. Hlava III, Ustanovení o orgánech, Obecná ustanovení o vnější činnosti, Kapitola 1, Obecná ustanovení o vnější činnosti Unie, Článek 10b, odstavec 2.

75 Ibid. Společná zahraniční a bezpečnostní politika, Kapitola 2, Zvláštní ustanovení o Společné zahraniční a bezpečnostní politice, Oddíl 1, Společná ustanovení, Článek 11, odstavec 1.

76 Více k sekundární roli Evropské komise v rámci CSDP viz ref. 4. S. 55-57.

přebrala hlavní iniciativu od EDA na poli posilování konkurenceschopnosti evropského obranného průmyslu a větší integrace obranného trhu EU. Právní báze, na kterou se Evropská komise v posledních letech odkazuje v kontextu EDF, je článek 173 Smlouvy o fungování Evropské unie, který hovoří o nutnosti zajistit „podmínky nezbytné pro konkurenceschopnost průmyslu Unie“.[77]

V tomto kontextu byly již v roce 2009 schváleny dvě nové směrnice, tvořící tzv. obranný balíček (*Defence Package*), které Evropská komise připravila: Směrnice o transferech produktů pro obranné účely 2009/43/EC mající za cíl pomocí nového licenčního mechanismu zjednodušit pohyb zboží k obranným účelům mezi členskými státy EU; a Směrnice o zadávání zakázek v oblasti obrany a bezpečnosti 2009/81/EC, jež stanovila nová pravidla pro obranné zakázky, které jsou z povahy věci komplexní a citlivé, a zjednodušila dosavadní postupy s cílem zvýšit transparentnost a otevřít tradičně velmi uzavřené obranné trhy členských států zahraniční konkurenci.[78] Na to navázalo několik koncepčních dokumentů: Směrem ke konkurenceschopnějšímu a účinnějšímu odvětví obrany a bezpečnosti z roku 2013 (*Towards a More Competitive and Efficient Defence and Security Sector*),[79] Nový program pro evropskou obranu z roku 2014 (*New Deal for European Defence*),[80] Evropský obranný akční plán z roku 2016 (*European Defence Action Plan – EDAP*),[81] Diskusní dokument o budoucnosti evropské obrany z roku 2017 (*Reflection Paper on the Future of European Defence*),[82] a konečně ze stejného roku Spuštění Evropského obranného fondu (*Launching the European Defence Fund*).[83] Jak je z těchto dokumentů patrné, Evropská komise se snaží finančně stimulovat a do značné míry i regulovat celé

77 Smlouva o fungování Evropské unie (Konsolidované znění) (C 326/47), Úřední věstník Evropské unie, 26. října 2012 [online]. [cit. 17. 8. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

78 Směrnice Evropského parlamentu a Rady 2009/43/ES ze dne 6. května 2009 o zjednodušení podmínek transferů produktů pro obranné účely uvnitř Společenství, Úřední věstník Evropské unie, 10. června 2009 [online]. [cit. 17. 8. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0043; Směrnice Evropského parlamentu a Rady 2009/81/ES ze dne 13. července 2009 o koordinaci postupů při zadávání některých zakázek na stavební práce, dodávky a služby zadavateli v oblasti obrany a bezpečnosti a o změně směrnic 2004/17/ES a 2004/18/ES, Úřední věstník Evropské unie, 20. srpna 2009 [online]. [cit. 17. 8. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0081.

79 Sdělení Komise Evropskému parlamentu, Radě, Evropskému Hospodářskému a sociálnímu výboru a Výboru regionů: Směrem ke konkurenceschopnějšímu a účinnějšímu odvětví obrany a bezpečnosti, COM(2013) 542, Brusel, 24. července 2013 [online]. [cit. 17. 8. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52013DC0542.

80 Sdělení Komise Evropskému parlamentu, Radě, Evropskému Hospodářskému a sociálnímu výboru a Výboru regionů: Nový program pro evropskou obranu, Prováděcí harmonogram ke sdělení COM(2013) 542; a Směrem ke konkurenceschopnějšímu a účinnějšímu odvětví obrany a bezpečnosti, COM(2014) 387, Brusel, 24. června 2014 [online]. [cit. 17. 8. 2019]. Dostupné z https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0387.

81 Ref. 34.

82 Diskusní dokument o budoucnosti evropské obrany, Evropská komise, COM(2017) 315, Brusel, 7. června 2017 [online]. [cit. 17. 8. 2019]. Dostupné z https://ec.europa.eu/commission/publications/reflection-paper-future-european-defence_en.

83 Ref. 28.

spektrum otázek související s evropskou obranou: od obranných zakázek, transferu zboží k obranným účelům, přes problematiku obranného průmyslu včetně kompetencí (*skills*) průmyslu, vlastnické struktury firem a zapojení malých a středních podniků do dodavatelských řetězců zahraničních firem, k zajištění dodávek vzácných surovin a podpoře obranného výzkumu. To má svoji nespornou logiku. Jak jeden z těchto dokumentů říká: „Bez trvalého investování do obrany hrozí evropskému průmyslu, že nebude technologicky s to vytvořit novou generaci zásadních obranných schopností. V konečném důsledku to ovlivní strategickou autonomii Unie a její schopnost jednat jako subjekt zajišťující bezpečnost.“[84] Cílem snažení Evropské komise není nahradit roli členských států (obrana zůstává jejich výlučnou pravomocí a Evropská komise nemá pravomoc do ní zasahovat), ale pomocí pákového efektu (*leverage effect*)[85] využít všech dostupných evropských nástrojů k podpoře obranné spolupráce mezi členskými státy, a především pak mezi jejich obranným průmyslem, který má „strategický význam pro bezpečnost Evropy“.[86]

Rostoucí zapojení Evropské komise do problematiky evropské obrany kulminovalo vytvořením již zmíněného *DG Defence Industry and Space*, kterým se realizovalo dlouho očekávané (neformální) rozdělení agendy evropské obrany mezi komunitarní (nadnárodní) a mezivládní část, kdy na straně jedné ta mezivládní (v rámci Evropské rady a jí podřízených institucí) formuluje cíle a priority budování evropské obrany, a na straně druhé ta komunitární část (Evropská komise a ji podřízené nově vytvořené *DG Defence Industry and Space*) připravuje související evropskou legislativu a řídí finanční nástroje na podporu cílů a priorit formulovaných Evropskou radou. Toto rozdělení jen dále podtrhuje mnohotvárnost přístupu EU k budování evropské obrany, které, jak bylo řečeno na začátku, brání jejímu snadnému ohraničení, a které v konečném důsledku přidává i na komplexnosti její implementace.

4.4 Evropský parlament

Podobně jako pro Evropskou komisi i pro Evropský parlament stála evropská obrana dlouho na okraji zájmu. S Lisabonskou smlouvou získal Evropský parlament spolu s Radou rozpočtové a legislativní pravomoci a funkci politické kontroly.[87] V rámci CSDP má právo klást Radě a Vysokému představiteli dotazy nebo podávat doporučení.[88] Dvakrát ročně pak pořádá rozpravu o pokroku v rámci CFSP a CSDP a vypracovává související zprávy. Vysoký představitel pak s Evropským parlamentem pravidelně konzultuje otázky související s mezinárodní situací a realizací CSDP. Parlament k nim organizuje diskuse,

84 Ref. 34. S. 3.

85 Ibid. S. 4.

86 Ibid. S. 3.

87 Ref. 14. Hlava III, Ustanovení o orgánech, Společná bezpečnostní a obranná politika, Kapitola 2, Zvláštní ustanovení o společné zahraniční a bezpečnostní politice, Oddíl 1, Společná ustanovení, Článek 41.

88 Ibid. Článek 36.

slyšení a semináře, které se často uskutečňují pod hlavičkou Podvýboru pro obranu a bezpečnost (*Subcommittee on Security and Defence – SEDE*).[89] Evropský parlament ve spolupráci s Radou každoročně také dohlíží na implementaci EUGS a v rámci své role v legislativním procesu EU (rovnocenné s Evropskou komisí) se podílí na tvorbě řady důležitých iniciativ souvisejících s evropskou obranou. Spolu s Evropskou komisí se například zasadil o vytvoření legislativního rámce pro EDF.

Druhá část článku bude uveřejněna ve VR 4/2020.

Autor: ***PhDr. Vilém Kolín, Ph.D., MGS,*** *narozen 1974. Titul Ph.D. získal v oboru Mezinárodní vztahy na Fakultě sociálních věd Univerzity Karlovy v Praze. Dále studoval na Joseph Korbel School of International Studies Univerzity v Denveru v USA. V letech 2005-2006 pracoval jako vědecký pracovník v Ústavu strategických studií Univerzity obrany v Brně, v letech 2006-2010 na Sekci vyzbrojování Ministerstva obrany. Od roku 2010 pracuje v Evropské obranné agentuře (EDA) v Bruselu. Zaměřuje se na problematiku Společné obranné a bezpečnostní politiky EU, obranného výzkumu, průmyslu a trhu a realizace mezinárodních projektů a programů.*

Jak citovat: KOLÍN Vilém. Společná bezpečnostní a obranná politika EU v kostce – část první. *Vojenské rozhledy*. 2020, 29 (3), 087-101. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz.

[89] Common Security and Defence Policy, European Parliament, duben 2019 [online]. [cit. 24. 8. 2019]. Dostupné z https://www.europarl.europa.eu/factsheets/en/sheet/159/common-security-and-defence-policy. Více k roli Evropského parlamentu v rámci CSDP viz ref. 4. S. 58-61.

Otiskli jsme před 100 lety

Předkládáme vám příspěvky z rubriky „Prameny k dějinám našeho vojska“ publikované v našem časopise č. 3/1920. Jedná se o rubriku, kde redakce časopisu pravidelně soustřeďovala příspěvky pro případné bádání.

Tento i další historické články si můžete prohlédnout, přečíst nebo stáhnout na webových stránkách našeho časopisu www.vojenskerozhledy.cz v nabídce archivu.

Redakce

PRAMENY K DĚJINÁM NAŠEHO VOJSKA.

Zborov.

(„Přerod“, roč. I., čís. 16., str. 2.)

Nastoupení ruského revolučního vojska je zahájeno. Dobrovolníkům československé brigády připadl čestný úkol v prvých řadách ve společném rozmachu svobodné armády zúčastniti se boje pro zabezpečení toho, čeho dobyla revoluce.

Dobrovolníci, s nadšením a vděčností přijali jsme zprávy o vašem hrdinství v tak rozhodné chvíli pro Rusko i pro nás. Pomněte, že všechen ujařmený národ s nadějí a vírou obrací své zraky na vás, volné v svojich činech syny, a očekává od vás, že mu přinesete osvobození z rakousko-uherského jha. Jsme hrdi u vědomí, že potomci husitů, bojovavších ve jménu svobody, spravedlnosti a národní svéprávnosti, vykonali a vykonají svou povinnost vůči národu, demokracii a lidstvu.

A vy, ostatní krajané, které osud zanesl do bratrské země, pomněte, že národ vás volá k hrdinským činům, že vy všichni, chcete-li býti hodnými jména svých otců, jste povinni zúčastniti se ve společném boji za svobodu a demokracii!

T. G. Masaryk.

*

253

Zpráva ze stanu vrchního velitele ze dne 20. června (3. července).

Ve směru na Zločov náš nástup pokračuje úspěšně. 19. června (2. července) okolo 15. hodiny (3. hod. odp.) po krutém a úporném boji zarajský pluk opanoval vesnici Przesowce a chrabrá vojska čtvrté finské divise a československé brigády opanovala silně opevněné nepřátelské posice na výšinách západně a jihozápadně vesnice Zborova a opevněnou vesnici Koršilov, prorvavše tři řady nepřátelských zákopů. Nepřítel odešel za řeku Malou Strypu.

Finská divise zajala 1560 důstojníků a mužstva, 4 zákopní děla, 9 strojních pušek a 1 minomet. Československá brigáda zajala 62 důstojníky, 3150 vojáků, 15 děl a mnoho strojních pušek, z nichž většina byla obrácena proti nepříteli. Obsazeny byly nepřátelské posice na západ od Josefovky.

Celkem v bojích 19. června (2. července) ve směru na Zločov bylo zajato 6300 důstojníků a vojáků, 21 děl, 16 strojních pušek a několik minometů. Zajatci stále přicházejí.

Na jihozápad od Břežan jdou boje s menším napětím. V bojích 18. června (1. července) v uvedeném okrsku bylo zajato 53 důstojníků a 2200 vojáků. Na ostatní frontě střelba.

*

Zpráva vlastního dopisovatele čas. „Russkoje Slovo".

Z fronty dne 19. června (2. července).

Největšího úspěchu dosáhla naše vojska (v neděli) v okrsku vesnice Koňuch. Tam náš úder padl na armádní sbor smutně známého generála Hoffmana (velitele 19. divise české — pozn. red.), pověstného v rakouské armádě svou smůlou. Kdykoliv jsme v této válce zahajovali nástup, generál Hoffman byl nejlepším dodavatelem zajatců. 81. český pluk, který se nám vydal celý i s plukovníkem Siegerem, byl pod vrchním velením Hoffmanovým. O vzdání tohoto pluku vypravují mezi jiným tuto podrobnost: Když počala naše dělostřelecká příprava, Češi se poskrývali do hlubokých děr a potom poslali do našich zákopů posly s prohlášením, aby Rusové netratili mnoho nábojů na jejich posice, protože Češi jen čekají na útok, aby se nám vzdali do zajetí. A skutečně Češi dodrželi slovo: bez nejmenšího odporu složili zbraně.

Podle zpráv, obdržených v polním stanu generála Gutora v 11 hodin v noci, jeden ze slavných československých pluků, překonav řadu nepřátelských opevnění, ukořistil 20 děl různého kalibru. Druhý náš pluk dobyl dvou děl.

*

Prof. Masaryk Československé střelecké brigádě.

Bratří!

Svou husitskou chrabrostí zjednali jste si uznání Ruska a celého spojeneckého světa; dokázali jste přátelům i nepřátelům, že náš národ je navždy rozhodnut domoci se své národní a politické samostatnosti. Vaše činy na bojišti dávají pravý smysl požadavkům našich poslanců ve vídeňském parlamentě. Vy jste živý protest proti protislovanskému a protiromanskému Rakousku-Uhersku a proti věrolomné dynastii, spojivší se proti právu, úmluvám a slibům s Němci a Maďary v prvé řadě proti Čechům a Slovákům. Vykořenili jsme všichni poslední zbytky důvěry v dynastii a státníky, kteří se otrocky poddali panskému všeněmectví.

Vzpomínáme vděčně bratří, kteří padli v boji za svobodu a demokracii našeho a celého slovanského národa; vzpomínáme jich v zármutku, ale hroznější je osud těch tisíců mučedníků, které katanská mstivost Vídně a Budapešti vám odpravila doma.

254

Nezapomeneme nikdy těchto obětí. Nezapomeneme těch, kteří trpí v rakouských žalářích, nezapomeneme těch, které rakouské vojenské a civilní úřady stále a krutě pronásledují. Komedie s neúplnou amnestií na splátky nás nezmýlí.

Bratří! Jsme s Vámi spojeni v horoucím úsilí a neúnavné práci pro samostatnost našeho národa; jsme s vámi za jedno v mužném odhodlání přinést každou oběť za uskutečnění našich národních ideálů — svobodné, nezávislé vlasti v svobodné, nezávislé Evropě. Pryč každá nadvláda národu a třídě, pryč pruský militarism, pryč Habsburkové a jejich násilnický stát, živořící z milosti Berlína, jako předvoj pangermanského světového panství!

Čechové, Slováci, vpřed! T. G. Masaryk.

*

Odpověď Masarykova na pozdrav vojska u příležitosti vítězství u Zborova.

Drahým vojínům a důstojníkům našeho vojska srdečné díky. My všichni provázíme jich nastoupení s blahoslovením. Víme, že splní svoji povinnost vůči vlasti. Oni jsou nejen chrabří, ale také ukázněni, jejich oddanost společné věci je nám všem příkladem. Ať žije svobodná Rus! Ať žije svobodný československý národ! Masaryk.

*

Prof. Masaryk ministru vojenství Kerenskému.

Blahopřejeme Vám k postupu, jedinému správnému prostředku boje s nepřítelem. Jsme rádi i tomu, že naše dobrovolnická vojska se zúčastnila tohoto slavného a zodpovědného činu ruské armády.

*

Prof. Masaryk generálu Brusilovovi.

Blahopřejeme ve Vaší osobě ruské armádě k vítězství. Jsme šťastni a děkujeme Vám, že jste naše části uznali za hodné účastniti se tohoto slavného a pro Rusko i Slovany významného činu. V Rusku dlící ostatní členové našeho národa jsou hotovi připojiti se ke svým druhům — hrdinům v boji, a doufáme, že budete nás podporovati v uskutečnění naší tužby.

*

Zpráva vlastního dopisovatele „Ruského Invalidy".

Z fronty ze dne 24. června (17. července).

Ministr Kerenský navštívil vojska, která se účastnila prvních bojů na zločevském směru.

Zástupce českoslov. brigády, která měla 18. a 19. července (1. a 2. července) ohromný úspěch, prohlásil: „Brigáda žádá, abyste českoslov. vojska nepokládali za národnostní pluky, nýbrž za revoluční vojsko, bojující spolu s Vámi za ideály svobody, rovnosti a bratrství! My jsme hotovi k novým obětem a věříme, že jen slovanský lid může dát světu všechny ideály, za které bojuje ruská revoluce!" Ministr války Kerenský přikázal, aby zasloužilí vojáci byli navrženi k povýšení na první hodnost důstojnickou, povýšil velitele armády generála Erdelyho na hodnost plného generála a velitele československé brigády plukovníka Trojanova na hodnost generálmajora. Ministr války dovolil doplnit československou brigádu nově zajatými Čechy. Zajatci šli ze štábu armády s rudými stužkami na prsou a s rudými květy na čapkách.

*

M. Zembič: Boje o opevnění u Koňuch.

(„Russkoje Slovo" 27. června (10. července) 1917.)

V prvních dnech nástupu největšího úspěchu bylo dostiženo na účastku nepřátelských opevnění u Koňuch.

Velitel armádního sboru, který se vyznamenal v tomto boji, generál Selivačev, nyní jmenovaný velitelem 7. armády, sdělil mně laskavě některé podrobnosti z bojů u Koňuch, které ukázaly názorně, co může udělat svobodná ruská armáda, jestli se patřičným způsobem užije jejího vznětu a nadšení.

Nepřátelská opevnění u Koňuch skládala se z několika řad opevnění s velkým množstvím míšků proti střelbě, betonovaných blindáží, kulometných hnízd s krásně zařízenými pozorovacími body. Rakušané, poučeni trpkou zkušeností dřívějších neúspěchů, s velkým úsilím pracovali na těchto opevněních už v srpnu předešlého roku a udělali je téměř nepřístupnými. Tato opevnění táhla se od vesnice Zarudzie do vesnice Byšků. Vzhledem na veliký strategický význam tohoto účastku chránila ho nejlepší maďarská vojska.

Dělostřelecká příprava nástupu trvala tam, tak jako u Břežan, dva a půl dne; potom 18. června (1. července) armádní sbor generála Nortbeka a levé křídlo armádního sboru generála Selivačeva současně zahájila nástup. Hned první úder našich vojsk obrátil Rakušany na útěk a v našich rukách ocitlo se celé pásmo jich opevnění. K večeru naše oddíly, postoupivše čtyři versty do předu, dostaly se ke koňušskému potoku. Pravé křídlo generála Selivačeva mělo zůstati pasivním a provést jen demonstraci.

Příštího dne uvedené armádní sbory rozvíjely dále úspěch dostižený předešlý den. Jejich zájem poutala hlavně výšina Mogila čili vrch 392, ovládající tento účastek; na ní měli Rakušané velmi dobře zařízený pozorovací bod. Boj o mogilovský vrch začal v 9 hod. večer a skončil odpoledne ve 2 hod. 40 minut. Hromové „urá", rozlehnuvší se široko daleko, oznámilo, že vítězství je naše.

Hrdiny tohoto boje byly pluky československé dobrovolnické brigády. Mluvě o jich válečné práci, generál Selivačev nenacházel dost pochvalných slov. Za starého režimu chovali se u nás krajně nepříznivě na tvoření československých dobrovolnických pluků, poněvadž to pokládali za podnik revoluční. Kdyby nebylo nynějšího náčelníka štábu jihozápadního frontu generála Duchonina, který velmi dobře ocenil Čechy, sotva byla by nyní vytvořena československá brigáda. Čechoslovákům byla v tomto boji dána úloha, aby provedli jen demonstraci. Nespokojujíce se touto úlohou, začaly československé pluky nástup zprvu jen v nevelikých oddílech, ale potom vyrazili ve střeleckých řetězích a hned po bajonetovém boji opanovali tři řady opevnění a začali zabírat zákopy směrem k Cenurce. Odvážný výkon československých dobrovolníků umožnil finské střelecké divisi, aby pronikla čtyři versty do předu. Rozvíjejíce dále tento úspěch, Češi podnikli útok na vrch Mogilu a opanovali ji po bajonetovém boji. Nastupující Češi mávali ve vzduchu čepicemi a volali na naše oddíly, které zůstaly za nimi: „Za námi, soudruzi, směleji!"

K večeru boj utichl. Čechoslováci a Finové opevnili se na nově obsazených posicích na linii Koňuchy — Chmielóvka. Velitel československé brigády plukovník Trojanov povýšen byl za tyto boje ministrem války Kerenským na generálmajora.

A. F. Kerenský děkoval Čechoslovákům za jich skvělý výkon a slíbil, že vymůže dovolení na tvoření nových československých pluků. V Rusku je 250.000 československých zajatců, kteří jsou hotovi všichni, jako jeden muž, bít se v našich řadách za svobodu Čech a Slovenska.

Pozn. red. V této rubrice budeme uveřejňovati příspěvky k dějinám našeho vojska. O dějinách našeho vojska bylo tolik a tak často psáno, že jest nutno, aby veškerý obrovský materiál byl soustředěn. Redakce „Vojenských Rozhledů" ujímá se této práce a jest přesvědčena, že prameny tyto budou důležitou pomůckou všem, kteří budou pracovati na dějinách našeho vojenství. Redakce žádá o laskavé zasílání příspěvků.

OBSAH

Řízení rizik v procesu plánování rozvoje Armády České republiky **3**
Miroslav Chylík, Josef Procházka

Znalost situace a současné informační prostředí **25**
Marek Fiebich

Odpor bez vůdce: vývoj, potlačování a výzkum povstaleckého konceptu **41**
Miroslav Mareš

Je Turecko připraveno na válku se Sýrií? **57**
Vladimír Bízik, Zdeněk Kříž

PŘÍLOHY

Příčiny vzniku a začlenění kybernetických sil a informačních operací do Armády České republiky **72**
Martin Havlík

Společná bezpečnostní a obranná politika EU v kostce – část první **87**
Vilém Kolín

Otiskli jsme před 100 lety **102**
Redakce

CONTENTS

Risk Management in the Armed Forces of the Czech Republic Development Planning Process **3**
Miroslav Chylík, Josef Procházka

Situational Awareness and Current Information Environment **25**
Marek Fiebich

Leaderless Resistance: Development, Countering and Research of Insurgent Concept **41**
Miroslav Mareš

Is Turkey Ready for a War with Syria? **57**
Vladimír Bízik, Zdeněk Kříž

ENCLOSURE

Reasons of formation and integration of cyber forces and information operations into the Army of the Czech Republic **72**
Martin Havlík

EU's Common Security and Defence Policy in a Nutshell – Part One **87**
Vilém Kolín

Printed 100 years ago **102**
Editorial Staff

VOJENSKÉ ROZHLEDY

Časopis VOJENSKÉ ROZHLEDY
čtvrtletník

Vydává:
Ministerstvo obrany České republiky, Tychonova 1, 160 01 Praha 6 – Dejvice

Vydávající instituce:
Univerzita obrany v Brně, Kounicova 156/65, 662 10 Brno

IČO: 60162694

Vojenské rozhledy č. 3/2020
Ročník: XXIX. (LXI.)

Datum předání do tisku: 8. září 2020

Rozšiřuje:
OKP MO, distribuce, Rooseveltova 23, 161 05 Praha 6
Olga Endlová, tel. 973 215 563, endlovao@army.cz

Redakce: Ing. Petr Koziel, telefon: 973 443 499
E-mail: vojenskerozhledy@unob.cz

Redakční rada: Ing. Ján Spišák, Ph.D. (předseda), PhDr. Miloš Balabán, Ph.D., pplk. Marco Biagini, Ph.D., prof. Mgr. Oldřich Bureš, Ph.D., M. A., doc. PhDr. Felix Černoch, CSc., plk. Florian Cîrciumaru, Ph.D., Mgr. Lukáš Dyčka, Ph.D., doc. PhDr. Jan Eichler, CSc., Mgr. et. Mgr. Jakub Fučík, Ph.D., prof. Dr. hab. Artur Gruszczak, plk. gšt. doc. Ing. Vladan Holcner, Ph.D., Ing. Vladimír Karaffa, CSc., prof. Ing. Aleš Komár, CSc., PhDr. Tomáš Kopečný, Mgr. Josef Kraus, Ph.D., brig. gen. Ing. Miloslav Lafek, prof. Juha-Matti Lehtonen, Ph.D., plk. gšt. Ing. Tomáš Novotný, Ph.D. MSc., Mgr. Martin Riegl, Ph.D., plk. Chris Rogers, MA, MMAS., doc. Hofrat Univ. Dr. Erwin Schmidl, Ph.D., Dr. hab. Zdzislaw Sliwa, RNDr. Pavel Štalmach, MBA, Ing. Miroslav Šuhaj, Ph.D., Mgr. et Mgr. Lukáš Tichý, Ph.D.

Tajemník redakční rady: Ing. Petr Koziel

Sídlo redakce: Kounicova 65, 662 10 Brno

Adresa pro zasílání pošty: Vojenské rozhledy – redakce, Kounicova 156/65, 662 10 Brno

Časopis Vojenské rozhledy v elektronické podobě naleznete na:
http://www.vojenskerozhledy.cz/

Časopis je evidován:
– v evropské databázi ERIH PLUS,
– v seznamu recenzovaných neimpaktovaných periodik vydávaných v České republice
– v mezinárodní databázi Index Copernicus Journals Master List 2015
– v katalogu Národní knihovny České republiky
– v databázi Central and Eastern European Online Library GmbH (CEEOL)
– v databázi Directory of Open Access Journals (DOAJ)

Grafická úprava: Adéla Zemanová

Tiskne: VGHMÚř Dobruška

Evidenční číslo: MK ČR E 6059

Identifikační číslo: ISSN 1210-3292 (print), ISSN 2336-2995 (on-line)

doi: 10.3849/2336-2995