
Recenzovaný článek

Komparace přístupů k elektronickému boji

Comparison of Approaches Towards Electronic Warfare

Petr Hlavizna

Abstrakt: Článek se zabývá odlišnými přístupy Severoatlantické aliance a ozbrojených sil Spojených států amerických k elektronickému boji, jako k vojenské činnosti v elektromagnetickém prostředí. Všechny výchozí materiály použité k analýze těchto přístupů, včetně specifik Armády České republiky k dané oblasti, byly získány z neklasifikovaných volně dostupných informací oficiálních vojenských zdrojů. Popisuje, vysvětluje a vizualizuje jednotlivé přístupy, komparací specifikuje a následně upozorňuje na rozdíly, včetně nesouladu v zavedených českých termínech, definicích a zkratkách. Poukazuje na neaktuálnost stále platné vojenské publikace Elektronický boj v AČR, jejíž používání je v současné podobě neopodstatněné a kontraproduktivní. Předkládá návrhy a doporučení pro unifikaci přístupu k problematice elektronického boje v Armádě České republiky tak, aby tyto byly v souladu se současně platným přístupem Severoatlantické aliance k činnostem v elektromagnetickém prostředí. Přispívá k pochopení doktrinálních pohledů na roli elektronického boje při plnění úkolů bojové podpory v soudobých vojenských operacích a vytváří podmínky pro eliminaci jejich nesprávného chápání v podmínkách Armády České republiky.

Abstract: The article examines the different approaches of the North Atlantic Treaty Organization and the United States Armed Forces towards Electronic Warfare, the military activity in the Electromagnetic Environment. All reference materials used for this analysis, including the specifics of the Army of the Czech Republic's approach toward the subject area, were obtained from unclassified military sources. It describes, explains and visualizes the individual approaches, and by their comparison it identifies and subsequently emphasizes cases of divergence, including non-compliance in established Czech terms, definitions and abbreviations. It highlights the obsolescence of the still valid military publication Electronic Warfare in the Army of the Czech Republic, the use of which, in its current form, has already been deemed as unfounded and counterproductive. It presents proposals and recommendations for unification of approach towards the Electronic Warfare issues within the Army of the Czech

Republic, in order to ensure consistency with the current North Atlantic Treaty Organization policy related to activities in the Electromagnetic Environment. It contributes to better understanding of doctrinal views on the role of Electronic Warfare in execution of combat support tasks in contemporary military operations, thus creating preconditions for elimination of associated misunderstandings in terms of the Army of the Czech Republic.

Klíčová slova: Elektronický boj; elektromagnetické prostředí; elektromagnetické spektrum; informace; terminologie.

Key words: Electronic Warfare; Electromagnetic Environment; Electromagnetic Spectrum; Information; Terminology.

ÚVOD

Zákonitosti elektromagnetického prostředí (EME – Electromagnetic Environment¹) zůstaly lidskému poznání skryty až do druhé poloviny 19. století, kdy vědecká a výzkumná činnost vyústila ve zformulování teorie elektromagnetického (EM) pole. Experimenty ověřily poznatky o šíření EM energie a potvrdily perspektivu jeho praktického použití, ke které došlo téměř okamžitě jak v civilní, tak i vojenské oblasti. Rozvoj bezdrátové telegrafie, hledání nových způsobů velení a spojení a činnost snažící se zabránit využívání elektromagnetického spektra (EMS – Electromagnetic Spectrum²) nepřitelem na bojištích rusko-japonské (1904-1905) a první světové války (1914-1918), následovány poválečným výzkumem, vedly nejenom k technickému zdokonalování tehdejších komunikačních prostředků, ale i k formulaci pravidel a postupů jak je použít a jak proti nim působit. Dříve využívaný pozemní, vzdušný a námořní prostor se tak přirozeně rozrůstal o další operační doménu, EME, které samo o sobě nebylo v tehdejší době ve vztahu k vojenskému umění jako samostatný operační prostor chápáno. I přesto začala narůstat potřeba řešit otázky využití EMS nejenom pro potřeby vlastních vojsk, ale i z důvodů zabezpečení ochrany proti cílené činnosti nepřitele. Začal se pozvolna formovat nový vojenský obor – elektronický boj (EB).

Důležitost EB rostla úměrně intenzitě využívání EMS, a to nejen ve vztahu k ofenzivní a defenzivní činnosti, ale i v souvislosti s aktivitami zaměřenými na zjišťování informací o nepříteli. Počátek EB souvisel s aktivitami v oblasti nižších kmitočtů EMS využívaných

1 *Record 18831 - EME: NATO Term* [online]. NATO Standardization Office, 1993 [cit. 2018-07-26]. Dostupné z: <https://nso.nato.int/natoterm/Web.mvc>

2 *AAP-15 (2016), Slovník zkratk používaných v dokumentech a publikacích NATO* [online]. Praha: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti – Odbor obranné standardizace, 2016 [cit. 2018-07-26]. Dostupné z: [http://www.oos-data.army.cz/aap15/AAP-15\(2016\).pdf](http://www.oos-data.army.cz/aap15/AAP-15(2016).pdf), s. 99

pro rádiové vysílání, následován dalším rozvojem reagujícím na pokračující obsazování ostatních kmitočtových pásem a zdokonalování způsobů vedení činnosti v EME. Proces rozvoje EB byl poměrně dynamický, přiměřený technickému a technologickému pokroku a rozvíjejícímu se umění vést bojovou činnost v EMS. Meziválečné období a konstrukce prvních radiolokátorů, stejně jako druhá světová válka stvrzující kritickou závislost aktérů mezinárodního konfliktu na včasných a věrohodných informacích, či fungujícím spojení, potvrdili vzrůstající požadavky na schopnosti velitelů umět adekvátně reagovat na činnost nepřítele v EMS. Vojenská činnost vedená v EME v období studené války i cílené aktivity v EMS prováděné aktéry lokálních konfliktů posledních desetiletí vedly a ve své podstatě neustále vedou ke kontinuálním změnám přístupů k EB a využívání EMS.

Rozdílné přístupy v chápání problematiky EB jednotlivými entitami, v tomto případě ozbrojenými silami (OS) jednotlivých států nebo jejich společnými vojenskými uskupeními, jsou způsobeny měnícím se charakterem operačního prostředí a vznikem nových hrozeb. Charakter operačního prostředí je ovlivněn mnoha faktory včetně nejen kontinuální inovace technického vybavení a zavádění nových technologií, ale i snazší dostupnosti vysoce sofistikované techniky pro široké spektrum uživatelů EME. Nové hrozby v EME vedou k nutnosti hledat eventuality pro snížení rizika. Ta mohou být jak v transformaci samotné obsahové náplně opatření EB a jeho dílčích součástí, tak i ve změnách stálých operačních postupů specialistů EB, kteří musí být připraveni v současných vojenských konfliktech reagovat mimo státní aktéry i na aktéry nestátní.

EB a informace o činnosti v EME byly vždy z důvodu jejich citlivosti předmětem nejvyšší ochrany. Snaha ochránit utajované informace (UI) spojené s aktivitami v EMS vedla k nastavení striktních pravidel a k implementaci řady opatření k zajištění ochrany utajovaných informací (OUI). Z toho důvodu je v současné době stále relativně obtížné získat ucelený přehled o jednotlivých přístupech OS k EB, stejně jako v detailech pochopit vzájemné difference a identičnost těchto přístupů, či celkově se v oblasti EB a EME orientovat. V případě řešení problematiky EB v jednotlivých OS je nejprve nutno pochopit přístup a specifika daného státu k aktivitám v EME jako takovým. Někdy totiž rozdílné pojmenování úkolů či opatření EB jednotlivých států může v konečné fázi znamenat shodnou obsahovou náplň a naopak. Severoatlantická aliance (NATO – North Atlantic Treaty Organization) se proto snaží sjednotit nejenom terminologii, ale i jednotlivé přístupy k řešení otázek EB.

Článek autora navazuje na některé výstupy jeho dosud nezveřejněné Analytické studie rozvoje EB Armády České republiky (AČR), kterou zpracoval s využitím terénního šetření v druhé polovině roku 2017. Respondenty analytické studie bylo celkem 21 vojáků z povolání (VZP) a 1 občanský zaměstnanec rezortu ministerstva obrany (MO), sloužící na taktickém i operačně-strategickém stupni velení a řízení AČR. Průměrná doba trvání jednoho nestandardizovaného rozhovoru se pohybovala v rozmezí 45-60 minut. Pro získání výpovědí respondentů z co nejširšího spektra byly nestandardizované rozhovory s VZP prováděny v hodnostních sborech od poddůstojníků až po vyšší důstojníky. Oslovení byli nejenom příslušníci odborné komunity EB AČR, ale i ti, kteří se na zabezpečování jejich odborné činnosti přímo podílejí. Článek se zabývá EB v NATO, u OS Spojených států amerických (USA) a v AČR, protože reaguje na zjištěné závěry provedené analytické studie v oblasti doktrín, přinášející poznatek o nesprávném vnímání přístupu k EB v AČR s nerespektováním některých, pro ČR závazných přístupů NATO k EB. Přístup USA k EB je

analyzován z důvodu vysvětlení rozdílů mezi přístupy k EB u OS USA a v NATO, které jsou ze strany příslušníků AČR často neúmyslně zaměňovány. Na základě deskripce a analýzy přístupů k oblastem EB a EMS, vytvořených v souladu s právními předpisy České republiky (ČR)³ a NATO v oblasti ochrany utajovaných informací⁴ a s Rozkazem ministra obrany (RMO) č. 16/2013, Věstníku o ochraně určených neutajovaných informací (UNI) v rezortu MO, ve znění pozdějších předpisů, jsou v článku uváděny pouze informace určené k volné distribuci. Přístup k oblastem EB a EMS je v NATO, OS USA a AČR popsán a analyzován bez nutnosti specifikace úrovně velení a řízení, stejně jako záměrně neuvádí všechny odlišnosti přístupů k EB u jednotlivých druhů OS, protože se jedná o deskripci a analýzu uceleného přístupu k problematice EB.

Cílem článku je na základě analýzy informací vysvětlit a vizualizovat přístupy NATO, OS USA a AČR k EB, komparací specifikovat a následně poukázat na rozdíly v jednotlivých přístupech a návrhem konkrétních doporučení pro zlepšení současného stavu reflektovat dílčí zjištění analytické studie o nesprávném vnímání zkoumané problematiky přístupu k EB v AČR.

1 ELEKTRONICKÝ BOJ V NATO

„Výzvy a příležitosti EB při podpoře vojenských operací jsou dány potřebou vojenských sil mít neomezený přístup k využívání EME.“⁵

Přístup NATO k EB (EW – Electronic Warfare⁶) je zastřešen dokumentem MC 0064, The NATO Policy for EW. Za dobu existence NATO byl již celkem desetkrát revidován, a to nejenom z důvodů reakce na změny v EME a operačním prostředí, ale i změny ve velitelské struktuře NATO a reakce na hrozby, kterým byla a je tato organizace nucena čelit. MC 0064 je odsouhlasen všemi členskými státy NATO a stanovuje, jakým způsobem má v oblasti EB docházet ke sjednocení a tvorbě společných vojenských doktrín a interoperabilních standardů.⁷

Je skutečností, že ani neutajované vojenské publikace o EB NATO označené jako NATO UNCLASSIFIED nejsou určeny k volné distribuci⁸ a z pohledu AČR je s nimi nakládáno jako s UNI. Mimoto existuje řada vojenských publikací a dokumentů, které jsou přímo klasifikovány jako utajované, a tudíž ani ty nemohou být předmětem následující analýzy. Se-

3 Právní předpisy. Národní bezpečnostní úřad [online]. [cit. 2018-07-26]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/>

4 Předpisy NATO vztahující se k ochraně utajovaných informací. Národní bezpečnostní úřad [online]. [cit. 2018-07-26]. Dostupné z: <https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/>

5 NATO Encyclopedia 2017 [online]. Brussels: NATO Public Diplomacy Division, 2017 [cit. 2018-07-27]. Dostupné z: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20180201_2017-nato-encyclopedia-eng.pdf, s. 225

6 ref. 2, s. 103

7 ref. 5, s. 226

8 ref. 4

znam současně platných standardů NATO je možné získat na webových stránkách Organizace NATO pro standardizaci (NSO – NATO Standardization Office)⁹. Z nich byly vybrány následující standardizační dohody NATO (STANAG – NATO Standardization Agreement) a standardizační doporučení NATO (STANREC – NATO Standardization Recommendation)¹⁰, které patří v oblasti EB k nejdůležitějším. Pro přehlednost byly doplněny o český překlad jejich originálních názvů a klasifikaci, uváděné na webových stránkách českého Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti – Odboru obranné standardizace (Úř OSK SOJ – OOS)¹¹:

1. STANAG 2607, Ed: 1, Guidelines for Interservice Electronic Warfare (EW) Support to Explosive Ordnance Disposal (EOD) Operations on Multinational Deployments – AEODP-11 VOL II EDITION A (Směrnice pro společné zabezpečení EB **při likvidaci výbušného materiálu během mnohonárodních nasazení, svazek 2**, NATO UNCLASSIFIED);
2. STANAG 3873, Ed: 6, Electronic Warfare in Air Operations – ATP-3.6.3 (EB ve vzdušných operacích, NATO UNCLASSIFIED);
3. STANAG 4658, Ed: 1, Cooperative Electronic Support Measure Operations – AEDP-13 EDITION A (Společná (kooperativní) opatření elektronického zabezpečení, NATO UNCLASSIFIED);
4. STANAG 6010, Ed: 3, Electronic Warfare in the Land Battle – ATP-3.6.2 (EB v pozemních operacích, NATO UNCLASSIFIED);
5. STANAG 6018, Ed: 3, Allied Joint Doctrine for Electronic Warfare – AJP-3.6 EDITION B (Spojenecká společná doktrína EB, NATO RESTRICTED);
6. STANAG 6519, Ed: 1, NATO Suppression of Enemy Air Defences (SEAD) Doctrine – ATP-3.6.4 EDITION A (NATO doktrína potlačení protivzdušné obrany nepřítele, NATO UNCLASSIFIED);
7. STANREC 4803, Ed: 1, Procedures for Standardized Exploitation of RCIED Switches, Radio Technologies, and Other Electronic Components – AEP-4803 EDITION A (Postupy pro standardizované využití přepínačů, radiotechnologií a dalších elektronických součástí RCIED, NATO UNCLASSIFIED);
8. STANREC 4805, Ed: 1, Overview of Compatibility Trial Procedures for Electronic Countermeasures Against Radio Controlled Improvised Explosive Devices – AEP-4805 EDITION A (Přehled zkušebních postupů k ověření kompatibility elektronických protipatření proti improvizovaným výbušným zařízením řízeným rádiem, NATO RESTRICTED).

Pro analýzu přístupu NATO k EB byly použity výhradně neklasifikované informace uvedené v oficiálních zdrojích NATO, přístupných široké veřejnosti. Jedním z nich je

⁹ List of Current NATO Standards. *NATO Standardization Office* [online]. [cit. 2018-07-26]. Dostupné z: <http://nso.nato.int/nso/nsdd/listpromulg.html>

¹⁰ *Jednotná forma zápisu odkazů na obranné standardy* [online]. Praha: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti, 2017 [cit. 2018-08-05]. STAND-4/17-Úř OSK SOJ/1-1.dopl. Dostupné z: <http://www.oos-data.army.cz/metodicke-pokyny/stand-04.pdf>, s. 4

¹¹ Standardizační dokumenty. *Odbor obranné standardizace* [online]. [cit. 2018-07-26]. Dostupné z: <http://www.oos.army.cz/standardizacni-dokumenty>

i terminologický slovník AAP-06, NATO Glossary of Terms and Definitions (English and French), který byl ve verzi z roku 2015 přeložen i do českého jazyka a zveřejněn na webových stránkách Úř OSK SOJ – OOS. Navzdory omezení použití pouze oficiálních a volně dostupných informačních zdrojů lze výstupy následující analýzy považovat za relevantní a vystihující současný přístup NATO k EB.

AAP-06 definuje EB v NATO jako vojenskou činnost využívající EM energii k získání znalosti situace a dosažení útočných a obranných účinků.¹² Z této definice vyplývá, že získání znalosti situace (SA – Situational Awareness), tj. znalosti prvků v prostoru bojové činnosti, která je nezbytná k přijetí rozhodnutí založeném na informacích¹³, by mělo být ve vztahu k EME a opatřením EB prováděno v prostoru operace sil a prostředků (SaP) EB cílenou činností v celém EMS. EME je definováno jako souhrn EM jevů existujících v dané lokalitě¹⁴ a EMS jako úplné a uspořádané rozložení EM vln podle jejich kmitočtu nebo vlnové délky (zahrnuje rádiové vlny, mikrovlny, tepelné záření, viditelné světlo, ultrafialové záření, rentgenové záření, EM kosmické záření a gama záření)¹⁵.

V oblasti EB jsou opatření přispívající k získání SA souhrnně nazývána jako elektronická podpůrná opatření (ESM – Electronic Warfare Support Measures¹⁶). Tato opatření jsou realizována SaP EB zaměřenými svou činností výhradně na vyzařování EM energie nepřitelem. Příkladem vyzařování mohou být nepřitelem používané radiolokátory, vysílače, rušiče anebo kterékoliv jiné zdroje, jenž využívají EM vyzařování ke své činnosti záměrně nebo EM energii vyzařují neúmyslně. Vlastní prostředky EB plní úkoly ESM mohou za určitých podmínek zjistit jakýkoliv zdroj EM vyzařování a tím tak přispět k získání SA v prostoru operace. Z výše uvedeného vyplývá, že při samotném plnění úkolů ESM vlastními SaP EB nedochází k záměrnému EM vyzařování. Všechna činnost vlastních SaP EB je při plnění úkolů ESM z hlediska aktivit vedených proti nepříteli v EMS tzv. pasivní, tedy cílenou činností nepřítelova EB (resp. jeho ESM) nejzjistitelná. Pokud ale vlastní prostředek EB plní úkoly ESM a vyzařuje EM energii v souvislosti s vlastním provozem (např. používání radiolokátorů na vzdušných či námořních platformách) či plněním operačního úkolu (např. používání radiostanice pro komunikaci s nadřazeným stupněm velení), stává se zdrojem EM vyzařování a tedy cílem pro SaP EB protivníka.

Analýzou definice EB NATO lze získat přehled činností, které je možno vedením EB v EME provádět. O těchto činnostech obecně hovoříme jako o vojenských činnostech v EME¹⁷:

¹² AAP-06 (2015), *Slovník NATO s termíny a definicemi (anglicky a francouzsky)* [online]. Praha: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti – Odbor obranné standardizace, 2015 [cit. 2018-07-26]. Dostupné z: [http://www.oos-data.army.cz/aap6/AAP-06\(2015\)cz-final.pdf](http://www.oos-data.army.cz/aap6/AAP-06(2015)cz-final.pdf), s. 131

¹³ ref. 12, s. 301

¹⁴ ref. 12, s. 129

¹⁵ AAP-6, *Edition 2017, NATO Glossary of Terms and Definitions (English and French)* [online]. Brussels: NATO Standardization Office, 2017 [cit. 2018-07-26]. Dostupné z: http://nso.nato.int/nso/zPublic/_BranchInfo/Terminology_Public/Non-Classified%20NATO%20Glossaries/AAP-6.pdf, s. 41

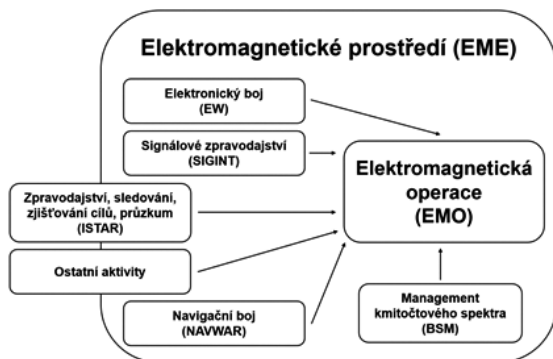
¹⁶ ref. 2, s. 101

¹⁷ ref. 12, s. 130-131

1. Elektronické sledování (ES – Electronic Surveillance) – využití EM energie k získání znalosti situace a informací zpravodajského charakteru;
2. Elektronický útok (EA – Electronic Attack) – využití EM energie k ofenzivním účelům;
3. Elektronická obrana (ED – Electronic Defence) – využití EM energie k poskytnutí ochrany a zajištění účinného využití EMS vlastními silami.

EB svými aktivitami výše uvedené činnosti ES, EA a ED realizuje, avšak není jejich jediným vykonavatelem. Proto je při plánování a vedení ES, EA a ED v EME vždy nutno zvažovat nejvhodnější variantu účinného a efektivního zapojení SaP, které jsou schopny se na těchto činnostech podílet.

Výše popsané činnosti mají úzkou souvislost s vedením elektromagnetických operací (EMO – Electromagnetic Operations¹⁸). EMO jsou z pohledu NATO definovány jako všechny operace, které formují nebo využívají EME, anebo jej používají k útoku nebo obraně, včetně použití EME k podpoře operací ve všech ostatních operačních prostředích. EMO zahrnují EB, signálové zpravodajství (SIGINT – Signal Intelligence¹⁹), zpravodajství, sledování, zjišťování cílů a průzkum (ISTAR – Intelligence, Surveillance, Target Acquisition, Reconnaissance²⁰), navigační boj (NAVWAR – Navigation Warfare²¹) a management kmitočtového spektra bojiště (BSM – Battle space Spectrum Management), přičemž nejsou jimi samotnými omezeny²² (ostatní aktivity). Vizualizace EMO ve smyslu této definice je znázorněna na obrázku č. 1. V rámci plánování a vedení EMO lze jednotlivé aktivity integrovat a koordinovat. Je však třeba si uvědomit, že některé aktivity (ISTAR, ostatní) mohou z podstaty jejich činnosti probíhat jak v EME, tak i mimo něj, a to zcela nezávisle na něm samotném. Rovněž platí, že jednotlivé aktivity mohou probíhat v EME samostatně, bez nutnosti plánovat a vést EMO. EMO je tedy nutno brát jako jednu z možností koordinace úsilí v EMS, nikoliv nutnost.



Obrázek č. 1: Elektromagnetické operace v NATO

¹⁸ ref. 15, s. 41

¹⁹ ref. 12, s. 364

²⁰ ref. 2, s. 143

²¹ ref. 2, s. 195

²² ref. 15, s. 41

EB je v NATO rozdělován dle realizace elektronických opatření²³:

1. Elektronická podpůrná opatření (ESM – Electronic Warfare Support Measures) – část EB zahrnující činnosti, jejichž účelem je vyhledat, zachytit a identifikovat EM vyzařování a upřesnit jeho zdroje s cílem okamžitě rozpoznat hrozící nebezpečí. Poskytuje zdroje informací nezbytné pro okamžitá rozhodnutí týkající se elektronických protiopatření, elektronických ochranných opatření a dalších taktických činností;
2. Elektronická protiopatření (ECM – Electronic Countermeasures) – část EB zahrnující aktivity uskutečněné za použití EM energie s cílem prevence nebo redukce možnosti protivníka efektivně využít EMS. Rozeznávají se tři oblasti elektronických protiopatření:
 - a. Elektronické rušení;
 - b. Elektronické klamání;
 - c. Elektronická neutralizace;
3. Elektronická ochranná opatření (EPM – Electronic Protective Measures) – část EB zahrnující opatření vedoucí k zajištění účinného využití EMS vlastními prostředky navzdory využívání EM energie nepřítelem. Existují dvě dílčí součásti elektronických ochranných opatření:
 - a. Aktivní elektronická ochranná opatření;
 - b. Pasivní elektronická ochranná opatření.

Z výše uvedeného je patrné, že realizací ESM dochází k vytvoření podmínek pro možné odhalení akutní reálné hrozby v EMS, namířené proti činnosti vlastních vojsk v prostoru operace. To může následně aktivovat ECM, EPM nebo další taktické činnosti, které by přispěly nebo dokonce vedly k okamžité degradaci nebo eliminaci zdroje identifikované hrozby. Z hlediska doby trvání tak v ideálním případě hovoříme o reakci provedené v čase blížícím se reálnému. Takovýmto přístupem se EB a jeho ESM liší například od činnosti elektronického zpravodajství (ELINT – Electronic Intelligence), definovaného jako zpravodajství získávané z EM, nekomunikačního vysílání²⁴ a komunikačního zpravodajství (COMINT – Communication Intelligence), definovaného jako zpravodajství, které využívá přenosu EM energie a komunikační systémy jiným způsobem než předpokládání příjemci a uživatelé²⁵. Hovoříme-li o NATO a ESM, je třeba si uvědomit originální obsah této anglické zkratky, vycházející ze slov Electronic Warfare Support Measures. Překlad zkratky ESM do českého jazyka není zcela správný, protože uvádí, že se jedná o „Elektronická podpůrná opatření“²⁶. ESM mají vždy vazbu pouze k EB a musí být takto i chápána. Proto by i český překlad ESM, pokud by byl proveden doslovně a v kontextu s obsahovou náplní, měl být definován jako „Podpůrná opatření elektronického boje“.

EB je součástí bojové podpory bojových jednotek. Elektronická opatření EB jsou vztažena prioritně k podpoře okamžitých rozhodnutí velitele daného stupně velení. SaP EB mohou v rámci ESM, ECM a EPM plnit tyto úkoly:

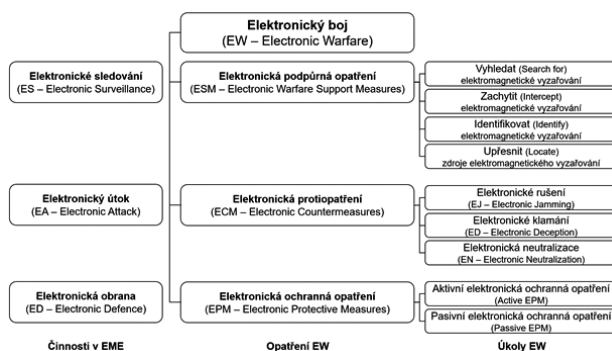
²³ ref. 12, s. 130-131

²⁴ ref. 15, s. 42

²⁵ ref. 15, s. 26

²⁶ ref. 12, s. 131

1. ESM²⁷:
 - a. Vyhledat (Search for) EM vyzařování;
 - b. Zachytit (Intercept) EM vyzařování;
 - c. Identifikovat (Identify) EM vyzařování;
 - d. Upřesnit (Locate) zdroje EM vyzařování.
2. ECM²⁸:
 - a. Elektronické rušení (EJ – Electronic Jamming) – záměrné vyzařování, opětné vyzařování nebo odrážení EM energie s cílem narušit účinnost elektronických zařízení, přístrojů nebo systémů nepřítele;
 - b. Elektronické klamání (ED – Electronic Deception) – záměrné vyzařování, opětné vyzařování, změna, pohlcování nebo odrážení EM energie způsobem, který předpokládá klamání, rozptýlení nebo odvedení pozornosti nepřítele nebo jeho elektronických systémů;
 - c. Elektronická neutralizace (EN – Electronic Neutralization) – záměrné využití EM energie s cílem buď dočasně, nebo trvale poškodit prostředky nepřítele, které pracují výhradně v oblasti EMS.
3. EPM:
 - a. Aktivní elektronická ochranná opatření (Active EPM) – zjistitelná opatření, jako změna parametrů vysílání, pokud je to potřebné, aby se zajistilo vlastní účinné využití EMS;²⁹
 - b. Pasivní elektronická ochranná opatření (Passive EPM) – nezjistitelná opatření, spočívající například v pracovních postupech a technických vlastnostech přístrojů pro zajištění efektivního využití EMS vlastními silami.³⁰



Obrázek č. 2: Rozdělení EB dle pojetí NATO včetně znázornění činností v EME

²⁷ ref. 12, s. 131

²⁸ ref. 12, s. 130-131

²⁹ ref. 12, s. 21

³⁰ ref. 12, s. 251

Na obrázku č. 2 je znázorněn EB dle pojetí NATO, jeho jednotlivá opatření a úkoly, které jsou při jejich realizaci plněny. V levé části obrázku jsou rovněž uvedeny činnosti, na kterých EB v EME může participovat. Z ní je patrné, že SaP EB prostřednictvím ESM realizují ES, prostřednictvím ECM realizují EA a prostřednictvím EPM realizují ED. Úkoly, které jsou vlastním SaP EB pro ESM, ECM a EPM vydávány, jsou znázorněny v pravé části obrázku a týkají se nejenom s operačních požadavků, ale zejména konkrétních příjemců úkolů v závislosti na jejich reálných technických i taktických schopnostech.

NATO ve svém terminologickém slovníku rovněž hovoří o dalších činnostech, které mají souvislost s aktivitami v EMS a EB jako takovým:

1. Řízené vyzařování (EMCON – Emission Control) – výběrové řízení vyzařované EM nebo akustické energie. Může mít dvojí cíl:
 - a. Minimalizovat možnost zjištění vyzařování protivníkem i využití takto získaných informací;
 - b. Redukovat EM rušení a tím zlepšit výkon vlastních senzorů;³¹
2. Elektronické maskování (Electronic Masking) – řízené vyzařování EM energie na vlastních kmitočtech tak, aby chránilo vysílání vlastních spojovacích a elektronických systémů proti ESM/SIGINT nepřítele, bez podstatného negativního vlivu na činnost vlastních systémů;³²
3. Přehled o elektromagnetické situaci (REM – Recognized Electromagnetic Picture) – ucelený a nepřetržitý přehled o EME s cílem pozitivně identifikovat a nepřetržitě sledovat všechny zdroje EM vyzařování a s nimi související platformy a zbraně v prostoru odpovědnosti;³³
4. Personál štábu určený pro plánování a vedení bojové činnosti v EME (EMB – Electromagnetic Battlestaff) – personál předurčený pro koordinaci EMO dle společných standardizovaných postupů, řešící EMO společně s ostatními schopnostmi v návaznosti na časový plán činnosti (BR – Battle Rhythm);³⁴
5. Společné operace v oblasti elektronických podpůrných opatření (CESMO – Co-operative Electronic Support Measure Operations) – standard umožňující výměnu a fúzování dat na nejnižší (technické) úrovni, sloužící pro společné operace elektronického sledování. Výsledky mohou být použity k získání znalosti situace, pro účely targetingu a ostatní činnosti.³⁵

NATO chápe důležitost ovládnutí EMS jako jeden z klíčových faktorů pro úspěšné vedení nejenom současných, ale i budoucích operací. Dalo by se říci, že úsilí NATO směřované k vybojování a udržení nadvlády v EMS má holistický charakter. Komplexnost přístupu NATO k aktivitám v EME podtrhuje snaha o standardizaci a dosažení adekvátní úrovně interoperability, akceptované v ideálním případě všemi členskými státy NATO bez výhrad. Tyto snahy jsou do jisté míry ovlivněny národními zájmy jednotlivých členských států, což má dopad na flexibilitu a rychlost implementace opatření do praxe. NATO přistupuje

³¹ ref. 12, s. 134

³² ref. 15, s. 42

³³ ref. 15, s. 95

³⁴ ref. 15, s. 41

³⁵ ref. 15, s. 30

k plnění dílčích úkolů EB v návaznosti na schopnosti, které je jim tato vojenská činnost schopna v EMS zprostředkovat. Proto jsou schopnosti EB využívány nejenom k podpoře EMO, ale i jiných typů operací, v nichž je EB schopen znemožnit protivníkovi využívat výhod a vlastním silám zajistit neomezený přístup k EMS. Soudobý EB tak má přesah do pozemního, vzdušného, námořního i kosmického prostoru, kde plní úkoly v souvislosti s komunikačními i nekomunikačními zdroji EM vyzařování nepřítel.³⁶

2 ELEKTRONICKÝ BOJ V OZBROJENÝCH SILÁCH SPOJENÝCH STÁTŮ AMERICKÝCH

„Společné síly jsou napříč všemi společnými funkcemi a doménami kriticky závislé na EMS. Aby v budoucím konfliktu zvítězili, musí zvítězit v boji za nadvládu v EMS.“³⁷

OS USA jsou dlouhodobě nejlépe systematicky budovanou bojovou silou na světě. Technická, technologická, zdrojová, ale i morální podpora, které se jim zejména na domácí půdě dostává, vede společně s kontinuálním rozvojem vojenského umění, posilováním praktickými zkušenostmi příslušníků OS z bojových i nebojových operací posledních desetiletí, k dosažení a udržení vysokého standardu úrovně bojeschopnosti vlastních vojsk. Je skutečností, že velení OS USA si je plně vědomo kritické závislosti společných sil na EMS. K tomu směřuje i doktrinálně funkční provázání činností v EMS, které prostupuje napříč všemi složkami OS USA a zasahuje do všech vzájemně sdílených funkcí a domén, stejně jako do dalšího rozvoje organizace, plánování a vedení společných operací v EMS.

Z veřejně dostupných informací uváděných na webových stránkách Spojeného výboru náčelníků štábů (Joint Chiefs of Staff)³⁸ OS USA vyplývá, že oblast EB je na úrovni společných sil primárně řešena ve společné publikaci JP 3-13.1, *Electronic Warfare*, 08 February 2012, která není určena k volné distribuci. Oblastí EB a EMS se zásadním způsobem nebo okrajově rovněž zabývají vojenské publikace:

1. JP 3-0, *Joint Operations*, 17 January 2017³⁹;
2. JP 6-01, *Joint Electromagnetic Spectrum Management Operations*, 20 March 2012⁴⁰;

³⁶ HLAIVIZNA, Petr. Elektronický boj – bojová činnost v elektromagnetickém prostředí. In: *Nové přístupy k zajištění bezpečnosti státu*. Brno: Univerzita obrany, 2018, s. 62. ISBN 978-80-7582-037-2.

³⁷ JDN 3-16, *Joint Electromagnetic Spectrum Operations*, 20 October 2016 [online]. [Joint Staff Pentagon, Washington, D.C.]: Joint Force Development, 2016 [cit. 2018-07-28]. Dostupné z: http://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn3_16.pdf?ver=2017-12-28-144149-910, s. v

³⁸ Home: Doctrine: Joint Doctrine Pubs: 3-0 Operations Series. *Joint Chiefs of Staff* [online]. [cit. 2018-07-26]. Dostupné z: <http://www.jcs.mil/Doctrine/Joint-Docctrine-Pubs/3-0-Operations-Series/>

³⁹ JP 3-0, *Joint Operations*, 17 January 2017 [online]. [Joint Staff Pentagon, Washington, D.C.]: Joint Force Development, 2017 [cit. 2018-07-28]. Dostupné z: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0_20170117.pdf

⁴⁰ JP 6-01, *Joint Electromagnetic Spectrum Management Operations*, 20 March 2012 [online]. [Joint Staff Pentagon, Washington, D.C.]: Joint Staff, 2012 [cit. 2018-07-28]. Dostupné z: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_01.pdf

3. JDN 3-16, Joint Electromagnetic Spectrum Operations, 20 October 2016⁴¹;
 4. DOD Dictionary of Military and Associated Terms, June 2018⁴².
 5. OS USA na úrovni Velitelství společných sil (JFC – Joint Force Command⁴³) realizují EB a činnosti v EMS za pomoci plánování, koordinace, vedení a vyhodnocování tzv. společných operací v elektromagnetickém spektru (JEMSO – Joint Electromagnetic Spectrum Operations). Budeme-li se zabývat jednotlivými druhy OS USA separátně, zjistíme následující⁴⁴:
 1. Armáda realizuje JEMSO primárně skrze tzv. prvek kyberneticko-elektromagnetických činností (CEMA Element – Cyber Electromagnetic Activities Element). Tento přístup je podrobně vysvětlen v polním manuálu armády FM 3-12, Cyberspace and Electronic Warfare Operations, April 2017⁴⁵. Idea tohoto přístupu je založena na vedení kybernetických operací a operací EB využívajících výše zmíněný prvek CEMA ve sloučených pozemních operacích⁴⁶;
 2. Námořní pěchota je odpovědná za identifikaci, stanovení priorit a integraci tzv. expedičních kybernetických schopností a schopností EB, které koordinuje s operačními silami, podpůrnými prvky a spolupracujícími součástmi při vedení vlastních operací;
 3. Námořnictvo provádí námořní operace v EMS za pomoci tzv. prvku operací v elektromagnetickém spektru (EMSO Element – Electromagnetic Spectrum Operations Element). Jeho úkolem je ve spojitosti s podřízenými složkami realizovat plán velitele k dosažení převahy v EMS námořních operací;
 4. Letectvo poskytuje JFC svoji podporu vlastním EB a managementem EMS skrze skupinu koordinace EB (EWCC – Electronic Warfare Coordination Cell⁴⁷) a vzdušné komponentní ředitelství pro komunikace;
 1. Pobřežní stráž uskutečňuje ve vztahu k JEMSO pouze tzv. elektromagnetický manévrový boj (EM Maneuver Warfare), který v současnosti zahrnuje pouze monitorování, vyhodnocování a poskytování zpravodajských produktů.
- Velitelé komponentních velitelství jednotlivých druhů sil a podřízení JFC zřizují pro podporu společného plánování, koordinaci a řízení EMS stálou tzv. skupinu společných operací v elektromagnetickém spektru (JEMSOC – Joint Electromagnetic Spectrum Operations Cell).⁴⁸

⁴¹ ref. 37

⁴² *DOD Dictionary of Military and Associated Terms* [online]. [Joint Staff Pentagon, Washington, D.C.]: [Joint Force Development], 2018 [cit. 2018-07-28]. Dostupné z: <http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-07-25-091749-087>

⁴³ ref. 2, s. 147

⁴⁴ ref. 37, s. vii

⁴⁵ *FM 3-12, Cyberspace and Electronic Warfare Operations, April 2017* [online]. [HQs, Department of the Army]: TRADOC, 2017 [cit. 2018-07-28]. Dostupné z: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf

⁴⁶ ref. 45, s. v

⁴⁷ ref. 2, s. 103

⁴⁸ ref. 37, s. vi

I přes existující specifika rozdílných přístupů a realizace opatření v oblastech EMS a EB představovaná jednotlivými druhy sil je obecné dělení a chápání EB v OS USA jednotné. Následující analýza EB v OS USA je postavena na veřejnosti dostupných informacích uvedených v polním manuálu FM 3-12. Ten se přitom v některých svých částech odvolává na JP 3-13.1, jehož přímému rozboru se s ohledem na striktní dodržování pravidel OUI a UNI v článku nelze věnovat. Další omezením při zpracování této kapitoly je neexistence oficiálních, terminologicky odsouhlasených překladů zdrojové literatury. Tyto omezující podmínky nemají zásadní vliv na pochopení přístupu OS USA k oblasti EB.

EB je v OS USA definován jako vojenská činnost zahrnující použití EM a směrované energie k ovládnutí EMS nebo útoku na nepřítele.⁴⁹ Termín směrovaná energie (DE – Directed Energy) zastřešuje označení technologií, které se vztahují k vytváření svazku koncentrované EM energie nebo atomárních nebo subatomárních částic.⁵⁰

EB v pojetí OS USA zahrnuje:⁵¹

1. Elektronický útok (EA – Electronic Attack) – část EB zahrnující použití EM energie, směrované energie nebo protiradiolokačních zbraní k útoku na síly, zařízení nebo prostředky se cílem snížit, neutralizovat nebo zničit bojové schopnosti nepřítele; je považován rovněž za jistou formu palby;⁵²
2. Elektronickou ochranu (EP – Electronic Protection) – část EB zahrnující činnosti, jejichž účelem je ochrana sil, zařízení nebo prostředků od jakýchkoliv účinků přátelského nebo nepřátelského využití EMS, které snižuje, neutralizuje nebo ničí bojové schopnosti vlastních vojsk;⁵³
3. Podporu elektronickým bojem (ES – Electronic Warfare Support) – část EB zahrnující činnosti vycházející z úkolů operačního velitele, nebo z jeho přímého řízení, směrované k pátrání (Search for), zachycení (Intercept), identifikaci (Identify) a určení polohy (Locate) nebo přidělení (Localize) zdrojů záměrného nebo neúmyslného vyzařování EM energie, za účelem okamžitého odhalení hrozeb, targetingu, plánování a vedení budoucích operací.⁵⁴

Všechny z výše uvedených složek EB lze rozbořením jejich činností blíže specifikovat jejich obsahovou stránku a složení:

1. Činnosti vztahující se k EA mohou být jak ofenzivní, tak i defenzivní. Po obsahové stránce a ve vztahu ke schopnostem jsou si ofenzivní i defenzivní EA velice podobné, avšak rozdíl je v účelu jejich použití. Defenzivní EA chrání vlastní síly, prostředky, zařízení nebo platformy, kdežto ofenzivní EA znemožňuje (Deny), narušuje (Disrupt) nebo ničí (Destroy) schopnosti nepřítele. Mezi činnosti EA patří⁵⁵:

⁴⁹ ref. 45, s. 1-25

⁵⁰ ref. 42, s. 69

⁵¹ ref. 45, s. 1-25

⁵² ref. 42, s. 76

⁵³ ref. 42, s. 76

⁵⁴ ref. 42, s. 77

⁵⁵ ref. 45, s. 1-27–1-28

- a. Protiopatření (Countermeasures) – jsou formou vojenské vědy, která za použití prostředků a/nebo technik má za cíl zhoršení operační účinnosti nepřátelských aktivit. Protiopatření mohou být použita preventivně nebo reaktivně. Zařízení a techniky používané jako protiopatření EB zahrnují:
- i. Elektrooptická a infračervená protiopatření (EO-IR CM – Electro-Optical-Infrared Countermeasures) – zařízení nebo technika používající elektrooptické a infračervené materiály nebo technologie, které mají snížit účinnost nepřátelské činnosti, zejména pokud jde o přesně řízené zbraně a senzorové systémy;
 - ii. Radiofrekvenční protiopatření (RF CM – Radio Frequency Countermeasures) – jakékoli zařízení nebo technika používající RF materiály nebo technologie, které mají snížit účinnost nepřátelské činnosti, zejména pokud jde o přesně naváděné zbraně a senzory;
- b. Elektromagnetické klamání (Electromagnetic Deception) – záměrné vyzařování, opětovné vyzařování, změna, pohlcování, potlačování, znemožňování, zkvalitňování nebo odrážení EM energie způsobem, který předpokládá oklamání nepřítele nebo nepřátelských zbraňových systémů závislých na využívání EMS, důsledkem čehož dojde k degradaci nebo neutralizaci jeho bojeschopnosti. Druhy EM klamání se rozdělují na:
- i. Manipulativní (Manipulative) – zahrnují činnosti vedoucí k eliminaci vlastního odhalení nebo předávání zavádějících příznakových indikátorů, které mohou být použity nepřátelskými silami;
 - ii. Simulační (Simulative) – zahrnuje činnosti simulující vlastní fiktivní nebo skutečné schopnosti, použité k oklamání nepřítele;
 - iii. Imitační (Imitative) – představují imitaci EM vyzařování nepřátelských systémů;
- c. Elektromagnetická intruze (Electromagnetic Intrusion) – záměrné zavedení EM energie do přenosových tras, a to jakýmkoli způsobem, s cílem klamat operátory nebo způsobovat zmatek. Často se provádí vložením nepravdivých informací (hlasové instrukce, falešné cíle, souřadnice pro vedení palby, zpětného vysílání předem nahraných datových přenosů);
- d. Elektromagnetické rušení (Electromagnetic Jamming) – záměrné vyzařování, opětovné vyzařování nebo odrážení EM energie s cílem zabránit nebo snížit efektivní využívání EMS nepřítelem a se záměrem snížit nebo neutralizovat bojové schopnosti nepřítele;
- e. Elektronické zkoumání/zjišťování (Electronic Probing) – úmyslné vyzařování navržené tak, aby se o zařízeních nebo systémech potenciálních nepřátel mohly zjistit jejich funkce a provozní schopnosti;
- f. Elektromagnetický impulz (EMP – Electromagnetic Pulse) – EM záření pocházející ze silného elektronického impulzu, nejčastěji způsobeného jaderným výbuchem, které může způsobit škodlivé proudové a napěťové

rázy, ovlivňující elektrické nebo elektronické systémy. EMP vyvolává velké proudy a napětí, které ničí elektrická zařízení nebo narušují jejich funkčnost. Nepřímým účinkem EMP může být požár elektrických zařízení způsobený přehřátím elektronických komponentů.

2. Činnosti vztahující se k EP mohou například zahrnovat opatření přijatá k zajištění vlastního využívání EMS. Nesmí docházet k záměně EP s defenzivním EA. Přestože obě součásti chrání vlastní síly, zařízení, schopnosti i prostředky, EP provádí ochranu před účinky EA (vlastního i nepřítele) a EM interference, zatímco defenzivní EA primárně chrání před letálními útoky nepřítele, a to znemožněním využití EMS například k navádění nebo odpalu jeho zbraní. Je důležité, aby z pohledu realizace vhodných opatření EP došlo k pochopení aktuálních hrozeb a zranitelnosti vlastních elektronických prostředků, protože jedině tak je možno ochránit vlastní síly, prostředky a zařízení před nepřátelským EA a ES. Mezi činnosti EP patří⁵⁶:
 - a. Elektromagnetická kompatibilita (Electromagnetic Compatibility) – schopnost systémů, prostředků a zařízení využívajících EMS pracovat, aniž by vlivem EM vyzařování nebo odezvy na něj docházelo k nepříjemnému nebo neúmyslnému snížení jejich schopností;
 - b. Zvyšování elektromagnetické odolnosti (Electromagnetic Hardening) – činnost prováděná za účelem ochrany sil, zařízení a/nebo prostředků pomocí technických opatření (filtrace, zeslabování, uzemnění, spojení a/nebo stínění) proti nežádoucím účinkům EM energie;
 - c. Elektronické maskování (Electronic Masking) – řízené vyzařování EM energie na vlastních kmitočtech způsobem, který chrání vyzařování vlastních komunikačních a elektronických systémů proti ESM/SIGINT nepřítele, bez podstatného negativního vlivu na samotnou činnost těchto systémů;
 - d. Management EMS (EMS Management) – plánování, koordinace a správa využívání EMS skrze operační, řídicí a administrativní procedury;
 - e. Řízené vyzařování (EMCON – Emission Control) – selektivní a řízené používání EM, akustických nebo ostatních emitorů k optimalizaci schopností velení a řízení, při minimalizaci (z důvodu operační bezpečnosti):
 - i. Detekce nepřátelskými senzory;
 - ii. Vzájemné interference mezi vlastními systémy;
 - iii. Nepřátelské interference se schopností realizovat vojenský plán klamání;
 - f. Válečné záložní módy/režimy (WARM – Wartime Reserve Modes⁵⁷) – nastavení a operační postupy vlastních senzorů, komunikačních systémů, navigačních prostředků, systémů rozpoznání hrozeb, zbraňových systémů a systémy protiopatření, které budou přispívat ke zvyšování jejich účinnosti, jestliže pro nepřítele zůstanou neznámy anebo jím budou před jejich použitím špatně pochopeny. V případě jejich předčas-

⁵⁶ ref. 45, s. 1-28–1-30

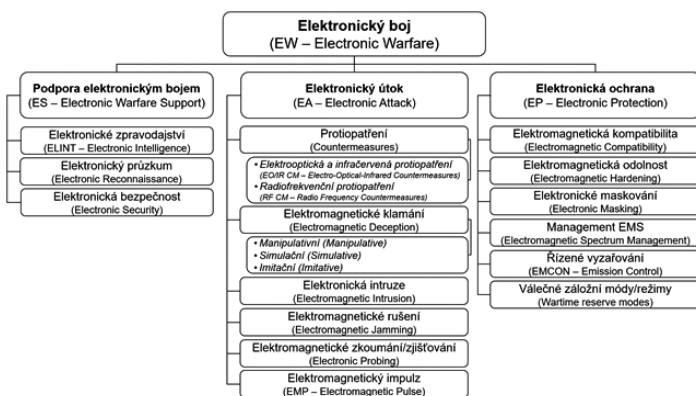
⁵⁷ ref. 42, s. 247

ného prozrazení by mohlo ze strany nepřítele dojít ke zneužití nebo neutralizaci těchto systémů. Válečné záložní módy/režimy jsou záměrně drženy v záloze pro válečné nebo nouzové stavy a zřídka jsou použity mimo konflikt.

3. Realizací činností ES je OS USA umožněno identifikovat EM zranitelnost nepřátelských nebo protivníkových elektronických prostředků a systémů. Znalost této zranitelnosti je vlastními silami využívána při vedení operací EB. Systémy ES OS USA jsou zdroji informací pro okamžitá rozhodnutí, mající vazby k realizaci EA, EP, targetingu a dalšímu taktickému použití vlastních sil. Mezi činnosti ES patří⁵⁸:

- a. Elektronické zpravodajství (ELINT – Electronic Intelligence) – technické a geolokační zpravodajství vyvozené z EM vyzařování cizích zdrojů nekomunikačního charakteru, pocházející od jiných než jaderných výbuchů a radioaktivních zdrojů záření. ELINT je součástí SIGINT;
- b. Elektronický průzkum (Electronic Reconnaissance) – detekce (Detection), určení polohy (Location), identifikace (Identification) a vyhodnocení (Evaluation) cizího EM vyzařování. Elektronický průzkum je použit k aktualizaci a udržení informací o charakteristikách hrozeb. Informace o charakteristikách elektronických hrozeb jsou použity v plánovacích a integračních procesech;
- c. Elektronická bezpečnost (Electronics Security) – ochrana vyplývající ze všech opatření navržených pro znemožnění přístupu neoprávněných osob k hodnotným informacím, které by mohly být získány zachycením a studiem nekomunikačního EM vyzařování, např. radiolokátoru.

Při realizaci úkolů ES a SIGINT mohou být používány stejné nebo podobné zdroje informací. ES se od SIGINT liší záměrem, účelem plněného úkolu, zamýšleným použitím zjištěné informace, mírou vynaloženého analytického úsilí, podrobností poskytovaných informací a požadovanými lhůtami pro splnění jednotlivých úkolů. ES reaguje na bezprostřední požadavky taktického velitele nebo přináší informace pro podporu budoucích kybernetických operací nebo operací EB.



Obrázek č. 3: Rozdělení EB dle pojetí OS USA

⁵⁸ ref. 45, s. 1-30–1-31

Na obrázku č. 3 je znázorněno rozdělení EB vycházející z pojetí OS USA. Pod jednotlivými složkami EB jsou uvedeny činnosti, které jsou v rámci nich realizovány. Kurzívou jsou u ES a elektronického průzkumu označeny úkoly, které při nich SaP EB OS USA plní. U některých anglických termínů je v tak specifické oblasti, jakou je EB, velice obtížné provést adekvátní překlad do českého jazyka. Situaci lze demonstrovat na příkladu ES a úkolů „Locate“ a „Localize“. Ve zde použitém významu je slovo „Locate“ třeba chápat jako určení polohy zdrojů EM vyzařování a slovo „Localize“ ve smyslu ekvivalentního „Assign to“, tedy „Přidělit“. Toto přidělení je vztaženo k úkolu EB, resp. ES, navést vlastní SaP plnící např. úkoly SIGINT, EA nebo targetingu na zdroje EM vyzařování nepřítele za účelem jejich sledování, vytěžení, neutralizace, ničení atd.

Jak bylo napsáno v úvodu této kapitoly, velení OS USA si je plně vědomo kritické závislosti vlastních OS na EMS. Důkazem jsou například vyjádření, která provedli ministr obrany USA Jim Mattis a generál Joe Dunford, předseda Spojeného výboru náčelníků štábů, ke členům senátního podvýboru pro obranu ve Washingtonu, D.C., v rámci slyšení ve věci rozpočtů Ministerstva obrany USA:

pro fiskální rok 2018 (14. 6. 2017): „Naše převaha na zemi v konvenčních vysoce sofistikovaných multifunkčních zbraních, schopných vést manévrový boj, je ohrožena zaváděním zbraní s dlouhým doletem vzduch – země a země – země, moderními obrněnými vozidly a protitankovými zbraněmi, a taktickými systémy elektronického boje.“⁵⁹;

pro fiskální rok 2019 (9. 5. 2018): „Rozpočet pro fiskální rok 2019 bude i nadále pokračovat v investicích do nejdůležitějších prostředků armády – vojáků, s nárůstem finančních prostředků na platy o 2,6 %. Připravenost a bojová účinnost budou zvýšeny navýšením finančních prostředků, nárůstem počtu pracovních sil, snížením počtu dnů plnění služebních úkolů mimo domácí posádky a zachováním souboru dovedností v oblastech kybernetických operací, elektronického boje a speciálních operací.“⁶⁰

Z výše uvedených vyjádření je patrné, že uvědomování si reálně existujících hrozeb, stejně jako vlastní závislosti úspěchu OS na vybojování nadvlády a udržení si převahy v EMS jsou důvody, díky kterým nejenom v současnosti, ale i blízké budoucnosti budou OS USA nadále investovat do všestranného rozvoje bojeschopnosti v oblasti EB.

3 ELEKTRONICKÝ BOJ V ARMÁDĚ ČESKÉ REPUBLIKY

EB je v AČR zastřešován Odborem vojenského průzkumu a elektronického boje MO (OVPzEB MO). OVPzEB MO, který mimo jiné plní úlohu zpravodajského štábu náčelníka Generálního štábu AČR, je koncepčním orgánem pro rozvoj a řízení prvků zpravodajství, průzkumu a EB, vojenské geografie a hydrometeorologie AČR a orgánem řízení výstavby

⁵⁹ *Secretary of Defense Jim Mattis, Senate Appropriations Subcommittee on Defense, Written Statement for the Record* [online]. 2017 [cit. 2018-08-05]. Dostupné z: <https://www.appropriations.senate.gov/imo/media/doc/061417-Mattis-Testimony.pdf>, s. 6

⁶⁰ *Secretary of Defense Jim Mattis, Senate Appropriations Subcommittee on Defense, Written Statement for the Record* [online]. 2018 [cit. 2018-08-05]. Dostupné z: <https://www.appropriations.senate.gov/imo/media/doc/050918%20-%20FY19%20DoD%20Mattis%20Testimony.pdf>, s. 10

sil a prostředků zpravodajství, sledování a průzkumu (ISR – Intelligence, Surveillance, Reconnaissance⁶¹).⁶² Metodou terénního šetření bylo nestandardizovanými rozhovory s příslušníky OVPzEB MO zjištěno, že ČR, jakožto člen NATO, přistoupila ke všem současně platným standardizačním dohodám NATO v oblasti EB (viz kapitola 2 Elektronický boj v NATO). Do současné doby byl zaveden formou předpisu pouze STANAG 6018, Ed: 3, Allied Joint Doctrine for Electronic Warfare – AJP-3.6 EDITION B, který je klasifikován jako dokument NATO RESTRICTED, a proto jeho analýza nemůže být předmětem tohoto článku. Ostatní STANAG, ke kterým ČR v oblasti EB přistoupila, jsou postupně za řízení OVPzEB MO zpracovávány tak, aby mohly být v souladu se schváleným plánem pro koncepční rozvoj ve stanovených termínech zavedeny k používání v AČR.

V AČR je v současnosti jedinou platnou vojenskou doktrínou z oblasti EB, která nespadá ani do oblasti OUI ani UNI, Pub-20-63-03, Elektronický boj v AČR. Účelem jejího zpracování bylo objasnit základní pojetí EB v AČR v souladu s tehdejšími pojetím EB v NATO a v návaznosti na tehdy platné dokumenty NATO. Doktrína byla zpracovávána s přihlédnutím k národním zvláštnostem chápání EB a má pouze doporučující charakter.⁶³ Přestože její tvorba vycházela z dokumentů NATO, do jisté míry reflektovala rovněž přístupy k EB v OS USA, které byly známy a zaujímaný v letech 2008–2010, tj. době, kdy byla připravována a vydána.

V Pub-20-63-03 je EB v AČR definován jako vojenská činnost, zahrnující použití EM a směřované energie, vedená s cílem ztížit nebo znemožnit využití EMS protivníkem a řídit činnosti k zabezpečení efektivního využití EMS vlastními silami. Jeho úkolem je vybojovat a udržet elektronickou nadvládu v prostoru operace a tím získat výhody pro vlastní velitele a štáby v jejich plánovacím a rozhodovacím procesu, stejně jako získat výhody pro vlastní vojska při vedení jejich bojové činnosti v EME.⁶⁴

EB byl v této doktríně rozdělen do tří základních složek, z nichž každá plnila svoji specifickou úlohu ať již v závislosti na ostatních složkách, nebo samostatně⁶⁵:

1. Elektronická podpora (EPo) – je pasivní (není vyzařována vlastní EM energie) součást EB, zahrnující pátrání, zachycení, identifikaci, zaměření a zjištění polohy zdroje úmyslného nebo neúmyslného vyzařování EM energie pro účely okamžitého rozpoznání hrozeb, targetingu, plánování a vedení následných operací. Poskytuje informace potřebné pro okamžitá rozhodnutí v oblasti vlastní elektronické ochrany, elektronického působení a v dalších taktických činnostech. Úkoly EPo jsou v rámci AČR plněny SaP rádiového a radiotechnického průzkumu (RPz a RTPz), které jsou organizačně začleněny v AČR v sestavě jednotek EB;

⁶¹ ref. 2, s. 143

⁶² Odbor vojskového průzkumu a elektronického boje MO [online]. 2018 [cit. 2018-08-08]. Dostupné z: <http://www.acr.army.cz/struktura/generalni-stab/odbor-vojskoveho-pruzkumu-a-elektronickeho-boje-mo-ovpzeb-mo-13587/>

⁶³ Pub-20-63-03, *Elektronický boj v AČR*. Vyškov: Institut doktrín VeV – VA, 2010, s. 3-4

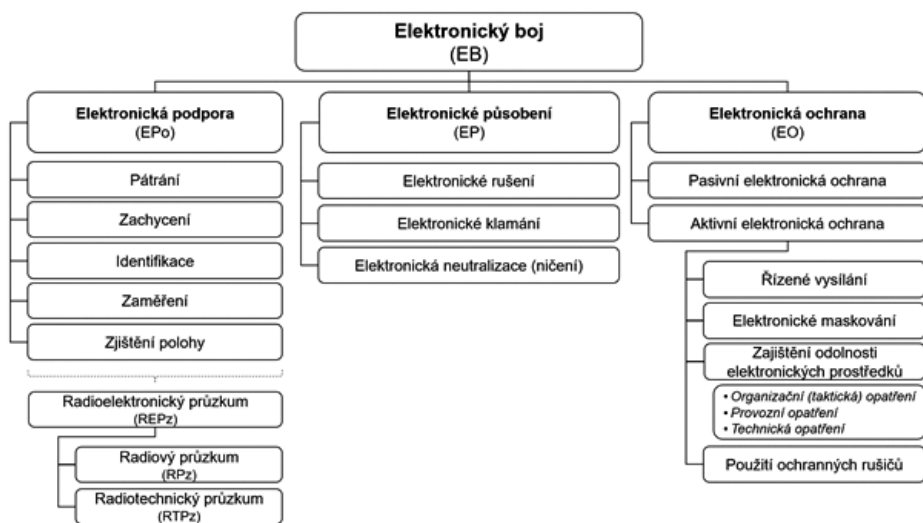
⁶⁴ ref. 63, s. 14

⁶⁵ ref. 63, s. 15-30

2. Elektronické působení (EP) – aktivní (ofenzivní) součást EB, zahrnující použití EM nebo směrované EM energie k působení proti silám, prostředkům nebo vybavení protivníka. EP se dělí na tři složky:
 - a. Elektronické rušení – úmyslné vyzařování, zpětné vyzařování nebo odražení EM energie s cílem snížení efektivnosti elektronických zařízení, prostředků nebo systémů protivníka;
 - b. Elektronické klamání – úmyslné vyzařování, změny, pohlcování nebo odražení EM energie za účelem oklamání, odvrácení pozornosti nebo svedení protivníka a jeho elektronických systémů;
 - c. Elektronická neutralizace (ničení) – cílené využití EM energie k dočasnému umlčení nebo trvalému zničení (elektronické ničení – zbraně se směrovanou energií) elektronických zařízení protivníka, která ke své činnosti využívají EMS;
3. Elektronická ochrana (EO) – součást EB, zahrnující činnosti k zajištění ochrany vlastních sil, prostředků nebo vybavení efektivním využitím EMS proti působení protivníka. EO tvoří dvě části:
 - a. Pasivní elektronická ochrana (pasivní opatření elektronické ochrany) – nezjistitelná (nedetekovatelná) opatření k zajištění efektivního využití EMS vlastními SaP;
 - b. Aktivní elektronická ochrana (aktivní opatření elektronické ochrany) – zjistitelná (detekovatelná) opatření k zajištění efektivního využití EMS vlastními SaP. Do aktivních opatření EO patří:
 - i. Řízené vysílání (řízené vyzařování EM energie) - selektivní řízení EM vyzařování, ovlivňující možnosti protivníka toto vyzařování zachytit a využít. Řízení vysílání je realizováno především cestou regulace vyzařovaných výkonů, použitím směrových antén a volbou vhodné základny;
 - ii. Elektronické maskování – vyzařování EM energie na vlastních kmitočtech způsobem, který ochraňuje (kryje) vlastní spojení a elektronické systémy před radioelektronickým průzkumem protivníka, bez výrazného omezení činnosti vlastních systémů;
 - iii. Zajištění odolnosti elektronických prostředků zahrnují následující opatření:
 1. Organizační (taktická) opatření k použití elektronických prostředků – opatření štábů, využívající teoretických poznatků a takticko-technických zásad použití (rozvinutí) SaP, které umožní vyloučit nebo alespoň předvídat případy ohrožení funkce vlastních elektronických prostředků, připravit se na ně, a tak snížit účinky působení EB protivníka;
 2. Provozní opatření – opatření obsluh, jejichž základem jsou stálé operační postupy (metodiky práce) obsluh pro použití EO a postupy k obnově odolnosti a tím i funkce elektronických prostředků;

3. Technická opatření – zahrnují možnosti, které poskytuje používaná technika. Jejich podstatnou součástí jsou požadované a realizované parametry elektronických prostředků zaváděných do výzbroje a jejich úprava (modernizace);
- iv. Použití ochranných rušičů – využití EM energie vyzařované vlastními prostředky (rušiči) za účelem znemožnění dálkového odpálení improvizovaného výbušného zařízení protivníkem.

Vizualizace EB AČR, vycházející ze skutečností uvedených v Pub-20-63-03, je znázorněna na obrázku č. 4.



Obrázek č. 4: Rozdělení EB AČR dle vojenské doktríny Pub-20-63-03

Pub-20-63-03 byla vydána v roce 2010. V květnu 2012 bylo přistoupeno ke STANAG 6018, která se v září 2014 zavedla do používání v podmínkách AČR. Nedošlo však ke zrušení nebo alespoň k aktualizaci obsahu stávající verze Pub-20-63-03, která by do jisté míry implementací veřejnosti přístupných informací o EB NATO vysvětlovala současný přístup AČR k EB. AČR dnes nemá veřejně přístupný materiál uceleně popisující oblast EB v AČR, který by alespoň částečně reflektoval závazný, prostřednictvím předpisu zavedená STANAG 6018. Dlouhodobě přetrvávající neujasněnost pojmového aparátu pro EB v AČR, která by odrážela STANAG 6018, stejně jako jeho omezená znalost a to dokonce i mezi příslušníky odborné komunity EB AČR, nepřispívají k jednotnému pochopení přístupu a rozvoji odborné diskuze na téma EB.

4 KOMPARACE PŘÍSTUPŮ K OBLASTI ELEKTRONICKÉHO BOJE NATO, OZBROJENÝCH SIL SPOJENÝCH STÁTŮ AMERICKÝCH A ARMÁDY ČESKÉ REPUBLIKY

Komparací analyzovaných informací uvedených v kapitolách 2 Elektronický boj v NATO, 3 Elektronický boj v OS USA a 4 Elektronický boj v AČR a terénním šetřením byly zjištěny následující skutečnosti:

1. Přístup k oblasti EB je v NATO odlišný od pojetí EB v OS USA, a to jak v základním rozdělení EB, jeho složkách a jejich obsahové náplni, tak i v používaném pojmovém aparátu. Markantní rozdíly jsou nejenom v chybějících opatřeních ESM, ECM a EPM v EB OS USA, ale i ve vydefinování pojmů, o kterých NATO samostatně vůbec nehovoří (Elektromagnetická intruze (Electromagnetic Intrusion), Elektromagnetické zkoumání/zjišťování (Electronic Probing), Zvyšování elektromagnetické odolnosti (Electromagnetic Hardening)). NATO a OS USA rovněž používají v oblasti EB shodné zkratky, které však mají jiný význam (např. ES – Electronic Surveillance (NATO) / Electronic Warfare Support (OS USA));
2. Terénním šetřením bylo zjištěno, že aktuálně příslušníci AČR přistupují k oblasti EB dle Pub-20-63-03, která je jim dostupná, avšak nereflektuje přístup NATO k EB, popsáný v zavedené STANAG 6018. Teoretické znalosti nejenom specialistů, ale i ostatních příslušníků AČR jsou v oblasti EB negativně ovlivněny chybějícími národními vojenskými předpisy a vojenskými publikacemi pro danou oblast. Terénní šetření odhalilo, že situace je směrem k této oblasti natolik nejasná, že ani mezi specialisty EB AČR nepanuje ve vztahu k oficiálnímu přístupu AČR k EB jednotný názor. Jen několik málo osob je schopno o vojenských předpisech a vojenských publikacích EB AČR i NATO vést odbornou diskusi a o jejich obsahu poskytnout relevantní informace;
3. Dostupné materiály OS USA popisující přístup k oblasti EB, šířené na oficiálních webových stránkách OS USA, přispívají k informovanosti široké veřejnosti o dané problematice, a to jak z hlediska chápání vlastních schopností, tak i hrozeb, které sebou využití EMS nepřítelem přináší. Veřejná informovanost zcela jistě přispívá k obecné podpoře úsilí OS USA budovat převahu v EMS, následovaná podporou finanční, materiální a personální, které jsou pro rozvoj této vojenské schopnosti nezbytné;
4. Relativně snadná dostupnost základních neklasifikovaných informací o řešení otázek EB v OS USA spojená s obecným povědomím o členství USA v NATO vede k hrozbě vytvoření mylného závěru o shodnosti přístupů OS USA a NATO k EB. Tento chybný závěr byl v několika případech patrný i z výsledků výše uvedeného terénního šetření, provedeného zejména na taktickém stupni AČR. Záměna přístupů je patrná i z informací otevřených zdrojů šířených zejména prostřednictvím sítě Internet, kdy je v některých elektronických materiálech o EB odkazováno na přístup NATO, ale ve skutečnosti se obsahová stránka informací týká přístupu OS USA;
5. Translace některých skutečností ve vztahu k oblasti EME a činností v něm, uvedená v současně zveřejněné české verzi AAP-06 (2015), není v kontextu původní odborné terminologie a vojenských publikací NATO pro oblast EB správná, což

má negativní dopad zejména na pochopení významu takto přeložených termínů (např. ESM – Electronic Warfare Support Measures: uvedeno elektronická podpůrná opatření (s. 131) a opatření pro zabezpečení EB (elektronické zabezpečení) (s. 358) místo podpůrná opatření EB; zkratka pro Electronic Defence: uvedená i EA (s. 130) místo ED (s. 357); ELINT – Electronic Intelligence: uvedeno zpravodajská informace elektronického zpravodajství (s. 5, 130 a 357) místo elektronické zpravodajství; COMINT – Communications Intelligence: uvedeno i rádiový průzkum (s. 90) místo komunikační zpravodajství (s. 356); SIGINT – Signals Intelligence: uvedeno i rádiový průzkum (s. 300) místo signálové zpravodajství (s. 364)).⁶⁶ Terminologická disproporce je i v českém překladu AAP-15 (2016) (např. SIGINT – Signals Intelligence: uvedeno radiotechnický průzkum (s. 268) místo signálové zpravodajství; EPM – Electronic Protective Measures: uvedeno i elektronická ochrana (s. 100) místo elektronická ochranná opatření (s. 100); ECM – Electronic Countermeasures: uvedeno i elektronické působení (s. 96) místo elektronická protipatření (s. 96)).⁶⁷ Jak je z výše uvedených příkladů patrné, tak nesoulad je rovněž mezi některými českými překlady AAP-06 (2015) a AAP-15 (2016) navzájem;

6. Současně zveřejněná česká verze AAP-06 (2015)⁶⁸ publikovaná Úř OSK SOJ – OOS není pro vysvětlení soudobého pojetí EB v NATO postačující, neboť neobsahuje všechny pojmy z oblasti EB jako poslední verze AAP-6 (2017)⁶⁹ (CESMO – Co-operative Electronic Support Measure Operations (s. 30), EMB – Electromagnetic Battlestaff (s. 41), EMO – Electromagnetic Operations (s. 41), EMS – Electromagnetic Spectrum (s. 41), REMP – Recognized Electromagnetic Picture (s. 95));
7. Komparaci přístupů NATO a OS USA k EB nelze stanovit, který z daných přístupů je správnější, neboť nahlíží na EB každý z částečně odlišné perspektivy. Oba přístupy jsou podpořeny dalšími dokumenty doktrinálního charakteru a v souhrnu tvoří kompaktní celky komplexně řešící oblast EB v NATO nebo EB v OS USA. Tato situace však nenastává u přístupu popsaného v Pub-20-63-03, který nereflektuje aktuální stav EB v AČR a neodpovídá ani pro AČR závaznému přístupu NATO k EB.

ČR patří v NATO dlouhodobě mezi státy, které se aktivně podílí na rozvoji oblasti EB, čímž získala v odborné komunitě EB renomé. Úspěch ČR a dlouhodobě vynikající výsledky AČR v této oblasti jsou ale více svázány s praktickým vedením činností v EMS, plněním úkolů EB v rámci bojové podpory bojových jednotek a s technickou a technologickou stránkou výzkumné, vývojové a produkční činnosti českého průmyslu nežli se samotným doktrinálním ukotvením EB.

Soudobému EB v AČR, který navázal na činnosti SaP radioelektronického boje, RPz a RTPz plnění úkolů v EMS v dobách studené války, se nepodařilo úplně oprostit od tehdy běžně zaužívaných, ale v NATO neexistujících přístupů. Typickou ukázkou tohoto pro AČR již neaktuálního přístupu je stále rozdělování SaP EB na ty, které plní úkoly RPz a RTPz. Tento nesprávný přístup je pak často umocňován snahou překládat činnost RPz

⁶⁶ ref. 12

⁶⁷ ref. 2

⁶⁸ ref. 12

⁶⁹ ref. 15

termínem COMINT⁷⁰ nebo v NATO neexistujícím anglickým překladem Communications Reconnaissance⁷¹ a RTPz jako Electronic Intelligence⁷² (ELINT). Uvedené příklady potvrzují nesprávné pochopení současné problematiky EB NATO ve vztahu k oblasti SIGINT, kdy nelze SIGINT (tj. COMINT a ELINT) s ESM ani slučovat, ani zaměňovat. Přitom bychom z hlediska správné terminologie a přístupu NATO k EB, k jehož zavedení se ČR zavázala, měli hovořit o tom, že se SaP EB AČR v EME podílejí na plnění úkolů elektronického sledování, které naplňují výhradně realizací vlastních ESM. V rámci nich pak plní úkoly vyhledávání, zachycení, identifikace a upřesnění zdrojů EM vyzařování. Jedině při dodržování tohoto přístupu bude AČR a její příslušníci schopni terminologicky správně komunikovat s partnery z NATO.

5 NÁVRHY A DOPORUČENÍ

Terénní šetření jednoznačně ukázalo na závažnost problému nejednotného chápání problematiky činností v EME a přístupu k EB v AČR, plynoucích z neexistence národních vojenských předpisů a vojenských publikací. Problém je o to závažnější, uvědomíme-li si provázanost EME se všemi klasickými operačními prostory a zcela zásadní závislost AČR, stejně jako ostatních moderních armád NATO, na moderních elektronických zařízeních a šíření EM energie jako takové. Nápravu stávajícího stavu lze řešit následujícími návrhy a doporučeními, realizovanými nad rámec plánu OVPzEB MO pro koncepční rozvoj, řešící zavádění STANAG pro oblast EB:

1. Rozšíření pracovní skupiny specialistů EB, kteří dle přesně stanoveného a ředitelem OVPzEB MO schváleného harmonogramu zahájí v oblasti EB postupné naplňování plánu vedoucího k odstranění nedostatků ve vojenské terminologii, vojenských předpisech a vojenských publikacích EB v AČR;
2. Provedení revize termínů, definic a zkratk z oblasti EME v českých překladech AAP-06 (2015) a AAP-15 (2016), vytvoření návrhu pro jejich sjednocení, porovnání s aktuálními verzemi originálu AAP-6 a AAP-15 a vytvoření návrhu překladu aktuálních verzí;
3. Zrušení Pub-20-63-03 a vytvoření nové vojenské publikace, anebo aktualizace stávající verze Pub-20-63-03, která v návaznosti na veřejnosti dostupné informace o EB v NATO a informace ve vztahu k realizaci EB v AČR poskytnou základ k otevřené odborné diskusi na téma EME a EB. Dané informace nesmí být klasifikovány jako UI nebo UNI, neboť je třeba vytvořit vojenskou publikaci poskytující základní informace jak pro potřeby rezortu MO ČR, ale i mimo něj. Pro inspiraci lze vyjít z volně dostupných vojenských publikací OS USA pro EB a EME⁷³, pokud tyto svým obsahem nejsou v rozporu s přístupem NATO nebo AČR k EB;

⁷⁰ ref. 12, s. 90

⁷¹ ref. 63, s. 50

⁷² ref. 63, s. 50

⁷³ ref. 39, 40, 41

4. Provedení překladu přijaté a v AČR zavedené STANAG 6018 a přijatých STANAG 3873 a STANAG 6010, vše v souladu s odsouhlasenou revizí termínů, definic a zkratk z oblasti EME v aktuálních verzích AAP-6 a AAP-15, navrhovanou v bodu 2 těchto návrhů a doporučení.

Realizace výše uvedených návrhů a doporučení je v odborné rovině EB záležitostí minimálně několika měsíců intenzivní práce expertů z této oblasti. Bez ní nikdy nedojde ke sjednocení náhledů AČR na oblast EB a provázání s přístupem NATO k EB.

ZÁVĚR

V soudobém vedení bojové činnosti nejsou operace v EME a EB jako takový problematikou, týkající se pouze úzké skupiny specialistů EB. Závislost na EME je aktuálním tématem nejenom současných, ale i budoucích operací od taktické, až po strategickou úroveň. Je přímo úměrná technické a technologické vyspělosti aktérů konfliktu, jejich schopnosti využívat a řídit aktivity v EMS a bojeschopnosti vlastních vojsk vést operace v EME. Opatření EB a úkoly pro jeho SaP nejsou izolovány od bojové činnosti bojových jednotek. Efektivní a účinná bojová podpora EB, poskytovaná bojovým jednotkám v prostoru operace, musí být schopna adekvátně a s dostatečnou flexibilitou reagovat na změny situace v EME. Všechny činnosti, na kterých se EB v EME podílí, musí být dobře zplánovány a zkoordinovány s ostatními aktivitami vlastních sil.

EB a činnostem v EME by měl v základní rovině porozumět každý voják. Velitelé musí rozvíjet své schopnosti vést operace v EME, a to nezávisle na tom, zda přímo velí či řídí SaP EB. Rozvíjení vojenského umění směrem k EME je totiž jedním z aspektů, který v podstatné míře nejenom ovlivňuje bojeschopnost vlastních vojsk, ale zároveň může rozhodnout i o celkovém vítězství. Správné pochopení EB a existence specifických přístupů k němu je jedním z klíčových předpokladů pro vybojování a udržení nadvlády v EMS. Bez definování a respektování jednotného přístupu k EB na národní úrovni, který bude jasně svázán s chápáním EB v NATO, nelze nikdy dosáhnout mezi jednotlivými OS členských států NATO plnohodnotné interoperability. Ta je závislá nejen na standardizaci v oblasti technické, ale i dodržování stálých operačních postupů a dohodnutých pravidel taktiky a operačního použití, které odrážejí potřebu vzájemné koordinace a synchronizace společného úsilí vedoucího k naplnění cílů operace.

Interoperabilita je jednou z klíčových schopností moderních SaP na bojišti. V přímé úměře k reálné vzrůstající schopnosti SaP vzájemně kooperovat a plnit úkoly v soudobém i budoucím EME prostupujícím napříč všemi klasickými operačními prostory bude docházet ke zvyšování možností jejich operačního použití. Činnost vlastních SaP bude vystavena působení EB protivníka a naopak. SaP EB, které jsou nosnou, nikoliv však jedinou složkou vedoucí vojenské činnosti (ES, EA, ED) v EME nebudou již působit samostatně, ale v rámci EMO. Je nutné, aby v ČR došlo ke sjednocení chápání přístupu AČR k EB a k činnostem v EME jak mezi odbornou, tak i laickou veřejností. Současně s tím musí dojít k vytvoření podmínek pro vedení terminologicky správné odborné diskuze k dané problematice. Je nezbytné nahradit stávající nevyhovující Pub-20-63-03 novou vojenskou publikací. Nová vojenská publikace by měla reflektovat přístup AČR k oblasti EB

v souladu se současně platnými standardizačními dohodami NATO v oblasti EB, ke kterým ČR přistoupila a které postupně zavádí. Bylo by vhodné, aby tato vojenská publikace neobsahovala UI a UNI a mohla být přístupná široké veřejnosti. Jejím zformováním dojde k ukotvení pojmového aparátu v návaznosti na reálnou činnost v EME a k vytvoření podmínek pro vznik názorové jednoty mezi AČR a civilním sektorem, reprezentovaným například českým obranným a bezpečnostním průmyslem nebo vývojovými a vědeckými pracovišti. V samostatné kapitole by se vojenská publikace měla zabývat vysvětlením rozdílnosti přístupu OS USA k EB, protože s tímto přístupem je nejčastěji laická i odborná veřejnost konfrontována. Na základě výsledků analýzy a výstupů komparace by měla být kompetentními orgány AČR iniciována revize překladů termínů z oblasti EB, které jsou součástí přeložených AAP-6 (2015) a AAP-15 (2016) a neodpovídají originálu. Zároveň by měl být vznesen požadavek na překlad termínů z oblasti EB ze současně platného originálu AAP-6 (2017), protože dnes do českého jazyka přeložená verze AAP-6 (2015) tyto termíny neobsahuje. Jen tak bude možné specialisty EB AČR provést správný překlad již zavedeného STANAG 6018 a přijatých STANAG 3873 a STANAG 6010 pro jejich následné zavedení do podmínek AČR.

Seznam použitých zkratk

Zkratka	Anglický termín	Český termín
AAP	Allied Administrative Publication	Spojenecká administrativní publikace
AČR		Armáda České republiky
AEP	Allied Engineering Publication	Spojenecká technická publikace
AJP	Allied Joint Publication	Spojenecká společná publikace
ATP	Allied Tactical Publication	Spojenecká publikace pro taktiku
BR	Battle Rhythm	Časový plán činnosti
BSM	Battle space Spectrum Management	Management kmitočtového spektra bojiště
CEMA	Cyber Electromagnetic Activities	Kyberneticko-elektromagnetické činnosti
CESMO	Co-operative Electronic Support Measure Operations	Společné operace v oblasti elektronických podpůrných opatření
COMINT	Communication Intelligence	Komunikační zpravodajství
ČR		Česká republika
DE	Directed Energy	Směřovaná energie
DOD	Department Of Defence	Ministerstvo obrany
EA	Electronic Attack	Elektronický útok
EB		Elektronický boj
ECM	Electronic Countermeasures	Elektronická protipatření
ED	Electronic Deception	Elektronické klamání
ED	Electronic Defence	Elektronická obrana
EJ	Electronic Jamming	Elektronické rušení
ELINT	Electronic Intelligence	Elektronické zpravodajství

EM	Electromagnetic	Elektromagnetický
EMB	Electromagnetic Battlestaff	Personál štábu pro plánování a vedení bojové činnosti v elektromagnetickém prostředí
EMCON	Emission Control	Řízené vyzařování
EME	Electromagnetic Environment	Elektromagnetické prostředí
EMO	Electromagnetic Operations	Elektromagnetická operace
EMS	Electromagnetic Spectrum	Elektromagnetické spektrum
EMSO	Electromagnetic Spectrum Operations	Operace v elektromagnetickém spektru
EMP	Electromagnetic Pulse	Elektromagnetický impulz
EN	Electronic Neutralization	Elektronická neutralizace
EO		Elektronická ochrana
EOD	Explosive Ordnance Disposal	Likvidace výbušného materiálu
EP	Electronic Protection	Elektronická ochrana
EP		Elektronické působení
EPM	Electronic Protective Measures	Elektronická ochranná opatření
EPo		Elektronická podpora
ES	Electronic Surveillance	Elektronické sledování
ES	Electronic Warfare Support	Podpora elektronickým bojem
ESM	Electronic Warfare Support Measures	Elektronická podpůrná opatření
EW	Electronic Warfare	Elektronický boj
EWCC	Electronic Warfare Coordination Cell	Skupina koordinace elektronického boje
FM	Field Manual	Polní manuál (příručka)
ISR	Intelligence, Surveillance, Reconnaissance	Zpravodajství, sledování, zjišťování cílů a průzkum
ISTAR	Intelligence, Surveillance, Target Acquisition, Reconnaissance	Zpravodajství, sledování, zjišťování cílů a průzkum
JEMSO	Joint Electromagnetic Spectrum Operations	Společné operace v elektromagnetickém spektru
JEMSOC	Joint Electromagnetic Spectrum Operations Cell	Skupina společných operací v elektromagnetickém spektru
JFC	Joint Force Command	Velitelství společných sil
JP	Joint Publication	společná publikace
JDN	Joint Doctrine Note	Podpůrná doktrína ke společné publikaci
MC	Military Committee	Vojenský výbor
MO		Ministerstvo obrany
NATO	North Atlantic Treaty Organization	Severoatlantické organizace
NAVWAR	Navigation Warfare	Navigační boj
NSO	NATO Standardization Office	Organizace NATO pro standardizaci
OS		Ozbrojené síly
OVPzEB MO		Odbor vojskového průzkumu a elektronického boje MO
Pub		Vojenská publikace
RCIED	Radio-controlled Improvised Explosive Device	Rádiově ovládané improvizované výbušné zařízení

REM	Recognized Electromagnetic Picture	Přehled o elektromagnetické situaci
RF CM	Radio Frequency Countermeasures	Radiofrekvenční protiopatření
RMO		Rozkaz ministra obrany
RPz		Radiový průzkum
RTPz		Radiotechnický průzkum
SA	Situational Awareness	Znalost situace
SaP		Síly a prostředky
SEAD	Suppression of Enemy Air Defences	Potlačení protivzdušné obrany nepřítele
SIGINT	Signal Intelligence	Signálové zpravodajství
STANAG	Standardization Agreement	Standardizační dohoda
STANREC	Standardization Recommendation	Standardizační doporučení
UI		Utajované informace
UNI		Určené neutajované informace
Úř OSK SOJ – OOS		Úřadu pro obrannou standardizaci, katalogizaci a státní ověřování jakosti – Odboru obranné standardizace
USA	The United States of America	Spojené státy americké
VeV – VA		Velitelství výcviku – Vojenská akademie
VZP		Voják z povolání
WARM	Wartime Reserve Modes	Válečné záložní módy/režimy

Autor: ***Pplk. Ing. Petr Hlavizna**, narozen v roce 1975. Je absolventem Vojenské akademie v Brně (2000). Působil v technických i štábních funkcích v oblastech elektronického boje (EB) a zpravodajství, včetně zahraničních pracovišť. V současné době pracuje na Katedře zpravodajského zabezpečení Univerzity obrany v Brně. Zabývá se problematikou v oblastech zpravodajství, sledování, průzkumu (ISR) a EB.*

Jak citovat: HLAVIZNA Petr. Komparace přístupů k elektronickému boji. *Vojenské rozhledy*. 2018, 27 (4), 078-104. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz.