

„The real target in war is the mind of the enemy commander, not the bodies of his troops.“ [1]

Captain Sir Basil Liddell Hart,

Thoughts on War, 1944

Současná doba je charakteristická mohutným rozvojem komunikačních a informačních technologií, čímž se šíření, dostupnost a využití informací stává snazším. S jejich pomocí získáváme obraz o událostech, které se dějí v okolním prostoru a napomáhají nám utvářet si svůj názor a postoj k těmto událostem. Informace tak představují velký potenciál, s jehož pomocí lze ovlivňovat chování a postoje osob, v konečném důsledku i jejich rozhodování. Zkušenosti z posledních válečných konfliktů dokazují, že řízením šíření informací lze zabezpečit podporu nejen vojenských operací, ale i politického a diplomatického úsilí. Proto je vhodné takové řízení rozšiřování informací provádět dostupnými prostředky a způsoby, s cílem ovlivňovat posluchače, diváky a čtenáře (příjemce informací) a získávat jejich podporu.

Při plánování této činnosti čelí řídicí orgány zásadnímu problému, jak splnit nebo dosáhnout požadovaného výsledku s minimálními ztrátami a maximálním ziskem. V konečném důsledku vyřešení uvedeného problému napomáhá posilovat důvěru v řídicí orgány mezi podřízenými a posiluje morálku. V ozbrojených silách je na vyřešení uvedeného problému kladen velký důraz, protože při dosahování požadovaného výsledku, může dojít i ke ztrátám na lidských životech. Při dosažení úspěchu s minimálními ztrátami na životech vojáků, a rovněž i mezi civilními obyvateli, nejenže potvrzuje správnost přijatých rozhodnutí, ale jako vedlejší účinek, napomáhá posilovat morální složku vojenské síly.

Morální složka – společně s fyzickou a koncepční – tvoří vojenskou sílu. Doktrína AČR charakterizuje morální složku jako odhodlání (vůli) lidí bojovat za zájmy státu a jeho občanů, což se projevuje v motivaci, umění velet a řízení. Proto může být rozhodovací proces předmětem působení protivníka nebo potenciálního protivníka (dále druhé strany) za účelem následného ovlivnění morální síly. Příklady ovlivňování rozhodování velitelů můžeme najít v různých studiích o válkách či v teoriích vedení válek. Všechny se shodují na tom, že ovlivnění rozhodovacího procesu se provádí přes informace, jejich zdroje, prostředky šíření a příjemce.

Definice a poslání informačních operací

Armády USA, Velké Británie, SRN a vůbec států NATO vedou k ovlivnění rozhodovacího procesu tzv. **informační operace** (Information Operations - INFO OPS nebo IO). Jde o relativně novou oblast, která na základě vývoje nových komunikačních a informačních technologií, spolu s využíváním nových forem komunikace nahrazuje boj v oblasti velení a řízení, informační válku (C2W - Command and Control Warfare).

Doktrína AČR, vydaná v roce 2001, definuje informační operace v podmínkách AČR jako **akce prováděné k ovlivňování řídicích orgánů pro podporu politických a vojenských cílů působení**

ním na informace potenciálního protivníka nebo protivníků a jeho nebo jejich informačních procesů v systému velení a řízení, komunikačního a informačního systému, a současně umožnit využívání a ochranu svých vlastních informací a informačních systémů.

V dílčí studii Ústavu strategických studií VA Brno pod názvem „Informační operace Armády České republiky“, vydané v roce 2002 pod označením S-2-016, jsou informační operace v podmínkách AČR definovány jako **souhrn koordinovaných činností k ovlivnění rozhodovacího procesu potenciálního protivníka a jeho spojenců působením na jeho informace, informační procesy a komunikační infrastrukturu při současném využívání a ochraně vlastních informací a komunikační infrastruktury.**

Z porovnání uvedených definic vychází, že informační operace představují souhrn vojenských činností [2], jejichž použití je koordinováno k působení na zdroje, prostředky šíření a příjemce informací a k ochraně vlastních zdrojů a prostředků.

Podle směru předpokládaného použití vojenských činností, informační operace rozdělujeme na útočné (ofenzivní) a obranné (defenzivní).

Místo a úloha informačních operací

Nejnovější studie [3] o vedení války docházejí k závěru, že v plánovacím procesu a řízení budoucích válek bude dosažení požadovaného výsledku záviset na kvalitě a kvantitě získaných informací. Snahou bude dosažení **informační převahy** nad řídicími orgány druhé strany, což může sehrávat větší roli než dosažení převahy ve fyzické složce vojenské síly. Dosažení informační převahy sehraje stejnou roli jako dosažení vzdušné převahy v průběhu druhé světové války.

„We will have to say that in any cause the decisive role does not belong to technology - behind technology there is always a living person without whom technology is dead.“ [4]

*Michal Frunze,
1985*

Informační převaha ve své ideální podobě vytváří podmínky k plnému využívání naší komunikační infrastruktury, získávání a využívání takových informací. Její dosažení není důležité pouze ve vojenství, ale její místo a význam můžeme najít i v diplomatickém, ekonomickém a politickém úsilí daného státu při řešení krize vnějšího charakteru (dále krize).

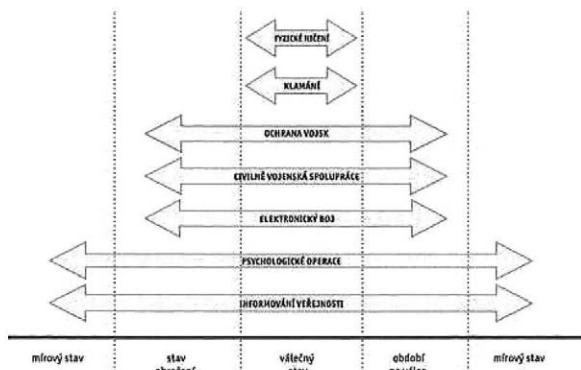
Musíme však vzít v úvahu, že i řídicí orgány druhé strany se budou snažit získat informační převahu. Proto dojde k **informační válce**, jež ale nebude vedena samostatně. V oblasti vojenství bude součástí války jako takové, s cílem podporovat vedení vojenských operací.

V podmínkách AČR budou informační operace představovat prostředek k vedení informační války s cílem získání informační převahy, a to nejen ve vojenské oblasti, ale rovněž k podpoře diplomatického (např. hrozba použití síly), ekonomického (např. podpora mezinárodních sankcí) a politického úsilí České republiky k vyřešení krize. Informační operace představují určitou strategii, jsou plánovány a řízeny centrálně, ale vedeny decentrálně.

Síly a prostředky AČR k vedení informačních operací

AČR může k vedení informačních operací ve vojenské oblasti použít síly a prostředky k fyzickému ničení, klamání, elektronického boje, k zajištění ochrany vojsk, orgány civilně-

-vojenské spolupráce a komunikace s veřejností a nově budované síly a prostředky k vedení psychologických operací (viz obr.)



Obr.: Grafické znázornění vojenských činností k vedení informačních operací v jednotlivých obdobích

Posláním **fyzického ničení**, jako jednoho z nejstarších způsobů vojenské činnosti k podpoře vedení útočných informačních operací, je neutralizace nebo zničení prostředků šíření informací a „likvidace“ řídicích orgánů druhé strany. Provádí se silami a prostředky pozemních a vzdušných sil, včetně speciálních, zejména v období samotné války. K vedení defenzivních informačních operací se síly a prostředky fyzického ničení používají k zabezpečení plnění opatření ochrany vojsk,

např. eliminace zpravodajských, průzkumných orgánů nebo diverzních skupin.

Podstatu **klamání**, jako další vojenské činnosti zasazované v plné míře k vedení informačních operací, vystihuje následující citát:

*„All warfare is based on deception.“ [5]
Sun Tzu, The Art of War
c. 500 BC*

Příklady použití **klamání** můžeme rovněž najít v studiích o válkách v minulosti. Jeho cílem je poskytnout řídicím orgánům protivníka jakýmkoliv způsobem informace, na jejichž základě přijme chybné rozhodnutí vzhledem k našemu předpokládanému záměru.

Základem úspěšného použití **klamání** je pochopení způsobu myšlení řídicích orgánů protivníka a schopnost odhadnout jeho reakci na vzniklou situaci, z hlediska operačních a taktických zásad vedení bojové činnosti.

K vedení **klamání** se budou používat dostupné vojenské síly a prostředky, včetně psychologických operací, za účelem poskytnutí klamných informací v různých formách. Ke **klamání** se nesmí využívat orgány civilně-vojenské spolupráce a komunikace s veřejností.

Elektronický boj patří mezi novější druhy vojenských činností, vyvinutých a používaných k působení na prostředky šíření informací druhé strany a posílení ochrany našich vlastních prostředků.

Základem úspěšného nasazení elektronického boje k vedení útočných informačních operací je analýza slabých a zranitelných míst komunikační a informační soustavy protivníka, zjištění její topologie a možnosti využívání jednotlivých komunikačních a informačních okruhů ke zpravodajským nebo klamným účelům. Stejně důležitá je i znalost možností našich prostředků elektronického boje. Úkolem sil a prostředků elektronického boje v obranných informačních operacích je podpora ochrany našich prostředků šíření informací.

Nevýhodou použití prostředků elektronického boje je, že v důsledku rychlého tempa ve vývoji a zavádění nových komunikačních a informačních technologií se nedaří zavádět adekvátní prostředky k působení a získávání informací.

V rámci profesionalizace ozbrojených sil České republiky bude u pozemních sil vybudována **jednotka psychologických operací**. Jejím hlavním posláním je přímé ovlivňování morální složky vojenské síly. Snižováním morálky vojsk a obyvatelstva protivníka, které se projevuje např. případy dezerce, vzpour, počtem zajatců a demonstracemi obyvatelstva, se vytváří předpoklady ke snižování počtu použitelné vojenské síly a ztrátě podpory domácí a zahraniční veřejnosti.

Ochrana vojsk je v podmínkách AČR velmi rozsáhlou oblastí, ve které mají své místo i obranné informační operace. Jsou směřovány k zabezpečení ochrany informací a prostředků jejich šíření, a to nejen vojenských, ale i obranných a národních [6].

V rámci informačních operací je cílem ochrany vojsk:

1. Zabezpečit ochranu vlastních vojsk před účinky psychologického působení (propaganda) protivníka stanovením opatření k vedení kontra propagandy doplněné šířením informací o dané situaci velitelskou cestou.
2. Zabránit protivníkovi v získávání informací z našich prostředků šíření nasazením sil a prostředků elektronického boje, které budou doplněny o opatření realizovaná jinými silami a prostředky. Základem ke stanovení účinných opatření je zhodnocení bezpečnostních mechanismů našich prostředků šíření, zhodnocení možného dopadu kompromitace přenášených informací a zhodnocení možností prostředků protivníka k jejich získávání.
3. Zabránit protivníkovi v působení na naše prostředky šíření informací. Základem ke stanovení účinných opatření, realizovaných stejnými prostředky jako v předešlém bodě, je analýza možností prostředků protivníka a zhodnocení bezpečnostních mechanismů našich prostředků šíření.

Opatření k zajištění ochrany vojsk jsou úzce spjata s klamáním, kde právě poskytováním klamných informací vytváří podmínky k zajištění ochrany vojsk. Důležitou roli ve stanovování opatření k ochraně vojsk v informačních operacích mají:

- zpravodajské a průzkumné orgány,
- složky komunikačních a informačních systémů štábů všech stupňů velení a řízení, které zpracovávají uvedené analýzy,
- velitelské orgány k zabezpečování plnění přijatých opatření,
- vojenské obranné zpravodajství a bezpečnostní složky (Vojenská policie, Policie České republiky).

Využití **orgánů informování veřejnosti** v informačních operacích je velice citlivou otázkou. Uvedené orgány se prostřednictvím informování domácí a zahraniční veřejnosti, cestou hromadných sdělovacích prostředků, nepřímo podílejí na získávání a posilování důvěry. Z tohoto důvodu nesmí být použity k šíření klamných informací.

Dobrým příkladem zapojení uvedených orgánů do informačních operací, s cílem získat informační převahu, můžeme najít v operaci „Pouštní bouře.“ S využitím prostředků fyzického ničení byly eliminovány možnosti Iráku poskytovat informace zahraniční veřejnosti o průběhu operace. Zástupci hromadných sdělovacích prostředků tak byli odkázáni pouze na informace od spojenců, resp. USA.

Obdobná situace je i ve využití orgánů **civilně-vojenské spolupráce** v informačních operacích. Poslání těchto orgánů vytváří podmínky k jejich působení mezi zástupci státní a místní

správy a zástupci mezinárodních humanitárních organizací v místě působení našich sil. Svým vystupováním při styku mohou napomáhat k získávání a posilování důvěry mezi uvedenými představiteli, která se může projevat např. v interpretaci pohledů na opatření velitele vojsk k dané situaci. Současně se mohou orgány civilně-vojenské spolupráce podílet na získávání názorů na situaci u těchto představitelů.

Operace ve výpočetních sítích

Operace ve výpočetních sítích (*CNO - Computer Network Operation*) představují novou formu vojenské činnosti, předurčenou k působení na prvky výpočetních sítí (např. získávání informací, eliminace prvků ap., samozřejmě i zabezpečení jejich ochrany před zneužitím).

Požadavek na jejich zavedení vychází ze stále větší závislosti armád na využívání výpočetní techniky a systémů k řízení, přenosu a zpracování informací. Na druhé straně, potřeba jejich zabezpečení vychází z přítomnosti nových forem hrozeb (aktivity hackerů), které jsou pro ně vlastní.

Na způsoby zabezpečení ochrany informačních systémů v podmínkách AČR ukázala 7. konference spojovacího vojska, zorganizovaná 1. fakultou VA Brno dne 10. prosince 2002. Neřešenou otázkou operací ve výpočetních sítích však zůstává její aktivní forma, tj. působení a získávání informací z výpočetní sítě protivníka. Proto by orgány určené k jejímu vedení v podmínkách AČR měly disponovat silami a prostředky elektronického boje.

Závěr

Při zavádění informačních operací v AČR v některých případech dochází k jejich zaměňování za komunikaci s veřejností. Objasnění rozdílů mezi nimi, komunikací s veřejností a psychologickými operacemi, z hlediska jejich účelu, cíle působení, použitých „zbraní“ a prostředků, je znázorněno v **tabulce**:

	Psychologické operace	Komunikace s veřejností	Informační operace
ÚČEL	ovlivnit	informovat	ovlivnit
CÍL	specifikován, postoje a chování cílové skupiny protivníka	nespecifikován, vnitřní a vnější veřejnost ve vztahu k resortu	rozhodovací proces protivníka
ZBRANĚ	informace , vybrané z hlediska účelu	informace/fakta	informace , vybrané z hlediska účelu a prostředky k působení na komunikační a informační soustavu protivníka
PROSTŘEDKY	vlastní	hromadné sdělovací prostředky	vlastní a hromadné sdělovací prostředky

Je samozřejmé, že na strategické úrovni velení a řízení bude docházet k určitému prolínání všech těchto aktivit. Hlavním způsobem jejich vedení budou informační aktivity politických a vládních představitelů státu. Zásadní rozdíly najdeme ve výběru informací, kde v případě „informačních operací půjde“ o klamné a zkreslené informace a protivníkovi bude zabraňováno získávat informace, popřípadě využívat informace, v jeho národní komunikační infrastruktuře. V případě komunikace s veřejností a psychologických operací se budou používat

informace spojené se snahou o získání důvěry. Dalším rozdílem je požadovaný konečný stav. U informačních operací se požadovaný konečný stav projevuje reakcí protivníka na danou situaci, která nám poskytuje výhodnější pozici k další činnosti při řešení krize než má protivník. Požadovaným konečným stavem u komunikace s veřejností je pochopení a následná podpora našich aktivit veřejností.

Informační operace představují koordinační nástroj nasazení vhodných vojenských činností k dosažení informační převahy nad protivníkem. Nevyžadují výstavbu nové jednotky, ale rozšiřují využívání schopností stávajících a nově budovaných sil a prostředků AČR k jiným účelům. Vytváří prostor ke kompenzaci s jinými formami převahy (např. v počtu techniky, živé síly) protivníka vůči nám. Na základě námi ovlivněných informací, které protivník použije v jeho rozhodovacím procesu, nebude mít možnost účinněji využít dané formy jeho převahy.

Poznámky k textu:

- [1] „Ve válce je skutečným cílem mysl nepřátelského velitele, ne životy jeho vojsk,“ *Joint Pub 3-13, Joint Doctrine for Information Operations*, Joint Staff, USA 1998.
- [2] Na strategické úrovni k vedení informačních operací armáda USA předpokládá použití i diplomatické, ekonomické a politické prostředky. V rámci NATO se předpokládá např. použití mezinárodních sankcí.
- [3] Např. Květoslava POLÁKOVÁ. Informační válka a informační zbraně. VA Brno, *Adresní informace* č. 74/2000.
- [4] „Musíme říct, že ve všech případech rozhodující úloha nepatří technologii – za technologií je vždy živá bytost, bez které je technologie mrtvá“, *Joint Pub 3-13, Joint Doctrine for Information Operations*, Joint Staff, USA 1998.
- [5] „Celá válka je založena na klamání,“ *Joint Pub 3-13, Joint Doctrine for Information Operations*, Joint Staff, USA 1998.
- [6] Vojenské prostředky šíření informací jsou určeny k přenosu informací v rámci armády; obranné prostředky šíření informací slouží k přenosu informací k zajištění obrany státu; národní prostředky tvoří prvky přenosu informací potřebných k řízení státu.

Použitá literatura:

- Pplk. Ing. Jaroslav MORAVČÍK. *Informační operace Armády České republiky*. Dílčí studie. Brno: ÚSS VA Brno, 2002, ÚSS/2002-S-2-16.
- Joint Pub 3 - 13: Joint Doctrine for Information Operations*. Joint Staff, Washington, USA, 1998.
- Květoslava POLÁKOVÁ. Informační válka a informační zbraně. *Adresní informace* č. 74/2000. VA Brno, 2000.
- FM 100-6 Information Operations, Headquarters*. Department of the Army, Washington, USA, 1996.
- MC 422/1 NATO Military Policy on Information Operations*. IMS 2002.