

Major Ing. Tomáš Novák

## Informační operace na pozadí současných ozbrojených konfliktů

**STRATEGICKÉ  
ŘÍZENÍ**

Vojenské rozhledy, 2014, roč. 23 (55), č. 4, s. 51–62, ISSN 1210-3292 (tištěná verze), ISSN 2336-2995 (on line).  
Článek prošel recenzním řízením.

## Information Operations on the Background of Contemporary Armed Conflicts

### Abstrakt:

Článek představuje teorii informačních operací na pozadí ozbrojených konfliktů na Ukrajině, v Iráku a Sýrii. V úvodu jsou informace představeny jako fenomén a akcelerátor vývoje společnosti. Jsou zde nastíněny základní informační kanály, jež přináší informace bezpečnostního rázu jejich příjemci. Dále se článek věnuje bezpečnostnímu a operačnímu prostředí, a také zranitelnosti, kterou s sebou vzrůstající závislost na informacích přináší. Jádrem článku jsou informační operace, které jsou prezentovány ve své teorii s autorovým komentářem k reálnému uplatnění ve vojenské praxi a v podmínkách Armády České republiky. Jako součást informačních operací jsou následně představeny psychologické operace, operace v počítačových sítích a elektronický boj. Článek je zakončen reálnými příklady informačních a psychologických operací v současných konfliktech a podmínkami jejich vedení v AČR. Závěr shrnuje obecné myšlenky o bezpečnostním prostředí a informačních operacích a zdůrazňuje význam informačních operací v současných i budoucích konfliktech.

### Abstract:

The article presents the theory of information operations on the background of contemporary armed conflicts in Ukraine, Iraq and Syria. In the introduction, information is presented as a phenomenon and the accelerator of social development. It outlines basic information channels that deliver security information to their recipients. Furthermore, the article discusses security and operational environment and also vulnerabilities being caused by increasing dependence on information. The core of the article are information operations presented in theory with the author's commentary on real application in military practice and in terms of the Czech Armed Forces. As part of information operations are subsequently introduced psychological operations, computer network operations and electronic warfare. The article ends with real examples of information and psychological operations in modern warfare, and conditions of their management in the Czech Armed Forces. The conclusion summarizes the general idea of the security environment and information operations, and stresses the importance of information operations in current and future conflicts.

### **Klíčová slova:**

Asymetrická válka, bezpečnosti hrozby, bezpečnostní prostředí, civilní obyvatelstvo, Evropa, globalizace, informační operace, informační válka, kybernetické hrozby, operační prostředí, psychologické operace, Rusko, trendy, Ukrajina.

### **Key words:**

Asymmetric war, security threats, security environment, civilians, Europe, globalization, information operation, information war, cyber threats, operational environment, psychological operations, Russia, trends, Ukraine.

## **Úvod**

Vývoj ozbrojeného konfliktu na Ukrajině, v Iráku a Sýrii se zájmem a znepokojením sleduje celá světová laická veřejnost. Pro bezpečnostní odborníky a vojenské specialisty však představují tyto konflikty i předmět hlubokých analýz. Bezpečnostní hrozby, které jsou součástí aliančních nebo národních doktrín a doposud se mnohdy jevily jako pouhé akademické úvahy, nabývají v mnohých ohledech reálnou podobu. Přestože krize na Ukrajině, v Iráku a Sýrii představuje odlišný ozbrojený konflikt, lze již dnes vyvodit řadu poznatků a zkušeností, které jsou pro všechny společné. Mnoho souvislostí, příčin a důsledků bude nutno analyzovat s odstupem času, ale už nyní lze říct, že v těchto ozbrojených konfliktech hrají média a různé druhy medializace velmi významnou roli. Z vojenského pohledu jde tedy o oblasti, které nazýváme psychologické a informační operace. Ve svém článku se pokusím tyto poznatky interpretovat z hlediska obecných východisek, doktrinálních principů informačních a psychologických operací a z pohledu svého působení v čele střediska psychologických operací Armády ČR.

## **Informace – fenomén a akcelerátor vývoje společnosti**

Pochopení globálního politického, ekonomického a ekologického světového řádu není myslitelné bez pochopení souvislostí vzniku a vývoje jednotného planetárního komunikačního prostředí, ve kterém se informace volně šíří a dále volně generují. Od masovějšího rozšíření internetu v devadesátých letech 20. století začala nová éra rozšiřování prostoru, ve kterém lidstvo hledá příčiny a souvislosti svého konání.

Přístup k datům a informacím dnes zabezpečují celosvětové datové sítě. Lidé zde získávají informace, diskutují a pohybují se v různých oblastech zájmů. Všechna nová zjištění sdílí a získávají proto, aby je následně použily v jiné, libovolné oblasti své činnosti a zájmu. Výsledkem takového opakujícího procesu je zrychlující se technologická a myšlenková inovace. Přičemž rozhodující roli v tomto prostředí hrají právě média jako fenomén, který svým vlivem vstupuje do věch sfér lidské společnosti.

Pozvolná ztráta státního informačního monopolu masmédií umožňuje přístup k alternativním interpretacím událostí a výkladu světa. Tím se otevírá možnost vzniku nových

společenských konfliktů ideologického typu. Dezinformace, klamání a polopravdy jsou nekontrolovatelně, záměrně i preventivně šířeny v rámci cílených informačních kampaní, psychologické války, lobbingu a veřejné diplomacie, jež provádí státní, polo-státní, ekonomické a politické zájmové skupiny. Cílem takových akcí může být narušení koherence mezi různými společenskými vrstvami, zpochybnění, zkresení a zamlžení informací a událostí, poškození vybraných skupin a důvěryhodnosti jednotlivců. Navíc se všechny tyto činnosti odehrávají souběžně a prakticky ve stejný okamžik. Společnost tak přechází do nové dimenze vnímání globální reality, kde je obtížné rozeznat fundamentální dobro a zlo a pravdu od manipulace.

S vytvářením nové dimenze vnímání přichází ve zcela nové a revoluční formě Rusko, které se vymyká již popsaným modelům a způsobům informační války islámských fundamentalistů v Iráku a Sýrii. [1] V rozvinuté společnosti, jež je charakteristická neustálým informačním tokem, je ovlivňování informacemi uplatňováno v jednoduchém vzorci: kdo klame, ten vede a umí (může) manipulovat, kdo manipuluje, má moc, kdo má moc, může tvořit obraz minulosti, kdo vytváří obraz minulosti, má kontrolu nad přítomností a budoucností. Hlavním úsilím ruské propagandy tedy není nikoho přesvědčit, ale udržet příjemce informací v nejistotě, zmatku a rozrušení. Takto se vytváří ideální prostředí pro vznik konspiračních teorií, které se dále samy příživují, a toto prostředí znemožní jakoukoliv další věcnou a logickou argumentaci. [2]

## Informační kanály

**Hlavní informační kanál** představují prohlášení jednotlivých představitelů zainteresovaných států nebo hlavních aktérů. Tyto jsou předkládány široké veřejnosti prostřednictvím uznávaných médií, a to zejména prostřednictvím televizního signálu. Tato prohlášení ve většině případů nejsou nahodilá a nejsou primárně určena běžné populaci. Jejich formulace je zpravidla pečlivě připravována štáby odborníků na strategickou komunikaci a obsahují specifický způsob kódování informací. Proto se v některých materiálech hovoří o strategické komunikaci jako o *veřejné diplomacii*, jež provádí nejen jednotlivé státy, ale je využívána i významnými celosvětovými organizacemi na mezinárodní úrovni. [3]

**Dalším informačním kanálem** jsou zpravodajské agentury a jednotlivý reportéři. Ti přinášejí očitá svědectví a vlastní informace a interpretace přímo z krizových oblastí. Míra autentičnosti zachycených informací je v tomto případě vysoká, avšak o objektivnosti reportáží lze často pochybovat. Významnou roli zde hraje sledovanost, utvrzení v předem zaujatém postoji nebo potvrzení mediálního stereotypu. [4] Způsob přinášení informací tímto informačním kanálem je stále více populistický a charakter takových produktů odpovídá jejich masové spotřebě. Když si dnes zpětně promítneme reportáže z první války v Iráku, neposkytují, a ani se nesnaží poskytnout, holistický pohled na situaci v celé její šíři a ve všech souvislostech. Spíš jde o dokola opakující se mediální stereotyp nadřazenosti a technologické vyspělosti spojenecké armády a zaostalosti a dezorganizovanosti armády Iráku. [5] Každá reportáž nebo prezentovaná informace, mnohdy účelově podaná, je tedy jen určitým fragmentem ve skládáče celkových událostí. Je nutné si uvědomit, že stejným způsobem fungují zpravodajské agentury a jednotlivý reportéři i dnes při zobrazování krize na Ukrajině, v současném Iráku a Sýrii.

**Posledním informačním kanálem** jsou tzv. nová média, mezi která patří zejména internet. Internet je šedou až černou zónou mediálního působení už i proto, že o původci informace a jeho záměru lze jen spekulovat. Názor, že internet je jedním z nejdůvěryhodnějších zdrojů informací, protože je můžeme vzájemně srovnávat, je nejen mylný ale i nebezpečný. Problém je v tom, že pro většinou populaci je nemožné vyhodnotit účel vydání jakékoliv informace a z jaké části názorového spektra pochází. V tomto prostředí se tak daří šířit a přizívat různé konspirační teorie, a je tedy velmi významným kanálem k vedení informační a psychologické války, která nezná, podobně jako internet, žádná pravidla ani hranice.

## Bezpečnostní a operační prostředí a informace

Komunikační a informační doména hraje v **globálním bezpečnostním prostředí** roli objektu i subjektu bezpečnostních hrozeb. Na jednu stranu umožnila globalizaci a všechny jevy s ní spojené, na druhou stranu se lidstvo stalo na komunikačních a informačních systémech závislé. Jejich globální či lokální narušení by znamenalo téměř kolaps světového řádu nebo přinejmenším zhroucení státní správy většiny států. Proto se v této souvislosti spekuluje o možnostech vytvoření zcela nových typů zbraní „hromadného ničení“. Mezi již známé a identifikované bezpečnostní hrozby 21. století patří především terorismus, organizovaný zločin, kybernetické hrozby, extremismus, možnost narušení bezpečnosti civilního letectví, korupce a další. Tyto bezpečnostní hrozby se mohou šířit a skrytě naplňovat právě v rámci informačního prostředí.

Volný přístup k alternativním a často i zcela protichůdným informacím má v demokratické společnosti jistě pozitivní efekt. Vytváří tlak na politické vedení státu provádět transparentní kroky a odpovědná politická rozhodnutí. S těmi by se společnost měla ztotožňovat a vnímat je jako svůj zájem. V opačném případě dochází k rozkolu a odtrženosti, jenž ve svém důsledku může vést k politické a sociální nestabilitě a ve výsledku ke zranitelnosti celého státního zřízení. Tato situace má však daleko větší efekt a drastický průběh v zemích s nedemokratickým a totalitním zřízením.

Nesoulad a odmítnutí podpory politické reprezentace státu ze strany jeho obyvatelstva mohou tedy být vážnou vnitřní bezpečnostní hrozbou. Předzvěstí takového stavu je pozvolná ztráta národní (občanské) hrdosti, znalost a úcta k vlastní historii, tradicím a kultuře. Existuje nebezpečí, že většinová populace by nemusela cítit potřebu aktivně reagovat a vystupovat proti nositelům bezpečnostních hrozeb. [6] Tato vnitřní hrozba může být záměrně cíleně podporována zvenčí jako součást psychologické války. [7] Příkladem je aktuální situace krize na Blízkém východě, vyvolané představiteli tzv. Islámského státu, kteří propagují a medializují masový teror na civilním obyvatelstvu a pohrdání vlastním životem. Zamýšleným efektem tak může být pocit, že takový nepřítel nemůže být nikdy poražen.

Součástí **operačního prostředí**, tj. prostředí, které tvaruje charakter vojenských operací v ozbrojených konfliktech, je také informační doména. Ta má hmotný, ale zejména nehmotný charakter. Informační a komunikační technologie umožňují nejen účinně řídit bojovou činnost, zvyšují účinnost použití zbraňových systémů, ale kladou také vyšší nároky na jejich ochranu. Pro bojovou činnost asymetrického charakteru je typické využívání (zneužívání) moderních a široce dostupných technických prostředků, počínaje

různými spínači, senzory, rušiči a chytrými telefony, a přístupem do internetu a světových sociálních sítí konče. Využití a zneužití různých variací a kombinací technických prostředků a informací jsou tak doslova nekonečné a jen těžko předvídatelné.

Účinně koordinovat obranu a útoky, analyzovat situaci a využívat slabá místa a neúspěchy nepřítele v informačním prostředí má za úkol na operační a taktické úrovni prvek informačních operací. Ten se v souladu se záměrem vojenské operace soustředí uje na koordinaci vytvářených efektů na vůli nepřítele a dalších významných aktérů konfliktu. Ovlivňuje možnosti a schopnosti nepřítele situaci správně vyhodnotit a pochopit, a dále omezuje kapacity nepřítele relevantní informace vůbec získat. Je to dáno provázaností tří oblastí, jež jsou vůle, pochopení a využití kapacit. Tyto dovedou odejmout protivníkovi svobodu v konání. Významným způsobem ovlivní a změní předpoklady, množství a kvalitu informací o prostředí operace a v konečném důsledku tedy vedou k zabezpečení významné převahy a výhody.

## Informační operace

Informační operace lze pro potřeby pozemního vojska [8] chápat jako „*nasazení klíčových kapacit elektronického boje, prostředků k vedení operací v počítačových sítích, vedení psychologických operací, klamání a maskování, nasazení prostředků k zajištění ochrany vlastních jednotek, v součinnosti s podpůrnými a logistickými prostředky, s cílem ovlivnit nebo ochránit informace a informační systémy a ovlivnit rozhodovací proces nejvyšších velitelů*“. [9]

Pro srovnání uvádím i definici NATO, jež se od americké interpretace liší mírou obecnosti. Informační operace jsou zde definovány jako „*vojenská funkce, která má za cíl poskytovat koordinaci vojenským informačním aktivitám k vytvoření zamýšleného efektu na vůli, pochopení a kapacity nepřítele, potencionálního nepřítele nebo jiné schválené strany tak, aby došlo k podpoře aliančních cílů v operaci*“. [10]

## Psychologické operace

Nejméně nákladným, a tedy nejčastěji využívaným způsobem vedení informační války je vedení psychologické války. Takto se prezentují mnohé fundamentalistické a teroristické organizace po celém světě. Na jiný způsob nemají prostředky, ani technologické vybavení.

Pro potřeby NATO jsou psychologické operace definovány jako „*plánovaná psychologická činnost v době míru a války zaměřená na osoby protivníka, vlastní nebo neutrální, s cílem ovlivnit postoje a chování, což má vliv na dosažení politických a vojenských cílů. Zahrnují psychologickou činnost na strategické úrovni, činnost k psychologické konsolidaci a psychologickou činnost na bojišti*“. [11] Psychologickou konsolidací jsou myšleny aktivity zaměřené na civilní obyvatelstvo v prostoru pod kontrolou vlastních vojsk s cílem dosáhnout takového požadovaného chování, které zabezpečuje dané vojenské cíle a dává volnost v jednání zabezpečovaným velitelům.

Naopak psychologická činnost na bojišti zahrnuje plánované psychologické aktivity, jež jsou prováděny jako nedílná součást bojových operací. Tyto aktivity jsou zaměřené

na vytvoření psychologického tlaku na nepřítele a civilní obyvatelstvo pod jeho kontrolou v prostoru bojové činnosti a mají pomoci k dosažení operačních a taktických cílů. Jinak řečeno, cílem psychologických aktivit je ovlivňovat nepřátelskou vůli bez použití zbraní. Navíc vedení psychologické války, buď samostatně, nebo jako součást války informační, není v neustálém informačním toku jednoduše rozpoznatelné, přestože je přítomna a má své výsledky. I z tohoto důvodu se nepovažuje ani za akt agrese nebo válečný akt ve smyslu válečného práva.

Řazení, výběr a načasování „vypuštění“ informací do vybraných informačních kanálů během vojenské operace má ve výsledku ovlivnit vědomí a vůli vybrané cílové skupiny, a tak přispět k dosažení vojenských podmínek konečného stavu. Význam vedení psychologických operací vzrůstá při vedení časově náročných operací větších rozměrů. I zde o úspěchu válečného tažení rozhodují hlavně vojenské bojové operace a výkon ekonomiky. Důležitým se ale stává i morální stav, odhodlanost a nezlomnost vlastních jednotek a na významu získává i podpora spřáteleného obyvatelstva v operačním prostoru.

Psychologické operace lze kategorizovat podle různých kategorií a hledisek. Prvním hlediskem je úroveň a druh operace. Obecně jsou to tedy strategické psychologické operace, psychologické operace k podpoře bojových operací a k podpoře nebojových operací. [12] K tomuto rozdělení se váže i druhé hledisko spjaté s cílovou skupinou. Tu můžou tvořit velké celky, jako jsou celé národy, vybraná etnika, politická frakce operačního prostředí, nebo menší celky, jako je konkrétní nepřátelská jednotka, její velení a obyvatelstvo tvořící určený prostor operace. Tyto hlediska pak určují následnou strategii použití psychologických operací.

## Strategické psychologické operace

Strategické psychologické operace jsou vedeny již v době míru i v průběhu krizí a v době válečného stavu. Jejich cílem je získat podporu a spolupráci spřátelených a neutrálních zemí a potlačit vůli a odhodlání nepřítele rozpoutat a vést válku. V tomto ohledu vede Rusko v současné době poměrně razantní a agresivní strategickou psychologickou operaci. [13]

V době míru jsou strategické psychologické operace součástí bezpečnostní a obranné politiky uplatňované v souladu s národními zájmy daného státu (aliance). V případě vzniku krizové situace, strategické psychologické operace demonstrují odhodlání, vůli a způsob, kterým ji chtějí řešit představitelé státu (aliance). Tyto strategické operace plánují, řídí a vedou státní orgány, zejména v působnosti ministerstva zahraničí jednotlivých států. [14]

Naopak, pro mnohonárodnostní organizaci jako NATO je provádění a vedení strategických psychologických operací, ke krizím ve kterých se přímo neangažuje, velmi obtížné. Navíc dosáhnout mezi členskými státy Aliance a Evropské unie rychlého politického konsenzu, jak se postavit k vývoji současných krizí na Ukrajině, v Iráku a Sýrii, mnohdy brání její těžkopádnost. Proto se tyto organizace mnohdy uchylují k velice opatrným až vágním prohlášením. Opačným případem jsou strategické psychologické operace Ruska a USA, které si jako suverénní státy a globální aktéři drží v informačním prostředí iniciativu a udržují volnost konání.

## Zásady psychologické operace k podpoře bojových a nebojových operací

Velmi důležité je, aby **psychologické operace k podpoře bojových operací** byly plánovány a vedeny jako neoddělitelná součást ostatních aktivit bojových operací. Tyto operace jsou plně pod kontrolou velitele mnohonárodního operačního uskupení. Odpovědnost za vedení a koordinaci psychologické operace by měla být svěřena jeho štábu, případně v přesně vymezeném rozsahu podřízeným velitelům. Ve srovnání se strategickými operacemi mají operačně-taktické psychologické operace omezené časové trvání, ale zároveň vyšší dynamiku. Cíle těchto psychologických operací vyplývají z cílů jednotlivých fází operačního plánu. Konkrétně podporují rozhodující body operace a v delším horizontu se snaží přispět k cílům jednotlivých linií (směrů) operace. I v tomto případě je trvalým úkolem vytvářet prostředí psychologického nátlaku na obyvatelstvo pod kontrolou protivníka a protivníka samotného tak, aby ho v prostoru operace znevýhodňoval.

Záměrem **psychologických operací k podpoře nebojových operací** je dosáhnout spolupráce mezi vlastními vojenskými jednotkami a místním obyvatelstvem. Trvalými úkoly jsou vytvářet všeobecný souhlas se stabilizací situace, prosadit déletrvající mír, přispívat k vytvoření a stabilizaci politického prostředí, kriminalizovat nelegální aktivity a budovat kredit bezpečnostní složek. Další konkrétní cíle psychologických operací se stanovují na základě okamžité potřeby. Může jít o snahu usměrňovat tok uprchlíků, rozšířit sběr informací od obyvatelstva, podpořit aktivity „*mysl a srdce*“.

V současné době ale dochází stále častěji k míchání bojových a nebojových aktivit v jednom prostoru operace. Tato praxe, označovaná někdy jako „*three block war*“, vyžaduje rychlou změnu v přístupu k aktuální situaci nebo vybrané cílové skupině. Psychologické operace hrají i klíčovou roli v přechodových fázích mezi stadiem intervence a stabilizace a následně mezi stabilizací a normalizací. Psychologické operace zde snižují riziko spojené s odchodem vojsk a recesí nežádoucího stavu. Praxe současných konfliktů tedy stírá rozdíly mezi psychologickými operacemi k podpoře bojových a nebojových aktivit. Uplatňuje se spíše jejich komplexnost a zdůrazňuje se zejména vysoká flexibilita.

## Operace v počítačových sítích

Operace v počítačových sítích, označované též jako **kybernetické operace**, jsou také částečně koordinovány a sladěny v rámci probíhající informační operace. Efektivita operací v počítačových sítích závisí samozřejmě na možnostech vlastních a nepřítelů, a jeho schopnosti využívat a zahrnovat do svého rozhodovacího procesu informační technologie. V tomto ohledu masivní pronikání počítačových systémů do všech oblastí společnosti, včetně většiny vojenských zbraňových systémů, systémů spojení, získávání a vyhodnocování zpravodajství a dalších, vytváří množství příležitostí a prostor pro inovace, ale zároveň přináší i rizika a zranitelnost.

Operace v počítačových sítích se dělí na několik základních činností.

Za prvé je to **útok a napadení** počítačů, zálohovacích a síťových zařízení, vložením škodlivého kódu nebo virem. Účelem může být jejich celkové zničení. Avšak chytřejší

kódy taková zařízení neničí, ale mění jejich charakteristiky, výkon a schopnosti. Tyto chytré kódy jsou zvláště nebezpečné, protože jejich činnost nemusí být po dlouhou dobu odhalena. Příčiny selhání se totiž hledají často nejprve úplně jinde. Možnost takových útoků se zvyšuje používáním komerčních softwarových produktů ve vojenských systémech a ve vojenském prostředí obecně.

Další činností je **zneužívání počítačových sítí a počítačů** k získávání informací. Počítačové kódy mají v těchto operacích za cíl proniknout do zabezpečené oblasti a získat možnost přistupovat, prohlížet, kopírovat, odesílat a jinak manipulovat s daty a informacemi. Poslední činností je činnost defenzivní. Důvodem obranných počítačových operací je ochrana proti počítačovým útokům a zabránění neoprávněné manipulaci s daty. Opatření počítačové obrany mají za cíl předejít přerušení, odepření, znehodnocení nebo destrukci vlastních informací umístěných v počítačích nebo počítačových sítích.

Počítačová obrana je nezbytná k udržení rozhodovacího procesu založeném na využití počítačů, počítačových sítí a dat v nich uložených. V mezinárodním prostředí je často diskutována otázka, jak uplatnit mezinárodní právo ve chvíli, kdy se cílem útoku stane členský stát Aliance.

## Elektronický boj

Proti operacím v počítačových sítích, které jsou vedeny ze stacionárních pracovišť strategické úrovně, má elektronický boj uplatnění zejména na nižších úrovních. Cílem elektronického boje, který je součástí informačních operací, je provádět zejména elektronické útoky s cílem narušovat systém velení a řízení nepřítele. Elektronický boj dokáže nejen destruktivně útočit na automatizované systémy potřebné k rozhodovacímu procesu technologicky vyspělého protivníka, ale velmi často i vytvářet podmínky pro sběr zpravodajsky významných informací a pro klamání.

Ochranná opatření elektronického boje jsou realizována při řízeném využívání a ochraně vlastního vysílacího spektra. V budoucnu lze očekávat, že využívání ochranných opatření elektronického boje na bojišti bude nalézat stále nové způsoby uplatnění. Naopak útočné aktivity budou i nadále usilovat o znemožnění přenášet kritické informace z bojiště k protivníkovi nebo do jeho informačních systémů. Novou oblastí útočných aktivit elektronického boje bude pravděpodobně přebírání kontroly nad zbraňovými systémy a prostředky nepřítele řízené počítačem nebo dálkovým signálem.

## Informační a psychologické operace v současných ozbrojených konfliktech

Už jsme si zvykli, že krátká tendenční videa z oblastí nestability se šíří internetem jako *virál* [15] přes sociální sítě. Jejich cílem je **vytvářet u příjemce rychlé závěry a předsudky**. Navíc přebírání těchto nahrávek do oficiálních médií jako je televize, jim automaticky přiřazuje společenskou důležitost. Domácí populace je tak vystavena psychologickému působení prostřednictvím „vizuálních informací“, které „unikají“ z prostoru bojů na jedné nebo druhé straně. Některé tyto produkty nemají za cíl



jen psychologicky působit a získat si příjemce na vlastní stranu nebo ho naopak odstrašit. Jsou produkty, jejichž poselství má mobilizovat k provedení reálných akcí.

Příkladem je vznik a činnost dobrovolnických praporů na obou stranách ukrajinské krize. Dalším příkladem je nárůst dobrovolníků bojující za tzv. Islámský stát z řad Evropanů. Spektrum potřeb, které mají zainteresované strany v současných konfliktech, je velmi široké, a tak je k jejich uspokojení třeba oslovit i odpovídající počet příjemců.

Dalším oblíbeným způsobem manipulace je **poměřovat neměřitelné**. Prohlášení významného veřejného činitele nebo autority se vyvrátí prohlášením „obyčejného člověka“, místními obyvateli nebo přímo vojáky v poli. Televizní divák má totiž tendenci přisuzovat respondentům (účinkujícím) stejnou váhu a často nekriticky vnímá reportáž jako celek, přičemž většinou jde naopak o účelově vybrané pasáže z rozhovorů nebo působivých segmentů z událostí.

Pro vedení každé vojenské operace je tedy důležité, aby prohlášení operačních a taktických velitelů, stejně jako řadových vojáků, byla v souladu se strategickými (politické) záměry a prohlášeními politických představitelů. Každé takové vystoupení plní nejen funkci informační směrem k veřejnosti, ale zároveň nese i psychologický efekt směrem k nepříteli. To vyžaduje koordinaci a sladění mezi politickým zadáním a jeho vojenským naplněním. Na informační nesoulad mezi prohlášeními ukrajinských separatistů a prohlášeními čelních představitelů Ruska upozornila „západní“ média během ukrajinské krize již několikrát. Ať již šlo o přítomnost ruských vojsk na Ukrajině nebo o satelitní snímky dokazující rozmístění ruských vojsk u hranic s Ukrajinou, nalézt podíl spoluúčasti specialistů na informační operace není tak těžké.

Je zřejmé, že obyvatelé Evropy jsou v souvislosti s děním na Ukrajině, v Iráku a Sýrii, vystaveni psychologickému působení jako předmět vedení informační války. [16] Tento druh boje není pro armády Aliance včetně ozbrojených sil ČR nic nového. Řešení bezpečnostní situace v Afghánistánu bylo a je doprovázeno psychologickou válkou. Ta je vedena hnutím Talibán a jinými fundamentalistickými organizacemi muslimského světa již řadu let. Její principy jsou dobře zmapovány a na toto téma byla vydána nejedna odborná studie. Jednotky Armády ČR byly svědky psychologického působení nepřítelů na místní obyvatelstvo v jednotlivých provinciích Afghánistánu ve formě různých výhrůzek a dopisů, demonstrativních popravách, ale i poskytování rychlé „spravedlnosti“ a „ochrany“.

Evropské populace se situace v Afghánistánu, a s ní spojené psychologické války, dlouhodobě příliš nedotýkala. Určitý zvrat v přístupu k informacím bezpečnostního rázu přinesl až rychlý a nepředvídatelný vývoj situace na Ukrajině a následný návrat pocitu ohrožení, jenž byl spojený se šířením skryté ideologie a propagandy.

Informační operace v podání Ruska předvedly vysokou míru sofistikovanosti. Médii proběhly zprávy o údajných úspěších ruského elektronického boje při převzetí kontroly nad cizími vojenskými systémy. Bylo zveřejněno množství odposlechů. Ruská média si zabezpečila a udržela informační monopol nad vlastním obyvatelstvem a úspěšně využívala každé „zaváhání“ nebo kontroverzní výroky zahraničních politiků a autorit ve svůj prospěch. [17] V případě Sýrie a Iráku se obyvatelům Evropy zdají tyto země možná příliš daleko a nemají k nim zafixovány ani žádné historické předsudky. Ve společnosti spíše tak rezonují lidské tragédie jednotlivých unesených osob, jež islámský stát využívá pro svoji psychologickou válku proti jejich vládám.

## Realita informačních a psychologických operací v AČR

V podmínkách AČR nelze uplatnit teorii vedení informačních operací v celé šíři tak, jak si to mohou dovolit jiné ekonomicky a politicky a vojensky silné státy. Nicméně neuplatnit z této teorie vůbec nic a informační operace vůbec do AČR nezavést, je opačný extrém. Základní komponenty informačních operací v AČR již existují. Jedná se o jednotky elektronického boje, Centrum CIRC [18] a středisko PSYOPS. [19] V případě zavedení informačních operací do Armády ČR jde tedy o nalezení způsobu, jak tyto kapacity zkoordinovat národní doktrínou informačních operací. O výhodách a potřebě většího zavedení a zapojení informačních operací do operací vedených na operační a hlavně taktické úrovni bylo, v souvislosti s různými strategiemi, napsáno bezpočet odborných teoretických i praktických článků. [20]

V souvislosti s teorií informačních operací, je nutno oponovat některým názorům, které často rezonují v odborných kruzích, že vedení informačních operací patří do gesce zpravodajských orgánů, a to at' vševojenských nebo Vojenského zpravodajství. Z podstaty výše uvedených řádků, ale zejména alianční doktríny AJP-3.10 (Informační operace), je zcela zřejmé, že informační operace patří jednoznačně do domény operační. Informační operace jsou v rámci operačního umění posuzovány a vytvářeny jako samostatná linie (směr) operace v rámci tvorby koncepce operace. Z této koncepce se poté na taktické úrovni odvozují a rozpracovávají jednotlivé konkrétní úkoly a opatření pro jednotlivé prvky informačních operací v rámci přiděleného prostoru operace. Je tedy nutno oponovat i současnému názoru v AČR, že na taktickém stupni o velikosti brigády [21] není třeba žádný prvek informačních operací. Pokud tomu tak i nadále zůstane, hrozí nebezpečí, že tato linie (směr) operace zůstane bez koordinace, nebo v horším případě nebude na přiděleném prostoru realizována vůbec, a to jak ve své útočné, ale hlavně obranné formě.

Význam psychologických operací, v rámci struktury pozemních sil AČR, v současné době pomalu klesá, spolu s útlumem aktivit spojených s nasazením do zahraniční mise v Afghánistánu. Navíc struktura brigádního úkolového uskupení si po dlouhý čas vystačila s činností dvou specialistů PSYOPS. Toto číslo vnímám jako hrubé poddimenzování a účast specialistů PSYOPS jako symbolickou. I po nedávné transformaci Armády ČR stále chybí odpovídající manažerská pozornost, která by ve výsledku vedla k přijetí koncepce rozvoje, vize, nebo stanovila této schopnosti nějaké specifické cíle. Ambicí Armády ČR je připravovat se a vést operace v celém spektru operací, a právě vedení psychologických operací hraje významnou roli v protipovstaleckých operacích, humanitárních operacích i v operacích na prosazení a udržení míru.

## Závěr

Současné krize na Ukrajině a krize v Iráku a Sýrii představují další modifikaci konfliktu zahrnující prvky asymetrického boje, protipovstalecké operace, informační a psychologické války a operace speciálních sil. Tento komplex vytváří zcela novou generaci válčení. Bezpečnostní hrozby, dříve jen teoretické, získávají reálnou podobu. Na plno se projevila těžkopádnost politického rozhodování NATO i Evropské unie.

Čelit reálným bezpečnostním hrozbám vyžaduje zrychlit jejich akceschopnost, a to mimo jiné i ve vztahu k vedení informační a psychologické války.

V informačním prostředí nejsou žádné hranice. Volně přístupný a neregulovaný prostor dává možnosti k ovlivňování a přístupu takřka kohokoliv kýmkoliv. Informační a psychologické války jsou směřovány k ovlivnění soudržnosti nepřítele a společné vůli, legitimitě současného vedení, oslabení morální základny, rozvrácení společenské soudržnosti a solidarity, diskreditaci vůdců a jejich podporovatelů. Podkopává politickou, vojenskou a sociální legitimitu společenského systému nepřítele, a tím oslabuje jeho záměry a nedestruktivně ničí jeho schopnost konat. Ekonomická nestabilita, restrikce v přístupu na světové trhy, pokles výkonu ekonomiky a nezaměstnanost, může vést k odtržení politické reprezentace od zastupované populace do té míry, že sníží národní (alianční) ochotu k přímé vojenské angažovanosti. Lidská populace se tak přesouvá do centra zájmu různých druhů a typů tichých válek.

Informační operace jako vojenská schopnost reaguje na požadavek přenesení strategických souvislostí do prostoru vojenské operace ve formě vedení psychologických operací. Zároveň pragmaticky koordinuje aspekty vedení bojové činnosti ve vztahu k informacím. Operace v počítačových sítích a elektronický boj působí na schopnost nepřítele uplatnit svoji vůli na bojišti tím, že mu brání ve volném přístupu k informačnímu toku z bojiště a na bojiště. Zároveň proti takovým snahám nepřítele aktivně vystupuje a chrání tak vlastní procesy velení a řízení, sběr a vyhodnocování informací a ve finále samotný rozhodovací proces.

V současné době není problematice informačních operací v Armádě ČR věnována odpovídající pozornost. To může do budoucna způsobovat a představovat závažný problém. Zvláště bude-li Armáda ČR po boku spojenců vystavena technologicky vyspělému protivníkovi, který prvky informačních operací ve své strategii dozajista využívá.

### Poznámky k textu:

- [1] Více o problematice např. HODNÝ Jiří. *Psychologické operace ve vojenství na počátku 21. století*. Brno, 2009, 152 s. Dizertační práce na Fakultě vojenských technologií Univerzity obrany. Vedoucí dizertační práce Lubomír Odehnal.
- [2] Více o problematice např. na <http://www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635/>.
- [3] Více o problematice např. na <http://orbis.ujak.cz/verejna-diplomacie.php>.
- [4] Jde o zjednodušené zobrazování, deformování celku, zvýrazňování charakteristických rysů a podobně. Příkladem může být zobrazování města Prahy záběrem na Pražský hrad z Karlova mostu.
- [5] Více o problematice např. na <http://www.ozbrojeneslozky.cz/clanek/medialni-stereotypy-na-prikladu-valecneho-zpravodajstvi-operace-iracka-svoboda>.
- [6] Analogii lze spatřovat v rozpadu římské říše, kdy vojenskou službu a úřední povinnosti v pozdějších letech stále častěji vykonávali zoldněři a příslušníci nižších společenských tříd místo *občanů*, kteří o veřejné záležitosti ztratili zájem.
- [7] Současná vnitřní politika Ruské federace a prezidenta Vladimíra Putina vůči vlastní populaci má pravděpodobně trend vzájemného odtržení zastavit, a naopak posílit národní hrdost, občanskou poslušnost a morálku. Může to být předzvěst vnějších změn, které Rusko může plánovat v globální politice, a jež mohou mít přímý dopad na jeho obyvatelstvo.
- [8] Vzdušné síly chápou informační operace odlišně. V jejich interpretaci jsou spojeny spíše se vzdušným ničícím infrastrukturou potřebné pro přenos, zpracování a šíření informací.
- [9] Z kontextu je zřejmé, že jde o pozemní vojska USA. *Information Operations: Doctrine, Tactics, Techniques, and Procedures*. Washington: Headquarters, Department of the Army, November 2003, 313 p. FM 3-13.

- [10] *Allied Joint Doctrine for Information Operations*. Brussels: NSA, November 2009. 82 p. AJP-3.10,
- [11] *Výkladový slovník pojmů a definic NATO*. Praha: MO ČR, Oddělení pro koordinaci standardizace, 1998, 250 s. Pomůcka AAP-6.
- [12] Středisko PSYOPS AČR je schopné vést operace k podpoře bojových a nebojových operací na taktické úrovni a podporovat jednotlivci a menšími uskupeními (analýza, plánování) úroveň operační.
- [13] Součástí jsou náročné nácviky vzdušných výsadek do polárních oblastí, rozsáhlé manévry a cvičení vojsk strategického významu, změna vojenských doktrín, ale i uzavírání nových ekonomických svazků a strategických partnerství, zvýšení výdajů na obranu.
- [14] Z tohoto pohledu je v případě Ruska zajímavé analyzovat vztah a vzájemnou koordinaci kroků mezi Vladimírem Putinem a jeho blízkým spolupracovníkem Sergejem Lavrovem.
- [15] **Virální marketing (virál)** je reklamním nástrojem používaným zejména k budování povědomí o značce nebo k masové propagaci konkrétního produktu. Charakteristickým rysem virálu bývá skutečnost, že se snaží zakrýt svou propagační podstatu a samotného objednavatele reklamy. Je anonymně vypuštěn a vydává se za atraktivní, tajně získanou nebo náhodně pořízenou ‚neověřitelnou‘ informaci či událost.
- [16] V tomto smyslu se v souvislosti s děním na Ukrajině několikrát v České televizi přímo vyjádřil i ministr obrany Martin Stropnický.
- [17] Ať již šlo o dodávku francouzských válečných lodí Rusku nebo nesoulad v sankcích a společném postupu.
- [18] **Centrum CIRC** (angl. Computer Incident Response Capability) je prvkem kybernetické bezpečnosti rezortu MO. Jeho úkolem je proaktivní identifikace bezpečnostních hrozeb a incidentů, jejich analýza a následné reportování zjištěných událostí a postupů řešení k relevantním
- [19] Pro psychologické operace se v anglickém jazyce ustálily dvě zkratky. V dokumentech Severoatlantické aliance se pro ně uvádí termín PSYOPS, americké ozbrojené síly užívají označení PSYOP.
- [20] Např. články v časopise *Infantry*, ISSN:0019-9532; *Armour*, ISSN:0004-2420; *Military Technology*. ISSN:0722-3226; *Doctrine*, ISSN:1293-2671.
- [21] Ambice divize byla v AČR již opuštěna.

## Seznam použité literatury:

- ČERNOHORSKÝ Vít. *Informační válka*. Praha, 2007, 118 s. Diplomová práce na Filozofické fakultě Univerzity Karlovy na Ústavu informačních studií a knihovnictví. Vedoucí diplomové práce Richard Papík.
- FTOREK, Jozef. *Public relations a politika: kdo a jak řídí naše osudy s naším souhlasem*. 1. vydání, Praha: Grada, 2010, 184 s. Politologie (Grada). ISBN 978-802-4733-760.
- FTOREK, Jozef. *Public relations jako ovlivňování mínění: jak úspěšně ovlivňovat a nenechat se zmanipulovat*. 2., rozš. vyd. Praha: Grada Publishing, 2009, 195 s. Manažer. ISBN 978-80-247-2678-6.
- HODNÝ, Jiří. Zpravodajská podpora psychologických operací. *Vojenské rozhledy*, 2008, roč. 17 (49), č. 2, s. 113-117, ISSN 1210-3292 (tištěná verze), ISSN 2336-2995 (on line), www.vojenskerozhledy.cz.
- HODNÝ, Jiří. Virtuální univerzita džihádu: výcvik a vzdělávání islámských teroristů v kyberprostoru. *Vojenské rozhledy*, 2009, roč. 18 (50), č. 1, s. 115-120, ISSN 1210-3292 (tištěná verze), ISSN 2336-2995 (on line), dostupné z www.vojenskerozhledy.cz.
- HODNÝ, Jiří. Islamisté online. *Vojenské rozhledy*, 2009, roč. 18 (50), č. 2, s. 70-78, ISSN 1210-3292 (tištěná verze), ISSN 2336-2995 (on line), dostupné z www.vojenskerozhledy.cz.
- HODNÝ, Jiří. Indoktrinace a rekrutace islamistů v kyberprostoru. *Bezpečnostní teorie a praxe*, 2009, č. 2, s. 51-58. ISSN 1801-8211.
- HODNÝ, Jiří. *Psychologické operace ve vojenství na počátku 21. století*. [dizertační práce]. Brno: Univerzita obrany, 2009. 152 s. partnerům.
- NOWACKI, Gabriel. *The Polish Views on Information Operations and PSYOPS*. AARMS [online]. 2003, Vol. 2, No. 1, s. 20 [cit. 2014-09-20]. Dostupné z <http://www.konyvvar.zmne.hu/docs/Volume2/Issue1/pdf/02NOWA.pdf>.
- VASÍČEK, Pavel. *Téma: Informační operace a její aplikace v rámci AČR*. Brno, 2011. 38 s. Závěrečná práce. Univerzita obrany. Vedoucí práce Ing. Pavel Zona, Ph.D. Kurz vyšších důstojníků.
- AJP-3.10.1(A). *Allied Joint Doctrine for Psychological Operations*. NATO Standardization Agency. Brussels: NSA, 2007, 33 s. ed.3. NATO/PIF unclassified.
- Doktrína AČR*. 3. vydání, Vyškov: Institut doktrín VeV-VA, 2013.
- Pub-31-10-01*, Pozemní síly v operacích. Vyškov: Odbor doktrín VeV-VA, 2011.