INFORMACE

Doc. Ing. Milan Kubeša, CSc.

Vojenské klamání v informačním věku

Vojenské rozhledy, 2013, roč. 22 (54), č. 1, s. 160–164, ISSN 1210-3292

Military Deception in the Information Age

Abstrakt:

Informační věk lze charakterizovat jako období raketového kvantitativního a kvalitativního nárůstu informací, a to především z důvodu prudkého rozvoje a využívání informačních a komunikačních technologií (ICT). Vojenské klamání v něm získává nový rozměr a v rámci operací ozbrojených sil ještě širší možnosti svého uplatnění. Tento článek představuje završení série statí uveřejňovaných ve VR věnovaných vojenskému klamání. Je zamyšlením nad otázkami, které vycházejí ze vztahu klamání a informačního věku, za jehož počátek lze považovat osmdesátá léta minulého století.

Abstract:

Informantion era could be characterized as a period of the steep qualitative and quantitative information rise, aroused namely by sharp development of information and comunication technologies (ICT). Military deception thus acquires new dimensions, wider chances to be employed in armed forces operations. This article concludes a free series of essays dealing with military deceiving. It is thinking over questions resulting from deception—information age relations, the beginnig of which could be situated into the 80s last century.

Klíčová slova:

Vojenské klamání, informační věk, informační a komunikační technologie, ICT, informační operace IO, informační válka, elektronický boj, měkké operace, bezpečnostní prostředí, hackeři, kybernetické útoky, digitalizace bojiště.

Key words:

Military deception, infomation era, information and comunication technologies, ICT, information operatios, IO, information warfare, electronic warfare, soft operations, hackers, cyber attacts, digitalization of battlefield.

V článku „Vojenskému klamání je třeba dát zelenou!“ (viz VR 3/2012) autoři věnovali pozornost podstatě vojenského klamání, načrtli své představy o možných úkolech, způsobech a formách klamání, jakož i o plánování klamání v období přípravy operací ozbrojených sil. V závěru je ve stručnosti zmíněn problém klamání v informačním věku. [1]

Informační věk je, kromě jiného, charakteristický zvýšením rychlosti v přenosu a distribuci informací – a to bez ohledu na časová a prostorová omezení, zvýšila se kapacita přenosu a ukládání informací, a také schopnost jejich interpretace téměř okamžitě po doručení. [2] Ve velké míře se zvýšila pružnost informačního toku, komunikace mezi nadnárodními institucemi, státy, regiony, různými organizacemi a lidmi samými se neobyčejně prohloubila a nabyla na intenzitě. Zvýšil se počet typů forem zprostředkování informací (hlas, data, obraz) a lze je vzájemně sdílet. Postupně se vytváří „informační společnost", která se dá charakterizovat jako společnost s enormní mírou využívání ICT, založených na prostředcích výpočetní techniky a s nimi spojenou digitalizací. Základem všeho rozhodování jsou informace, jejímiž příjemci jsou nejen lidé, ale i technické systémy, což na jedné straně umožňuje rychlejší a přesnější rozhodování, ovšem na straně druhé je i záludnější z hlediska pravdivosti přijímaných informací.

Bezpečnostní prostředí, informační věk a vojenství

Vývoj bezpečnostního prostředí a projevy informačního věku mají významný dopad na celou oblast vojenství. Bezpečnostní prostředí se mění stále vyšší rychlostí a změny jsou intenzivnější v porovnání s nedávnou minulostí. [3] Nastupují zcela nové hrozby, na které lidstvo prozatím hledá v rámci řízení rizik protiopatření s cílem snížit dopady, nebo zcela některé hrozby eliminovat. Lze uvést nekončící finanční krizi, která má negativní dopady na celou šíři sociálního, ekonomického a vojenského sektoru. Kolabující finanční sektor přináší svým způsobem hrozbu regionální, resp. globální ekonomické války. Útoky na počítačové sítě a další kybernetické aktivity hackerů mohou způsobit kolaps informační infrastruktury, což může ve svém důsledku přinést ekonomický úpadek a následné politické třenice a chaos. Zbraňové systémy jsou sice stále dokonalejší po stránce technologické a účinnější po stránce palebné síly, ale před kybernetickými útoky, které se stávají integrální součástí ozbrojených konfliktů, zatím ve vyšší míře bezbranné. Zaváděním neletálních zbraní se zároveň mění charakter bojových aktivit, což má významný dopad na přijímání reálných rozhodnutí soupeřících stran konfliktu. Významnou hrozbou v blízké budoucnosti může být nedostatek klíčových komodit (ropa, plyn, uhlí, další nerostné suroviny, pitná voda, potraviny atd.), což může být příčinou nestability a války s cílem získat tyto životodárné suroviny. Dnes se dokonce hovoří o krizi vládnutí, což je důsledkem oslabující role světových bezpečnostních institucí (NATO, OSN a svým způsobem i EU).

Bez uplatnění širokého přístupu k bezpečnosti, kombinujícího moderní nevojenské a vojenské nástroje, nebude možné těmto a dalším predikovaným hrozbám čelit. V tomto smyslu se jeví nutnost skutečné kooperace a intenzivního oživení nejen diplomatických a politických aktivit řídících struktur těchto institucí, ale i potřeba prohlubování vzájemné důvěry v horizontální i vertikální rovině.

Druhou neméně významnou složkou, dopadající na vojenství, jsou **projevy informačního věku**. Kromě již výše zmíněné kybernetické aktivity hackerů jde především o aplikování ICT ve vojenském prostředí. Za základní projevy informačního věku se v současnosti považuje obrovský **nárůst objemu dat a informací**, které jsou základem pro kvalitu rozhodování v jakémkoli konfliktu, v prvé řadě v ozbrojeném konfliktu, **rozvoj složitosti a pestrosti komunikačního prostředí,** tvořeného pasivními i aktivními systémy, umožňujícími přenos informací (satelitní, internetové, rádiové, radioreléové,

linkové, dnes i s využitím optických vláken), **bezpečnost**, což ve vojenství především znamená ochranu dat a šifrování, **interoperabilita**, kdy jde o snahu popisovat a vyjadřovat se „stejným jazykem“. To se týká především informačních systémů pro podporu velení a řízení (C2IS), které spolu musí navzájem komunikovat. Významným projevem informačního věku v oblasti vojenství je **digitalizace bojiště**, jejímž cílem je sdílení společného obrazu bojiště, což je podmínkou zefektivnění a hlavně zrychlení rozhodovacího procesu velitelů a štábů a v neposlední řadě **rozmach médií**, a to především internetu a televizního vysílání, která umožňují nejen psychologicky, ale i klamavě působit na protivníka, nebo zkreslovat nebo ovlivňovat veřejné mínění. [3]

Informační válka, informační operace a klamání

Informační válka je jednou z „měkkých“ forem války. Jde o působení na protivníka (na strategické, operační i taktické úrovni) prostřednictvím informačních prostředků k dosažení konkrétního cíle, a to nepřetržitě od mírového do válečného stavu a v době války. Dříve byla uplatňována pouze jako podpůrný prostředek, např. v první světové válce byly rozšiřovány letáky mezi vojáky protivníka s výzvami k zanechání odporu. V posledních letech je očividný posun od tvrdé techniky vedení bojů k masivnímu rozvoji jednotlivých forem vedení informační války.

Hlavní výhodou informační války je příznivý poměr mezi vynaloženými náklady na pořízení „účinné zbraně“ na straně jedné a mírou poškození protivníka na straně druhé. Informační válku je možné vést letálními nebo neletálními prostředky, hrubou silou či nesmrtícími prostředky („v rukavičkách“). [4] Dále ji lze členit na útočnou či obrannou – podle toho, zda informace ochraňujeme, nebo se na ně snažíme působit.

Pojem *informační válka* bývá zaměňován termínem *kybernetická válka*, který se ale vztahuje výhradně k válce na platformě výpočetní techniky a počítačových sítí. Naproti tomu informační válka zahrnuje řadu dalších forem, které se navzájem prolínají a doplňují: působení na velení a řízení, zpravodajské působení, elektronickou válku, psychologickou válku, ekonomicko-informační válku, diplomatickou válku, hackerskou válku, a konečně i zmíněnou kybernetickou válku. [5]

V rámci informační války se plánují a realizují **informační operace (IO)**. [4] Tyto se však provádějí i v míru (např. k ovlivnění veřejného mínění na určitou věc, v rámci reklamních či volebních aktivit apod.). V případě informační války jde o centrálně plánovanou a prováděnou (vojenskou i mimovojenskou) činnost s cílem ovlivnit myšlení, chápání, vůli a možnosti protivníka (či potenciálního protivníka) tak, aby bylo dosaženo konkrétního postupného nebo konečného cíle. V případě vedení bojové či nebojové operace by měla IO tuto operaci podporovat nebo být přímo její součástí. V rámci IO se plánuje a provádí řada informačních aktivit. Důležitými cíli informačních aktivit jsou zejména řídící subjekty protivníka nebo osoby, které mají výrazný vliv na rozhodování, popřípadě samy rozhodují. IO zahrnují jak aktivity, ovlivňující chápání a vnímání situace protivníkem nebo potencionálním protivníkem k ovlivnění dat a informací, které protivník potřebuje pro své rozhodování, tak i informační aktivity chránící vlastní jednotky, umožňující volnost manévrování vlastních jednotek a ochranu vlastních dat.

Pro úspěšné provedení informačních operací je důležitá dobře fungující součinnost osob řídících IO a zpravodajských štábů. Vedle IO se plánují a vedou v bojových i nebojových operacích ještě další vojenské aktivity. Základní aktivitou je palebné (fyzické)

ničení a umlčování, psychologické působení, elektronický boj, kybernetické působení a **klamání protivníka.** Nezbytnou vojenskou aktivitou pro vlastní ochranu se provádí soubor činností, spadající do oblasti operační bezpečnosti (zahrnující jak fyzickou tak i informační bezpečnost). Směrem ke spolupůsobícím aktérům v operaci (vládní a nevládní organizace, mezinárodní organizace a civilní obyvatelstvo v zájmovém prostoru) pracuje CIMIC, se kterým se také musí v rámci IO spolupracovat.

Vztah mezi výše jmenovanými oblastmi, jakož i místo klamání v informačních operacích lze (velmi zjednodušeně) vyjádřit graficky podle následujícího obr. [6]

Obr.: Místo klamání v informačních operacích

Tendence vývoje klamání v operacích

Rostoucí podíl měkkých forem války bude s velkou pravděpodobností znamenat i růst podílu „měkkých operací“, ke kterým patří informační, psychologické, kybernetické, diplomatické, ekonomické, finanční, humanitární a jiné nebojové operace, které neupřednostňují uplatnění vojenské síly a efekt ničení a zabíjení, ale naopak, neletální zbraně a zbraňové systémy. To ovšem neznamená, že klasické války a všechny možné formy bojových operací již nebudou aktuální. Technologická a informační revoluce bude mít zásadní vliv na rychlost, přesnost a celkovou kvalitu rozhodovacích procesů nejen v civilním, ale i ve vojenském prostředí. Informace budou nadále hybatelem společenského vývoje, což může znamenat i intenzivnější změny v problematice klamání v operacích. I hospodářská recese a následná tendence v postupném snižování výdajů na vojenství, resp. obranu, ovlivňuje přesun těžiště úsilí politiků a vojenských manažerů k nebojovým taktikám. Klamání k těmto taktikám bezesporu patří, stává se postupem času nedělitelnou součástí procesu velení a řízení vojskům. Proto se v problematice uplatňování klamání v operacích mohou projevovat následující tendence: [4]

1. Klamání se pravděpodobně bude uplatňovat vůči dalším aktérům v operacích. Pokud bude směřovat k dosažení cíle v operaci, může být klamáno v pozitivním smyslu i obyvatelstvo v regionu nebo i veřejnost s cílem příznivě ovlivnit názory a nálady ve prospěch zasahujících vojsk. Takto mohou být ovlivňovány i vybrané nevládní či mezinárodní organizace a instituce prostřednictvím médií (televize, rozhlas, tisk, film, internet apod.).

2. Prostředky klamání se budou stále více zdokonalovat, a to souběžně s rozvojem technologií. Možnosti průzkumu budou stále dokonalejší, což si vyžádá vývoj dokonalejších maket různých zbraňových systémů, maskovacích prostředků ke skrývání (maskovací sítě, maskovací nátěry, zdroje tepelného vyzařování, odražeče radiolokačního záření, různé svislé a horizontální masky atd.). Nové druhy bojových operací (protipovstalecké, protiteroristické a různé typy stabilizačních operací) zvýší poptávku po těchto nově vyvinutých prostředcích klamání na taktické a z části i na operační úrovni.
3. Rozmanitost forem bojové činnosti bude vytvářet prostor i pro nové metody a techniky klamání. Na strategické a částečně i na operační úrovni budou rozvíjeny a používány sofistikované metody tvorby virtualit, zvláště v oblasti internetové dezinformace a diverze. Modernizace bude probíhat i v oblasti plánování operací, což se bude promítat do stylu řízení a velení s dopadem na celý režim utajení.
4. Klamání a psychologické působení bude postupně integrální součástí *informačních operací*, které budou splývat s *psychologickými operacemi*. Klamání a psychologické ovlivňování vůle rozhodovacích autorit a jejich nejbližších spolupracovníků (v armádě velitelů a jejich štábů) se bude stále více řešit s využitím principů jednotného zaměření, jednotného cíle a centrálního řízení.
5. Na plánování klamání a dalších způsobů působení na protivníka a další aktéry v operaci se bude klást daleko větší důraz v porovnání se současným stavem. Rozhodujícím kritériem bude nákladovost a efektivita vynakládaných sil, prostředků a energie. Tento požadavek bude iniciovat zaměření úsilí do vzdělávacích a výcvikových programů vojsk. Problematice neletálního působení na protivníka bude věnována stejná, ne-li větší pozornost nežli bojovému působení.

Informační věk a změny v bezpečnostním prostředí se promítnou do způsobů použití vojenské síly. Prudký rozvoj ICT na jedné straně umožní soupeřícím stranám rychlejší a kvalitnější rozhodování, na straně druhé způsobí větší zranitelnost, včetně možností využití sofistikovanějších způsobů klamání, psychologického, elektronického, ale i bojového působení. Komplexní přístup k plánování operací bude znamenat „vtažení" dalších aktérů do jejich vedení. Těžiště úsilí se bude přesouvat k použití neletálních forem vedení operací, kde budou důležitou roli sehrávat informační operace s podstatným podílem aktivit spojených s klamáním a psychologickým působením.

Literatura:

[1] KUBEŠA, Milan a Ján SPIŠÁK. Vojenskému klamání je třeba dát zelenou. *Vojenské rozhledy,* 2012, roč. 21, č. 3, s. 65-71. ISSN 1210-3292.

[2] BUŘITA, Ladislav. *Informační věk, informační společnost a vojenství*. 1. vyd. Praha: Ministerstvo obrany České republiky, Agentura vojenských informací a služeb, 2007, 141 s. ISBN 978-80-7278-379-3.

[3] BALABÁN, Miloš, Martin POTŮČEK a Antonín RAŠEK. Rodící se nová ohrožení v neklidném světě. *Vojenské rozhledy,* 2011, roč. 20, č. 4, s. 3-21. ISSN 1210-3292.

[4] STRUŽKA, Petr. *Informační operace v NATO* [online]. Vyškov, 2009 [cit. 2012-11-22]. ISSN 1803-036X. Dostupné z: http://doctrine.vavyskov.cz/_casopis/2_09_A4.html.

[5] Terminologický slovník pojmů z oblasti krizového řízení a plánování obrany státu kybernetickou válku definuje jako: „Souhrnný název pro teroristické aktivity, jejichž cílem útoku, použitým prostředkem nebo přenašečem, je tzv. kyberprostor … a prováděné prostřednictvím počítačové sítě." In RAŠEK, A. Kybernetická válka pokračuje. *Vojenské rozhledy*, 2012, roč. 21 (53), č. 4, str. 73-89, ISSN 2010-3292.

[6] KUBEŠA, Milan a Ladislav KOLÁČEK. *Klamání v operacích*. 1. vydání. [Studijní text Univerzity obrany]. Brno: Vydavatelské oddělení UO, 2012, 107 s. ISBN 978-80-7231-896-4.