Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví
Studijní obor: informační studia a knihovnictví

Vít Černovský

Využití informací a informačních systémů ve vojenských operacích

Rigorózní práce

Konzultant rigorózní práce PhDr. Richard Papík, Ph.D.

Praha 2008

Prohlášení:

Prohlašuji, že jsem rigorózní práci zpracoval samostatně a že jsem uvedl všechny použité informační zdroje.

V Praze, 5. března 2008 Vít Černovský

Identifikační záznam

ČERNOVSKÝ Vít. *Využití informací a informačních systémů ve vojenských operacích (Use of Information and Information Systems in Military Operations)*. Praha, 2008. 155 s., 5 s. příl. Rigorózní práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví 2008. Konzultant rigorózní práce PhDr. Richard Papík, Ph.D.

Abstrakt

Tématem rigorózní práce je využití informací a informačních systémů ve vojenských operacích. Cílem práce je vysvětlit význam informačních operací, tj. informací a informačních systémů při vedení bojových kampaní a mírových misí, přiblížit a analyzovat jejich přínos pro současné i budoucí bezpečnostní operace. Práce se nejprve zabývá vzájemným vztahem informační a vojenské vědy a jejich pojetím informace. Dále vysvětluje pojem informační válka, včetně možných důsledků jejího působení. Analyzuje principy klamání a dezinformace a uvádí příklady jejich použití v reálných operacích. Pokračuje typologií informačních operací, včetně analýzy jednotlivých typů. Zabývá se rovněž plánováním informačních operací s důrazem na nejdůležitější kroky plánovacího procesu. V rámci strukturace historie informačních operací poukazuje na důležité mezníky v dějinách vojenství. Součástí práce je rovněž analýza využití a úspěšnosti vedení informačních operací v současných vojenských kampaních spolu s uvedením příkladů z krizových oblastí ve světě. Dále je zkoumána využitelnost informačních operací při boji s teroristickými skupinami, v prostoru fyzického bojiště a ve virtuálním prostředí internetu. V neposlední řadě se práce věnuje obraně proti informačním útokům a různým obranným opatřením. Vlastním přínosem autora je úvaha o možném vývoji informačních operací v brzké budoucnosti. Využití informací a informačních systémů je v této práci prezentováno jako výsledek činnosti vojenského umění a vědy, jehož význam prudce roste a který by se mohl stát i novým parametrem při porovnávání bojových kapacit ozbrojených sil.

Abstract

This rigorous thesis analyses use of information and information systems in military operations. The objective is to explain importance of information operations (information and information systems) in military campaigns and peace missions, clarify and analyse

their contribution to contemporary and future security operations. Thesis first examines a relation of both Information science and Military science. It further discusses their slightly different approach to information. Next, thesis explains the term information warfare with all possible impacts on an opponent. Thesis continues with comprehensive description and analysis of principles of deception and disinformation. Moreover it gives various examples of use of these techniques in real operations. Then it discusses the current typology of information operations and analyses the IO types. Thesis further describes the IO planning process with an emphasis on its main steps. Afterwards it highlights historical examples of IOs in well-known armed conflicts. Then, examples and analysis of use and success of IO in contemporary military campaigns follow. Further it looks into the problem of the IO deployment at war on terror. The author perceives the necessity of appropriate defence measures against the possible IO attacks as well and therefore concentrates on this topic in a special chapter. The author also believes that the importance of IO cannot be fully understood without a brief examination of IO in the future and comes out with his own ideas about the possible IO development. The study presents use of information and information systems as a result of military art and science of war. The significance of information and information systems grows so rapidly that they could once become new criteria for comparison of armed forces.

Klíčová slova

informační válka, informační operace, psychologické operace, elektronický boj, kybernetická válka, dezinformace, velení a řízení, klamání, informační systémy, internet, bojová operace, bezpečnostní složky, koaliční jednotky, al-Káida, teroristické skupiny, zpravodajské služby, informační nadvláda, propaganda.

Keywords

information warfare, information operations, psychological operations, electronic warfare, cyberwar, disinformation, command and control, deception, information systems, internet, military operation, security forces, coalition forces, Al-Qaeda, terrorist groups, intelligence services, information dominance, propaganda.

OBSAH

SEZNAM POUŽITÝCH ZKRATEK

AČR	Armáda České republiky
BBC	British Broadcasting Corporation
C2	Command and Control
C2I	Command, Control and Intelligence
C2W	Command and Control Warfare
CD	Compact Disc
CDMA	Code Division Multiple Access
CIA	Central Intelligence Agency
CNN	Cable News Network
CPO	Combat Psychological Operations
CRPO	Crises Response Psychological Operatinos
ČR	Česká republika
DIA	Defense Intelligence Agency
DVD	Digital Versatile Disc
EB	Elektronický boj
EIW	Economic Information Warfare
EM	Elektromagnetický
EW	Electronic Warfare
FUSAG	First United States Army Group
GIMF	Global Islamic Media Front
GLONASS	Globalnaja Navigacionaja Sputnikovaja Sistema
GPS	Global Positioning System
GSM	Global System for Mobile communications
IBW	Intelligence Based Warfare
INFOSYS	Informační systémy
IO	Information Operation
ISAF	International Security Assistance Force
IW	Information Warfare

KFOR	Kosovo Force
KGB	Komitet Gosudarstvenoj Bezopasnosti
LOAC	Laws of Armed Conflict
MO	Ministerstvo obrany
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
OSN	Organizace spojených národů
OSS	Office of Strategic Services
PSYOP(S)	Psychological Operation(s)
PSYW	Psychological Warfare
RSHA	Reichssicherheitshauptamt
SD	Sicherheitsdienst
SFOR	Stabilisation Force in Bosnia and Herzegovina
SPO	Strategic Psychological Operations
TDMA	Time Division Multiple Access
USA	United States of America
USD	United States dollar

PŘEDMLUVA

Tématem mé rigorózní práce je problematika využití informací a informačních systémů ve vojenských operacích. Práce vychází z mé diplomové práce *Informační válka*. Diplomová práce však byla zaměřena především na ofenzivní informační činnost vojenských jednotek. Tato rigorózní práce je doplněna o další kapitoly věnované plánování informačních operací a možným způsobům obrany proti informačním útokům. Přepracována je pasáž zabývající se klamáním, která byla doplněna o problematiku dezinformací a propagandy. Těmito metodami informačního působení se diplomová práce nezabývala, pouze se o nich zmiňovala. Doplněny byly také oddíly zabývající se informacemi z pohledu informační a vojenské vědy, rozšířena byla část analyzující různé definice informační války a rovněž typologie informačních operací. Kapitoly týkající se informačních operací teroristických skupin a budoucnosti informačních operací byly aktualizovány o nejnovější poznatky z této problematiky.

Toto téma rigorózní práce jsem si zvolil z několika důvodů. Prvním je skutečnost, že stále pracuji na Ministerstvu obrany České republiky a proto je mi tato oblast, zejména v době reálných kybernetických útoků, odborně blízká. Mým druhým důvodem je, že jsem během zpracování diplomové práce nezužitkoval veškeré poznatky a zdroje získané v letech 2003 až 2004 během studia na Cranfield University, na fakultě Royal Military College of Science ve Shrivenhamu. Již tam mě tato problematika velmi zaujala, i když nebyla přímo součástí studia. Byla zde probírána v souvislosti s tzv. revolucí ve vojenských záležitostech. Proto jsem se při volbě tématu rozhodl využít příležitosti zabývat se informačními operacemi, tedy problematikou, která prolíná oběma obory, jak informační vědou, tak vojenskou vědou. V této rigorózní práci jsem využil dosavadní zkušenosti a znalosti získané z praxe, ze studia ve Velké Británii a zcela nové poznatky získané během studia na Ústavu informačních studií a knihovnictví. Jako příslušník vojenského rezortu jsem měl vždy tendenci nahlížet na informační operace z hlediska vojenského, tzn. z hlediska vedení operace za účelem dosažení stanoveného cíle, ale ne z hlediska

informačního, protože jsem tyto vědomosti postrádal. Podstatu využití informací a informačních systémů ve vojenských operacích je však možné, podle mého názoru, mnohem lépe pochopit, když člověk získá vojenské i informační vzdělání. Informace a informační systémy totiž v současné době zásadním způsobem ovlivňují úspěšnost jakékoliv bezpečnostní operace, včetně dlouhodobé války proti terorismu. Využívání informací nelze v žádném případě zlehčovat nebo podceňovat na úkor vlastní bojové činnosti, protože právě ta je přímo ovlivňována včasností, přesností a věrohodností dostupných informací.

Cílem této rigorózní práce je vysvětlit význam využití informací a informačních systémů ve vojenských operací, přiblížit ho v historickém kontextu, nastínit využitelnost a význam klamání a dezinformací, vysvětlit proces plánování informačních operací, specifikovat jednotlivé typy informačních operací, objasnit složitost a komplexnost obrany proti informačním útokům a poukázat na nezbytnost využívání informací a informačních systémů ozbrojenými složkami v současných a v budoucích vojenských operacích. Informační operace nevedou pouze silové složky, ale některé z nich běžně využívají komerční firmy v civilním sektoru. Vzhledem k rozsahu se však tato práce zaměřuje pouze na informační operace ozbrojených sil, tj. na operace, kde jsou informace a informační systémy nasazeny do vojenských operací jako jedna z mnoha zbraní. Problematika informačních operací v civilním sektoru by byla novým, ne příliš probádaným tématem, který by si určitě zasluhoval samostatné zpracování.

Tato práce není první svého druhu. V zahraničí jsou informační operace běžným tématem diplomových a disertačních prací, zejména na vojenských školách a univerzitách. V západní Evropě a ve Spojených státech se jimi zabývá i řada autorů, kteří nejsou z rezortu obrany, ani se nepovažují za vojenské odborníky a teoretiky. Počet zahraničních publikací proto každoročně přibývá. V České republice však dosud nebyly informační operace komplexně zkoumány a analyzovány. Tato rigorózní práce je proto jednou z prvních, ne-li vůbec první, která se zabývá nejenom nasazením informací a informačních systémů do operací, ale i plánováním těchto operací a ochranou nasazených sil a prostředků. Právě tato skutečnost, nedostatek českých publikací, kterou jsem si plně uvědomil již při zpracování diplomové práce, se stala mým třetím důvodem volby tématu. Rozhodl jsem se problematiku ještě rozšířit a dopracovat, aby se stala rigorózní práce ucelenou studií, která by se mohla stát základem odborné knižní publikace v době, kdy je

toto téma aktuální a Česká republika dokonce zvažuje vybudování centra boje proti kyberterorismu.

Při psaní rigorózní práce jsem čerpal informace z otevřených zdrojů, zejména odborných knih, periodik a neutajovaných amerických a aliančních vojenských předpisů. Rovněž jsem využíval internetové zdroje, včetně komerčních databází jako např. Jane's a Middle East Newsline. Kromě otevřených zdrojů jsem se rozhodl využít i rozhovoru s bývalým příslušníkem koaličních jednotek v Afghánistánu, Přemyslem Horáčkem. Jako doplňkový zdroj jsem využil pro zpracování příloh rovněž archivní materiály z Vojenského historického archivu v Praze. Problematiku informací a informačních systémů řeší z mnoha různých pohledů i různé utajované vojenské předpisy a řády. V případě jejich využití by však musela mít patřičný stupeň utajení i tato rigorózní práce. Z tohoto důvodu jsem se při jejím zpracování rozhodl utajované dokumenty nevyužívat. Podkladů, ze kterých bylo možné čerpat potřebné informace k jednotlivým částem diplomové práce bylo, vzhledem k možnosti využít soukromý knižní fond z Velké Británie dostatek. Přesto však množství literatury, které je dostupné pouze komerčně přes zahraniční internetové prodejce a v knihovnách zahraničních vojenských akademií, zůstává neprostudováno.

Způsob citace použité literatury vychází z norem ISO 690 a ISO 690-2.

Za poskytnutí cenných rad, konzultací a vstřícný přístup v průběhu zpracování práce bych rád poděkoval na tomto místě konzultantovi mé rigorózní práce PhDr. Richardu Papíkovi, Ph.D. Poděkování patří rovněž Přemyslu Horáčkovi za poskytnutí cenných informací získaných na základě vlastních zkušeností přímo z vojenské operace.

ÚVOD

Rigorózní práci tvoří celkem deset kapitol. Pomyslně ji však lze rozdělit na čtyři části. První a poslední jsou úvahou o daném tématu, druhá až čtvrtá jsou kapitoly teoretické, šestá až osmá se zabývají skutečnými příklady využití informací a informačních systémů ve vojenských operacích. Zvláštní povahu mají kapitoly pátá a devátá, jejichž obsah je zčásti teorie, zčásti úvaha. V praxi jsou obě chápány jako návod, či předpis, avšak nikdy se nesmí stát neporušitelným dogmatem. Ve skutečných operacích má velký podíl na úspěchu kromě dodržování předpisů i lidská předvídavost a intuice. Vlastní obsah jednotlivých kapitol stručně popisuje následující text.

První kapitola se zabývá možným vztahem informační vědy a vojenské vědy, včetně informačních operací. Stručně objasňuje, jak oba vědní obory vnímají pojem informace, jaké jsou její vlastnosti a jaký je pohyb informace v rámci zpravodajských služeb. Kapitola dále vysvětluje, že rozdílnost pojetí informace nestaví tyto vědní obory proti sobě, naopak mají mnoho společného a dokonce se vzájemně prolínají.

Druhá kapitola se věnuje pojetí fenoménu „informační válka“. Nejprve se jím zabývá v obecné rovině, poté uvádí a vysvětluje definice americké a evropské provenience. V těch dosud neexistuje shoda, vojenští velitelé, teoretici a filosofové se přou o vhodnost obecné, nebo naopak konkrétní a úzké definice tohoto pojmu. Mezi jinými definicemi je zde uvedena i zajímavá definice profesora Bellamyho z Royal Military College of Science z Velké Británie – psyberwar. V kapitole je dále vysvětlen pohled čínských odborníků na tuto problematiku.

V kapitole třetí je objasněna podstata klamání, včetně procesu vnímání okolní reality. Stručně jsou také představeny možné způsoby klamání, včetně několika příkladů. Kapitola se dále zabývá teorií dezinformace, včetně propagandy, různých technik a metod provádění dezinformačních kampaní. V této souvislosti jsou, s cílem lépe objasnit problematiku, uvedeny příklady historických dezinformačních akcí.

V kapitole číslo čtyři je uvedeno, v souladu s nejběžnějším způsobem dělení, sedm typů informačních operací (působení na velení a řízení, zpravodajské působení, elektronický boj, psychologická válka, ekonomicko-informační válka, hackerská válka a kybernetická válka). Informační operací se rozumí využití informací a informačních systémů jako zbraní a zbraňových systémů proti protivníkovi. Každý typ informačních operací je postupně vysvětlen, včetně možných způsobů jeho vedení. Většina těchto typů se při bezpečnostních operacích běžně používá, některé z nich jako např. kybernetická válka a hackerská zaznamenávají v současné době prudký rozvoj a jejich možnosti pravděpodobně sahají mnohem dále, než se dosud předpokládalo. Kapitola zdůrazňuje, že se při vojenské kampani zpravidla nevede jenom jeden typ informačních operací, ale používá se několik typů současně, protože jejich kombinace a vzájemné doplňování jejich účinnost znásobuje.

Pátá kapitola přináší stručný popis plánovacího procesu informačních operací, a zaměřuje se na jeho nejdůležitější fáze. Zdůrazňuje nezbytnost plánování nasazení sil a prostředků k provedení informačních operací. Bez něj by situace v prostoru nasazení byla chaotická a ani nasazení vyspělé techniky v nesprávný okamžik by k úspěchu nevedlo. Kapitola rovněž poukazuje na některá možná omezení, která je nutno do plánu zahrnout, protože jejich zanedbání by mohlo ohrozit nejen úspěch informační operace, ale i celé vojenské kampaně.

Po vysvětlení teorie a návodu na vedení informačních operací následuje kapitola šestá, která poukazuje na skutečnost, že informační operace nejsou nic nového, ale že jsou skutečně staré jako válka sama. Principy informační operace zvládl již ve čtvrtém století před naším letopočtem čínský stratég Sun Tzu, i když jí tehdy informační operací nenazýval. V kapitole jsou postupně uváděny vybrané historické příklady z období před druhou světovou válkou a z druhé světové války, kdy nastal skutečný rozmach informačních operací. Kapitola pokračuje příklady z druhé poloviny minulého století, včetně nedávné bojové operace „Pouštní bouře“ a nebojové operace v Bosně a Hercegovině.

Následující sedmá kapitola se zabývá informačními operacemi v současných vojenských operacích. Zaměřuje se na tři nejznámější a nejdůležitější krizové oblasti – Kosovo, Irák a Afghánistán. Vysvětluje způsoby vedení informačních operací v prostoru nasazení

mezinárodních vojenských kontingentů, včetně důvodů použití právě těchto forem. Zdůrazňuje zejména rostoucí význam psychologické války jako součásti všech současných vojenských kampaní. V případě vojenské operace v Afghánistánu poukazuje na skutečnost, že informační válku zde vede i protivník koaličních jednotek – hnutí Talibán.

V kapitole osmé, která vysvětluje použití informačních operací v boji proti terorismu, je k jejímu správnému pochopení nejprve uvedena stručná charakteristika současného terorismu. Její první část vysvětluje význam internetu pro současné teroristické skupiny a popisuje způsoby jeho využívání. Teroristé zatím využívají světovou síť internet jako podpůrný prostředek k dosažení svých cílů, ne k fyzickým útokům ani útokům proti infrastruktuře. Jejich způsoby a metody využití jsou však čím dál dokonalejší a současná bezpečnostní opatření (včetně informačních operací), kterými se zabývá druhá část kapitoly, nejsou zatím příliš efektivní. Závěr kapitoly proto dospívá k názoru, že rozhodující válka proti teroristickým skupinám – válka v počítačové síti na bezpečnostní složky teprve čeká.

Možnosti obrany proti působení nepřátelských informací a informačních systémů se věnuje devátá kapitola. Vysvětluje obtížnost obrany státní infrastruktury před informačními útoky, které se nebudou soustředit pouze na vojenské cíle. Vzhledem k provázanosti státního a soukromého a vojenského a civilního sektoru je k zajištění minimalizace hrozeb a účinků informačních útoků zcela nezbytná součinnost státních orgánů, soukromých firem, záchranné služby a silových složek. V této souvislosti jsou v kapitole vysvětleny problémy, které mohou nastat právě kvůli širokému spektru kooperujících orgánů. Silové složky, zejména vojenské jednotky mají pro případy informačního útoku vypracovány postupy, jakým způsobem vést účinnou obranu, tzv. protiopatření. Nejdůležitější z nich jsou v kapitole vysvětleny.

Kapitola desátá se zamýšlí nad významem a vývojem informačních operací v brzké budoucnosti. Vysvětluje jejich rostoucí význam a uvádí příklady různých vizí brzké budoucnosti. Ty pokládají za rozhodující faktor k dosažení vítězství nad protivníkem získání informační nadvlády. V kapitole je dále uveden předpokládaný rozvoj některých současných typů informačních operací, možné nové typy informačních operací a není vyloučen ani, v souvislosti se zaváděním pokročilých technologií a využíváním nových materiálů, vznik typů zcela nových.

. INFORMACE Z POHLEDU INFORMAČNÍ A VOJENSKÉ VĚDY

ÚVOD

Současná společnost se stále více přibližuje představám informační společnosti, jejímiž hlavními rysy jsou převaha práce s informacemi, interaktivita, integrační a globalizační tendence. Z technologického pohledu lze říci, že informační společnost je společnost s vysokou mírou využívání informačních a komunikačních technologií založených na prostředcích výpočetní techniky a s nimi spojenou digitalizací. Stoupající potřeba komunikace, sdílení a výměny informací však charakterizuje nejen civilní, ale i vojenské instituce. Vzrůstající závislost vojenské techniky na elektronických prostředcích, které pracují s nepředstavitelným množstvím informací a rostoucí význam informací samotných způsobily, že se informace staly lukrativním cílem bojového působení, ale současně i hodnotnou zbraní. [141] Tyto změny jsou přímo převratné z hlediska pohledu na informaci i z hlediska způsobu vedení války. Není proto divu, že se v současné době stále více hovoří o tzv. informační válce[1]. Ta je výsledkem činnosti vojenské vědy a vojenského umění a má mnoho společného s informační vědou. Společným předmětem zájmu informační vědy i informační války, kterou lze v nejširším pojetí charakterizovat jako „*společné nasazení dostupných bojových kapacit k ovlivnění, znehodnocení, ovládnutí a zarušení nepřátelských velitelských kapacit, včetně automatizovaných prostředků rozhodování; a současně zajistit ochranu všech těchto vlastních prostředků před nepřítelem*“, [32] jsou totiž informace.

POJETÍ INFORMACE

Informace je mnohovýznamový pojem, s nímž se každý člověk setkává téměř denně; uvádí Cejpek. [21] Je to jev univerzální, pevně spjatý nejen s každodenním životem člověka

[1] Pojetí a definice informační války jsou podrobně rozebrány v samostatné kapitole.

a společnosti, ale i s živou a neživou přírodou, pokračuje Cejpek a zabývá se, z jeho pohledu, jejími čtyřmi základními významy:

- psychofyziologický jev a proces v lidském vědomí;
- početní míra odstranění neuspořádanosti (entropie), míra organizace v systému;
- ve smyslu potenciální informace – znakově zaznamenané informace a cirkulující data v technických zařízeních;
- výraz různorodosti v objektech a procesech přírody.

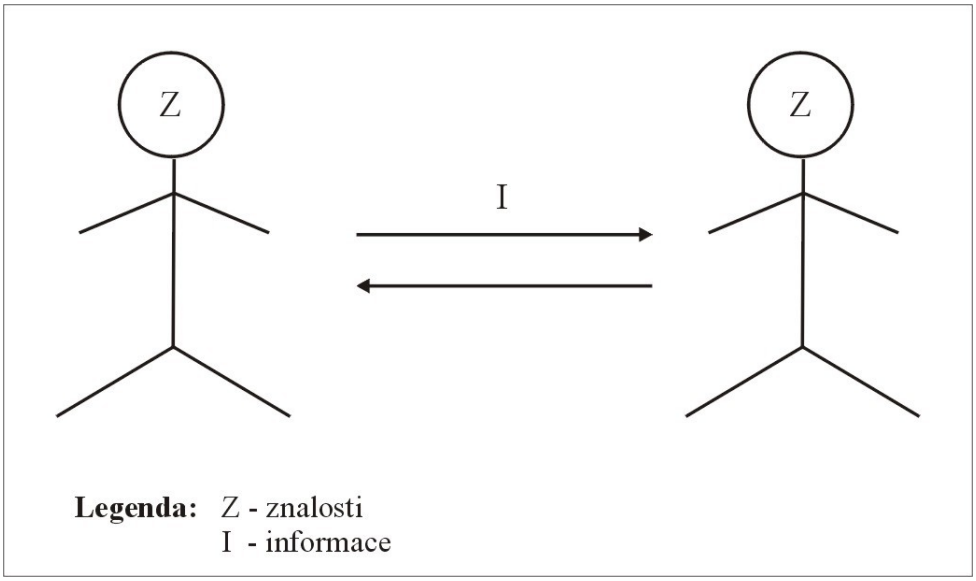
Definic pojmu informace v současné době existuje řada, dokonce tak mnoho, že to podle Cejpka může vést k závěru, že se jedná o pojem, který lze vykládat z nejrůznějších hledisek odlišně. V nejobecnějším slova smyslu však lze informaci chápat jako údaj o reálném prostředí, o jeho stavu a procesech v něm probíhajících.

Pojetí informace v informační a vojenské vědě

V informační vědě se informací rozumí především sdělení, komunikovatelný poznatek, který má význam pro příjemce nebo údaj usnadňující volbu mezi alternativními rozhodovacími možnostmi. [106] Vickery hovoří o informaci jako o znalosti, nebo spíše o druhu znalosti. Znalost přitom specifikuje jako to co lidé znají nebo si myslí, že znají. V tom případě je informace nový nebo modifikovaný poznatek, který je přidán, nebo asimilován do „znalostní struktury“ jednotlivce. [132] V této souvislosti se Britz dokonce domnívá, že Vickery chápe ze sociální perspektivy informaci jako proces, který probíhá mezi zdrojem (informace) a uživatelem (informace). Informace není tedy pouze část nebo produkt procesu, ale proces samotný (od vzniku informace až po její využití). Jedná se samozřejmě o jeden z přístupů k pojetí „informace“. Jako další lze zmínit uživatelský přístup, což v nejširším pojetí znamená, že informace je to co redukuje výši, či stupeň nejistoty. Z hlediska obsahového přístupu pak lze za informaci považovat to co je mezi lidmi komunikováno. Podle kybernetického pojetí Norberta Wienera je informace název pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním. Informace není, podle něj ani hmotou, ani energií; Wiener jí tím řadí, zdůrazňuje Cejpek, k univerzálním pojmům, jako jsou např. hmota a energie. [21] Oppenheim podobně jako Vickery považuje informaci za určitou jednotku, či stavební

kámen znalostí. Znalost totiž charakterizuje jako „*větší struktury vzájemně souvisejících informací*“. [96] Informace se transformuje na znalost, pokračuje Oppenheim několika různými způsoby, mj. vzájemným porovnáním, následkem (jak daná informace souvisí s následným rozhodnutím, jak je pro něj důležitá), prostřednictvím souvislostí (jak spolu souvisí jednotlivé bity znalostí) a konverzací či komunikací mezi lidmi (co si ostatní myslí o dané informaci). Podle kognitivního modelu (viz obr. 1) jsou znalosti jakási „vnitřní hodnota“ v mysli lidí, která nemůže být přímo komunikována.

Obrázek 1. Princip komunikace



Zdroj: Upraveno a převzato z OPPENHEIM Charles, STENSON Joan and WILSON Richard. Studies on Information as an Asset I: Definitions

K tomu slouží právě informace, které tak tvoří most mezi subjektivními znalostmi a objektivní znalostmi, které již mohou být komunikovány a přenášeny. Oppenheim v této souvislosti zmiňuje definici Elizabeth Orny, podle níž „*je informace to co člověk transformuje ze svých znalostí do sdělení, když potřebuje komunikovat s ostatními lidmi*“. Téměř stejně pojetí informace chápal již v roce 1976 Farradane z Univerzity Západního Ontaria, když na konferenci Institutu informačních vědců definoval informaci jako „*jakoukoliv fyzickou formu reprezentace, nebo jinou náhražku znalostí či konkrétní myšlenky použitou pro komunikaci*“. [42] Rozumný smysl toho co je mezi lidmi komunikováno a celý kognitivní model je samozřejmě závislý, zdůrazňuje Oppenheim, na individuální schopnosti lidských bytostí přenést svoje znalosti na informace, které mají být komunikovány (předávány v rámci lidské společnosti). Existují i další přístupy, jak uvádí Britz, např. ideologický, znalostní nebo anti-definiční. Zastánci posledně zmiňovaného

jsou proti pokusům definovat termín informace, protože to údajně nemá žádný praktický význam pro informační vědu. [16]

Vojenská věda se pojmem informace zabývá z jiného pohledu, protože má i rozdílné poslání než informační věda. Jejím cílem není zkoumat informaci jako takovou, ale její efektivní využití v rámci bojové činnosti. Z hlediska vojenského má proto informace mnohem užší význam a je definována jako: „*nezpracované údaje jakéhokoli popisu, které je možné použít při vytváření zpravodajství*“. [134] Zpravodajstvím se v této souvislosti rozumí činnost, jejímž výsledkem je zpravodajská informace. Ta je pak definována jako „*výsledek zpracování informací, týkajících se cizích států, nepřátelských a potenciálně nepřátelských sil nebo prvků či prostorů aktuální nebo potenciální bojové činnosti*“. [122] Další možné vymezení zpravodajské informace – termín, který označuje informaci, jenž je konečným produktem zpracovaných údajů získaných zpravodajskou činností a zpravodajskými prostředky. Tím se rozumí, že nejde o údaje běžně dostupné. Kromě těchto vymezení může mít zpravodajská informace, jak uvádí Bucharová, [19] ještě několik jemnějších významů (různá pojetí rozsahu):

- Informace získaná pouze operativní cestou (pak zpravodajský = operativní) - nejužší.
- Informace získaná (všemi) skrytými metodami – širší.
- Informace získaná všemi skrytými metodami, zpracováním otevřených zdrojů a následnou analytickou prací – nejširší.

Vlastnosti informace z pohledu vojenské vědy

Informace má z pohledu vojenské vědy a tudíž i v kontextu jedné z forem moderní války – informační války několik základních vlastností, které jsou naprosto v souladu s pojetím informační vědy. Jedná se, podle Waltze, o tyto důležité, jedinečné a zároveň obtížně měřitelné vlastnosti [141]:

- Informace je abstraktní pojem – je nehmotná; může mít formu různé entity (podstatné jméno – např. lokalita, popis, rozměr) nebo procesu (sloveso – např.

vyjadřující proces kódování, chemický proces, vztah zbraňových systémů nebo jednotek).

- Informaci lze mnohonásobně využít, kromě toho umožňuje i současné využití více uživateli. Stejnou informaci (jednotku informace, např. o přesné lokalitě a frekvenci rádiového vysílače) lze využít spojovacími jednotkami k účelům navázání spojení, jednotkami EB k zarušení vysílače, raketovými jednotkami k přesnému zaměření a zničení vysílače, atd. Informaci o počasí mohou dokonce využít obě válčí strany a z hlediska informačního bude pro obě přínosná.
- Informace je nevyčerpatelná (na rozdíl od jiných zdrojů), avšak její hodnota[2] se v čase mění (může úplně pozbýt hodnoty), lze tedy říci že je dočasná - aktuální informace má okamžitou hodnotu (doslova akční – pro vojenské využití), stará informace může mít pouze historickou hodnotu. Zároveň je informace také nijak neomezená je „bez hranic“ – lze jí objevit, vytvořit, transformovat nebo opakovat.
- Vztah informace a jejího užití (využitelnosti) je komplexní a nelineární. Využitelnost nebo hodnota informace není jednoduše pouze funkcí objemu a množství informačních jednotek. Závisí na svém obsahu a jeho čitelnosti (zda je nebo není poškozen – např. působením nepřátelských jednotek) a na účinku nebo dopadu na znalosti o reálném světě (ve vojenství obrazu bojiště).

Vojenská věda stejně jako informační věda zkoumá rovněž vzájemný vztah dat, znalostí, informací a okolního prostředí, které formování znalostí ovlivňuje. Kromě procesu přijímání dat, vytváření znalostí a následné komunikace pomocí informací je však v zájmu vojenské vědy zjistit možnosti jak lze vztah jednotlivých součástí komunikačního procesu ovlivnit nebo naopak zajistit jeho ochranu. Pokud k ovlivnění dojde (informačním útokem), je jeho výsledkem záměrně znehodnocená a nepravdivá informace (viz. příloha č. 1). Právě to je však cílem informačních operací.

Pohyb informace v rámci vojenských zpravodajských služeb

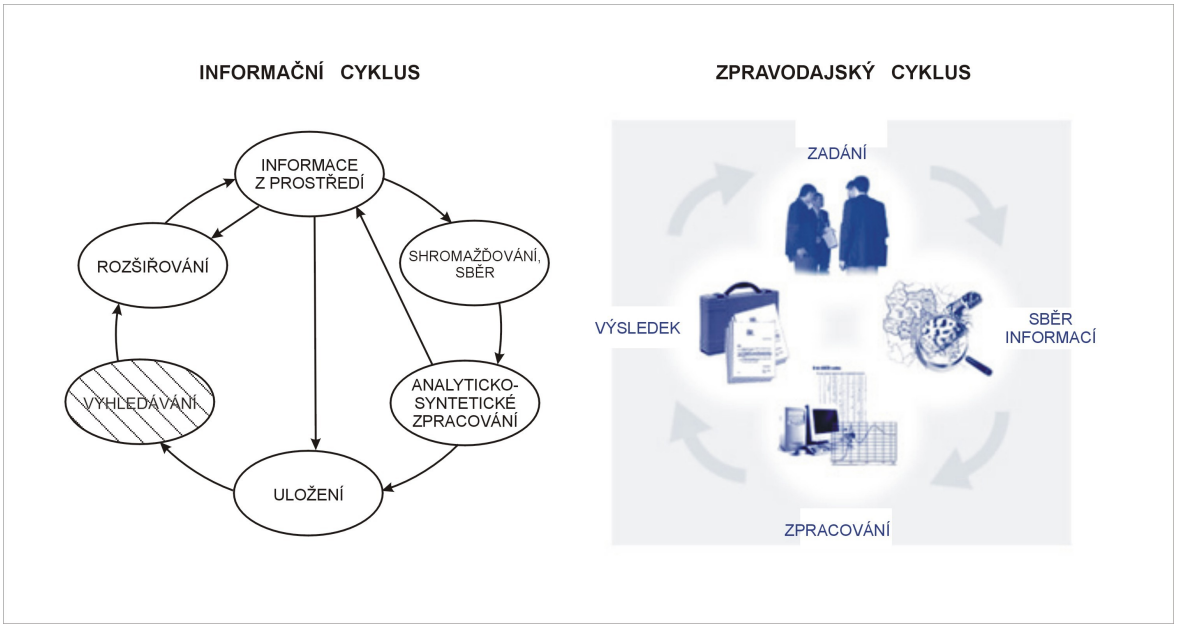
Z hlediska informačního lze v rámci ozbrojených sil považovat za informační instituci především vojenskou zpravodajskou službu. Informace stejně jako u civilních

[2] Autor v této souvislosti úmyslně použil výrazu „hodnota“ jako překladu pro anglický výraz „value“. Lze ho chápat také jako význam nebo ocenění; ve vojenství se však preferuje termín hodnota.

informačních institucí jedou nejen směrem ke zpravodajské službě – zpravodajská služba nejen informace shromažďuje, ale po zpracování a vyhodnocení je rovněž distribuuje. Předané informace jsou důležité pro rozhodovací činnost státu, jak uvádí Bucharová. [19]

Pohyb, nebo – li řetězec postupných a vzájemně navazujících činností, při nichž jsou informace získávány, zpracovány, vyhodnoceny a předány uživatelům se nazývá zpravodajský cyklus „*intelligence cycle*“[3]. Je složen ze čtyř fází: řízení, shromažďování, zpracování a šíření [122] a má podobný průběh jako klasický informační proces (viz. obr. 2).

Obrázek 2. Informační cyklus a zpravodajský cyklus



Zdroj: BUCHAROVÁ Lenka. *Informační zdroje v oblasti bezpečnosti státu*.

Používané názvy jednotlivých fází se mohou lišit, jedná se však o synonymní termíny. *Výkladový slovník pojmů a definic NATO* popisuje jednotlivé fáze zpravodajského cyklu následovně [134]:

a) řízení – stanovení zpravodajských požadavků, plánování a sběru informací, vydání rozkazů a požadavků orgánům pro sběr informací a udržování neustálé kontroly nad jejich činností;

[3] Ve zpravodajské terminologii se používá i termínu zpravodajský proces „intelligence process“.

b) sběr (shromažďování) – využití zdrojů orgány pro sběr zpráv a dodání získaných informací příslušné jednotce, která se zabývá jejich zpracováním;
c) zpracování – přeměna informací na zpravodajské informace pomocí porovnání, analýzy, spojení a výkladu;
d) šíření – včasná distribuce zpravodajských informací[4] ve vhodné formě a jakýmikoli vhodnými prostředky těm, kteří je potřebují.

V amerických vojenských předpisech, jako např. v *Doktríně pro zpravodajskou podporu společných operací* [33] se rozlišuje dokonce fází pět (viz. příloha č. 2). Zpracování a analýza informací jsou odděleny do dvou samostatných fází; při fázi zpracování a vytěžování dochází k přeměně (předzpracování, či prvotní zpracování) „surových informací“ do formy, kterou jsou schopni bez problémů využít analytičtí pracovníci. Jedná se mj. o popis družicových snímků, přeměnu získaných dat do čitelné podoby, překlad dokumentů nebo dekódování zpráv. Praktickým příkladem jsou data získaná signálovým zpravodajstvím (frekvence, vlnový rozsah, atd.), která převede do podoby čitelné pro analytika odborný technický personál a sdělí mu přímo identifikační údaje příslušného radiolokátoru. Rozdílné typy informací získané různými prostředky samozřejmě vyžadují i různý stupeň a způsob zpracování, než je využije analytický personál. Při analytické fázi zpravodajského cyklu dochází k syntéze, analýze, porovnání, vyhodnocení a interpretaci, stejně jako při fázi zpracování uváděné *Výkladovým slovníkem NATO*. V podmínkách ČR je „prvotní zpracování“ součástí sběru informací, při vlastním zpracování (analýze) se již pracuje s „čitelnými“ informacemi. Důvodem jeho zařazení jako samostatné fáze v amerických podmínkách jsou pravděpodobně odlišné kapacity a možnosti průzkumných prostředků a zdrojů všeho druhu ve srovnání s ozbrojenými silami jiných států. Informací získaných těmito zpravodajskými orgány a prostředky je nesrovnatelně více, proto je i jejich prvotní zpracování náročnější a pro další využití důležitější.

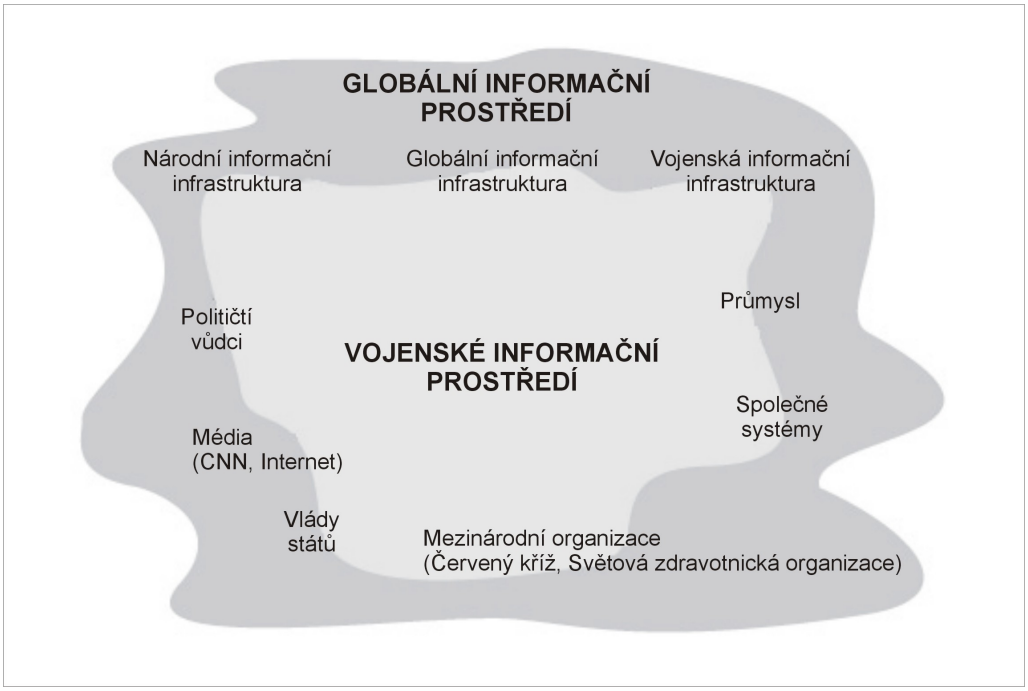
PROLÍNÁNÍ INFORMAČNÍ A VOJENSKÉ VĚDY

Rozdíl v chápání informace nijak nestaví oba vědecké obory proti sobě, naopak dochází k jejich vzájemnému prolínání. Vojenská věda se s ohledem na své zaměření mj. soustředí na vojenské informační prostředí, které je samozřejmě součástí globálního informačního

[4] Starší literatura používala někdy místo termínu zpravodajská informace výraz zpráva, jako překlad anglického termínu „intelligence“.

prostředí a prolíná se i s civilním sektorem (viz. obr. 3). Vojenské informační prostředí je definováno jako prostředí, které je součástí globálního informačního prostředí a je tvořeno informačními systémy, organizacemi spřátelenými i nepřátelskými, vojenskými i nevojenskými, které podporují nebo významně ovlivňují konkrétní vojenskou operaci. [58]

Obrázek 3. Globální informační prostředí



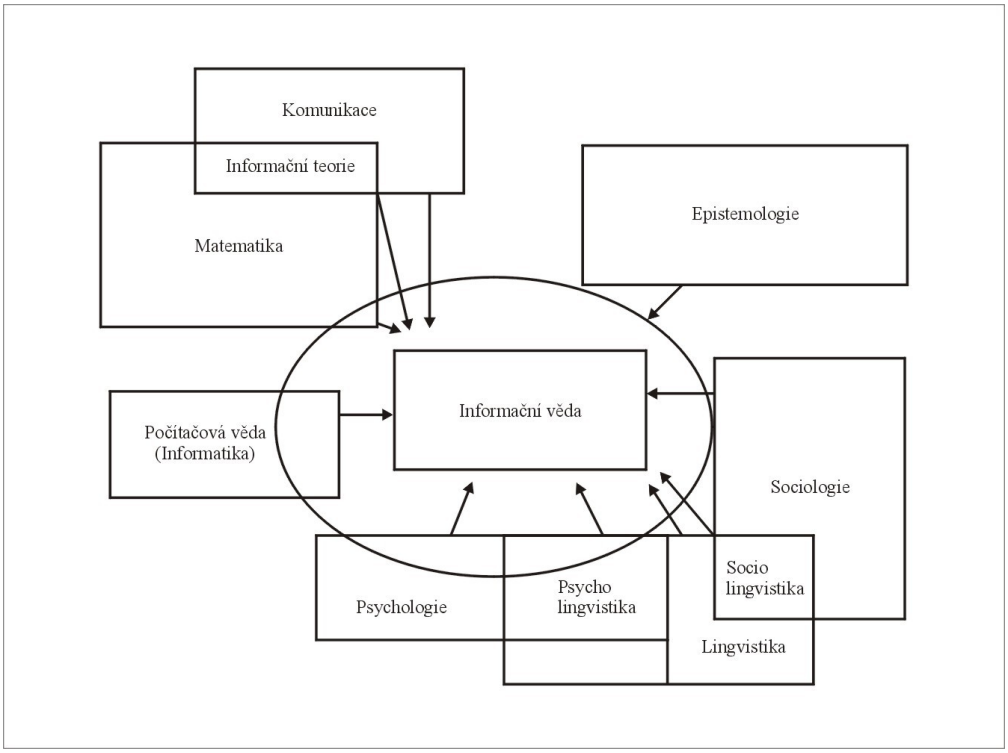
Zdroj: Upraveno a převzato z *Information Operations* FM 100-6.

Vojenská věda patří do kategorie věd společenských. Svým postupným formováním ve vědu v průběhu 19. a zejména 20. století patří k nejmladším, první podnět k jejímu vzniku však daly již vyhodnocované vzájemné střety různých ozbrojených skupin až armád ve starověku. Je obecně definována jako „*systém poznatků o charakteru a zákonech války, o vojenské přípravě státu a ozbrojených silách na válku a o způsobech jejího vedení*“. [119] Základním předmětem jejího zkoumání je proto ozbrojený zápas. Ten je třeba důsledně chápat, zdůrazňuje Novotný, jako cíleně organizované vzájemné se ničení dvou proti sobě působících ozbrojených systémů, prosazujících politickým vedením svých států či koalice států jim stanovené cíle ozbrojenou silou – armádami. [94] Vzniku vojenské vědy předcházely shromažďování, třídění, rozbory (analýzy) a vyhodnocování informací, poznatků a zkušeností z válek všech období zejména novověku, počínaje 19. století. První ucelenou teorií zásad vedení ozbrojeného zápasu je traktát *O válce*

Karla von Clausewitze. Těžiště postupného formování vojenské vědy souvisí s první a zejména druhou světovou válkou a po nich následujícím období až do současnosti. Přitom stejně jako pro všechny společenské i technické vědy, úzce spjaté s vědeckotechnickým poznáním a jeho uplatněním v praxi, platí také pro vojenskou vědu, pokračuje Novotný, že je vědou otevřenou a že její bádání a rozvoj skončí se zánikem ozbrojených konfliktů.

Informační vědu lze definovat v nejširším pojetí jako vědu o informaci (fyzikální, biologické, kulturní). „*V užším významu se jedná o vědu interdisciplinárního charakteru zabývající se zákonitostmi procesů vzniku, zpracování, měření, kódování, ukládání, transformace, distribuce a recepce informací ve společnosti*“. [106] Cílem informační vědy je, uvádí *Výkladový slovník české terminologie z oblasti informační vědy a knihovnictví*, zabezpečit a racionalizovat sociální informační a komunikační procesy. Vickery chápe informační vědu jako „*studium komunikace informací ve společnosti*“. [133] Takovou definici však považují někteří odborníci za příliš obecnou a širokou. Mezi ně patří např. Ingwersen z dánské Royal School of Library and Information Science, který definuje informační vědu jako „*nauku o vytváření, komunikaci a využívání informací*“. [62] Samozřejmě existuje celá řada dalších definic informační vědy, vzhledem k rozsahu této práce však představuji již jen definici, kterou zmiňuje Sheila Webber „*informační věda je interdisciplinární věda, která zkoumá vlastnosti a chování informace, zákonitosti kterými se řídí tok a využití informací a způsoby (techniky) zpracování informací k jejich optimálnímu uložení, vyhledávání a rozšiřování*“. [137] Informační věda čerpá, pokračuje Sheila Webber, z teorie psychologie, lingvistiky, sociologie, počítačové vědy (informatiky) a technických (inženýrských) věd [138] (viz. obr. 4).

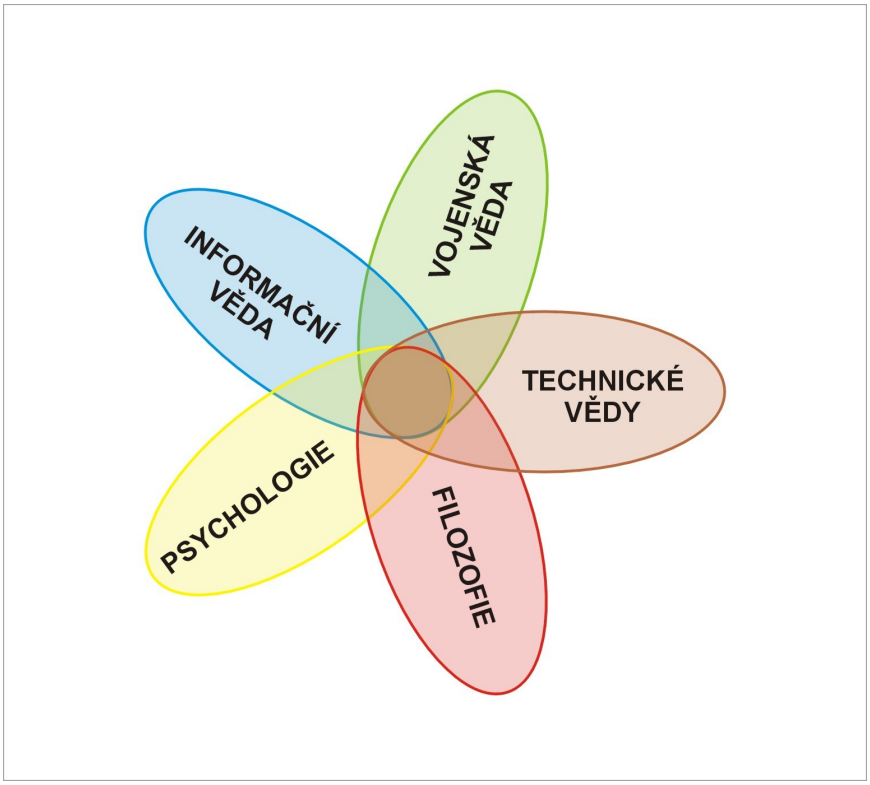
Obrázek 4. Vědecké disciplíny související s informační vědou



Zdroj: WEBBER Sheila and JOHNSTON Bill. Conceptions of information literacy: new perspectives and implications

Je tedy zřejmé, že informační věda není vědou izolovanou, ale zasahuje mj. do oblasti technických věd a informačních technologií (zejména výpočetní a komunikační techniky), psychologie, filozofie, atd. Vojenská věda také zasahuje do technických věd a samozřejmě do informačních a komunikačních technologií, součástí vedení války a velení vojskům je i filozofie a psychologie. Oba vědní obory spolu tedy nejenom souvisí, ale lze dokonce hovořit o jejich vzájemném prolínání, minimálně v těchto oblastech (viz. obr. 5).

Obrázek 5. Prolínání vědních oborů



Zdroj: Autorův vlastní diagram.

ZÁVĚR

Informační věda a vojenská věda, včetně informačních operací, které lze v této souvislosti chápat jako výsledek činnosti vojenské vědy, mají více společného než by se mohlo na první pohled zdát. Přestože obě disciplíny používají některé rozdílné termíny a definice, pojetí informace se v zásadě neliší, naopak lze říci, že v obecném slova smyslu informaci chápou naprosto stejně. Oba vědní obory se dokonce bez rozdílu shodují na tom, že na rozdíl od hmotných produktů se informace, tím že se využívá, nespotřebovává, a to i když ji využívá více lidí najednou. [21] Pro vojenskou vědu je vzájemné překrývání s informační vědou a vzájemnéپÀ24 lení poznatků nesmírně důležité. Informace totiž sehrávají v operačním prostředí roli samostatného činitele a postupně se stávají hlavním článkem jakéhokoli konfliktu. Pro informační vědu může být zase velmi zajímavé a prospěšné zaměřit se na vojenské prostředí, které skýtá obrovské možnosti z hlediska aplikace informačních znalostí a možného výzkumu dalšího uplatnění informace a informačních systémů nejen jako podpůrných prostředků vedení války, ale v informačním věku i jako zbraní.

. FENOMÉN ZVANÝ INFORMAČNÍ VÁLKA

ÚVOD

Žijeme v komplikované, a podle amerického geografa Gearóida Ó Tuathaila [97], ve zmatené době, v prostoru proloženém globalizací a zdeformovaném intenzitou a rychlostí informačních technologií. Čelíme třetí civilizační vlně informačního kapitalismu, která nastolí nový řád norem, hodnot, lidského chování a pravděpodobně i hmotných statků. Horizontálně organizované a virtuálně zasíťované digitální soupeřivé prostředí se stává charakteristickým rysem 21. století. Toto prostředí bývá často označováno jako infosféra nebo pátá dimenze. [105] Zbraně v něm používané se vyskytují ve formě nepřátelského software a pátá dimenze se v tomto smyslu stává prostředkem k získání strategické nadvlády. Tento druh konfliktu bývá nazýván jako kybernetická válka, digitální válka, virtuální válka, nebo zejména novináři jako informační válka. Tím je však podstata informační války zkreslována, protože se jedná pouze o jednu její formu. Rozsah informační války je totiž mnohem širší a neomezuje se pouze na virtuální svět počítačových sítí.

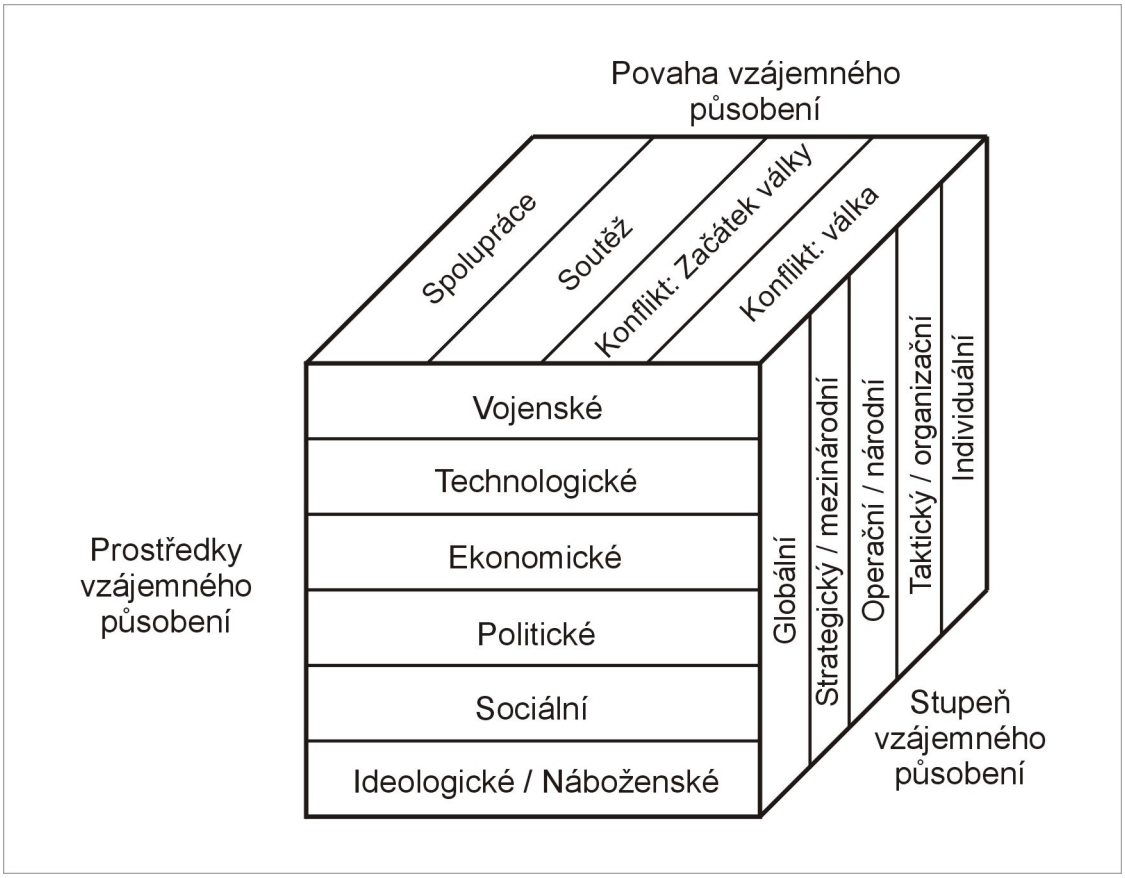
OBECNÉ POJETÍ

Pojem informační válka „*Information Warfare (IW)*“[5] může být chápán různě, dodnes neexistuje shoda na jeho vymezení. Někteří autoři spatřují v informační válce aktivity v oblasti komunikací, další zásahy do počítačových sítí informačních systémů, jiní vstupy a narušování datových sítí, zásahy do přenosů informací z průzkumných systémů a prostředků, nebo do systému velení a řízení vojskům. To proto, že konkrétní náplň a vnější projevy informační války, jak uvádí Hluboček [51], nejsou vždy zcela hmatatelné a přesně vymezené hlavně proto, že dosud nejsou přesně známy všechny její možné

[5] Téměř výlučně se používá termín Information Warfare, ne Information War. Použití termínu War naznačuje, že se jedná o válku v souladu s mezinárodním právem, tzn. v souladu se zákony války – „Laws on War“. Podle nich má válka oficiální začátek, je vyhlášena oficiálním právnickým subjektem (v tomto případě státem). Logicky potom tato válka i oficiálně skončí (formy ukončení jsou různé, např. uzavření mírových smluv, kapitulace, dohoda o příměří, jednostranná deklarace, atd.). Warfare se naproti vztahuje k vyjádření vlastní bojové činnosti, či prostředků k vedení bojové činnosti, např. elektronická válka (electronic warfare), námořní válka (naval warfare), apod. Termín válka a anglický ekvivalent war s oblibou používají novináři, často však v rozporu s uznávanou terminologií.

způsoby a formy. Na rozdíl od jiných, známých druhů války, lze stěží rozpoznat zahájení dílčích přípravných aktivit, ofenzívy a přesně stanovit její rozsah. [51] Ten může být různý. Informační válku lze totiž vést, jak uvádí David Alberts [2] ve sféře ekonomické, technologické nebo vojenské; na politické úrovni, operační, taktické nebo individuální; kromě toho se vzájemné působení (soupeřících stran) může odehrávat v míru, v období diplomatického napětí i během vlastního ozbrojeného konfliktu (viz. obr. 6).

Obrázek 6. Vzájemné působení soupeřících stran – rozsah informační války



Zdroj: Upraveno a převzato z ALBERTS David. *Defensive Information Warfare*.

Obtížné je rovněž vyhodnotit prvky informačních systémů, které byly napadeny a způsob tohoto napadení, vyčíslit ztráty, apod. Na první pohled relativně bezvýznamné napadení určité části informačního systému obvykle způsobuje řetězovou reakci, jejíž důsledky mohou být dalekosáhlé. Informační válka není zdánlivě ani vidět, ani slyšet. Je-li však rozpoutána v plné síle, její dopady a důsledky jsou deprimující, má vliv na pokles morálky a bojového ducha vojáků a ve svém důsledku má přímý vliv na bojeschopnost armády jako celku.

Pojem informační válka není sice dosud ustálen, k předběžnému orientačnímu vymezení lze však, podle Josefa Požára [102] z Policejní akademie ČR, použít skutečnosti, že další specifikací pojmu válka je nejčastěji prostředí, kde se válka odehrává. Pak je to válka námořní, vzdušná, kosmická, světová, lokální, apod. Druhým faktorem jsou prostředky vedení války. Jsou to mj. zbraně konvenční, jaderné, bakteriologické a také informační. V tomto smyslu je tedy např. válka konvenční vedena konvenčními zbraněmi nebo kosmická válka vedena kosmickými zbraněmi v kosmu. Analogicky pak informační válka je válka, která je vedena v oblasti informací nebo válka, v níž se bojuje informacemi. Informační válku by tedy bylo možné dále chápat jako válku o informace, tedy válku, kterou vedou lidé pracující s informacemi, případně jako válku, kterou charakterizují informace. Informace totiž v současné době sehrávají klíčovou úlohu nejen v civilní sféře, ale i ve vojenství. Mohou být dokonce jednou z nejmocnějších novodobých zbraní. Efektivnost použití složitých zbraňových systémů, jak zdůrazňuje Hluboček [51], je přímo závislá na kvalitě věrohodnosti a včasnosti informací o protivníkovi. Význam informace musí být v tomto smyslu chápán v co nejširším smyslu, jako synonymum pro poznání nebo vědění. Jen tak se totiž lze ujistit, že při zkoumání pojmu informační válka nic důležitého nechybí. Informační válka by v žádném případě neměla být chápána jako něco nového, výlučně spojeného s počítači, počítačovými sítěmi nebo dalšími moderními technologiemi, na tom se nezávisle shodují Hluboček [51] a Szafranski [120].

DEFINICE INFORMAČNÍ VÁLKY

Pokusů o definici informační války bylo mnoho. Shody však dosud mezi vojenskými odborníky dosaženo nebylo. Někteří autoři, jako např. Martin Libicki [78], se proto zabývají myšlenkou, zda je vůbec možné dosáhnout v tomto smyslu konsensu, dopracovat se jednotné definice, a zda je to vůbec nutné. Příliš úzká definice je nepřesná, protože zdůrazňuje, jak uvádí Bellamy [9], pouze jednu formu informační války na úkor ostatních. Na druhé straně příliš obecná a široká definice je nejasná a neumožňuje pochopit, co se pod pojmem informační válka skrývá. V takovém případě bude, podle Libickiho, velmi obtížné dát do přímé souvislosti její dvě základní součásti - informace a válku. [78] Typickým příkladem širokých, obecných definic jsou některé z prvních definic z počátku devadesátých let minulého století. Ty definují informační válku jako konflikt znepřátelených stran, který probíhá na strategické, operační a taktické úrovni; v době míru,

krize, eskalace napětí, války, ukončení konfliktu a obnovení míru, přičemž zúčastněné strany využívají informačních prostředků k dosažení svých cílů. [78] Taková definice, zdůrazňuje Libicki, zahrnuje většinu lidské činnosti, která je běžná při jakýchkoliv konfliktech. Nicméně, z perspektivního hlediska je užitečná k dalšímu rozpracování, neboť zahrnuje i využití informací. V tvorbě definic informační války se angažují zejména američtí a evropští vojenští odborníci. Čínská lidová armáda se rovněž v současné době velmi intenzivně zabývá koncepcí informační války. Její definice byly zpočátku většinou americké definice převzaté, nebo částečně upravené. [87] To však již neplatí, Čína se soustředí na zvládnutí informační války velmi intenzivně a usiluje o vytvoření vlastní, propracované koncepce jejího vedení a pojetí.

Americké definice

Americké vojenské námořnictvo definuje informační válku jako „*konflikt, ve kterém informace je současně zdrojem, cílem i zbraní*“. Podle Bellamyho se jedná o typický příklad příliš úzké definice, protože se zcela omezuje na kybernetickou válku „cyber-war“. [9] Podobně úzkou definici vypracovala i kanadská armáda, která ji ztotožňuje. s operacemi proti systému velení a řízení. Za informační válku považuje vojenskou strategii, která kombinuje opatření k narušení, zničení, nebo zamezení využití informací nepřátelskými prostředky velení a řízení. Termín strategický naznačuje, že by se mělo jednat o politicko-strategickou úroveň, což je však v rozporu s všeobecně známou praxí. Operace proti prostředkům velení a řízení se totiž vedou na operační úrovni. [9] Další definice, se kterou přišli američtí novináři, zdůrazňuje nutnost chápat informační válku ve třech různých souvislostech. V procesu řízení (managementu) je informace chápána jako zpráva či sdělení; v souvislosti se systémy určenými k ničení živé síly a prostředků protivníka je bojovým prostředkem a v souvislosti s využíváním protivníkem je zdrojem, který je primárním cílem útoku (likvidace). [9]

Americké vojenské letectvo uvádí ve svém dokumentu *Cornerstones of Information Warfare* [28] několik příkladů, kdy lze vzdušný úder považovat za informační válku. Prvním je pumový útok na spojovací uzly s cílem paralyzovat protivníkovo spojení, čili přenos informací; druhým jsou protiopatření a obrana vlastních prostředků spojení proti leteckému úderu protivníka a třetím je nasazení antivirových programů do operačního

použití k zajištění ochrany vlastního hardware a software, tedy možnost informaci přijmout, zpracovat, uložit a distribuovat. Kromě toho považuje za informační válku také útok na strategické cíle protivníka a protivzdušný úder k zastavení protivníkova útoku, tedy leteckou válku. Jsou to tedy, jak uvádí Libicki [78], útočná a obranná opatření s cílem přerušit, nebo zabránit informačnímu toku z nejvyšších míst velení a řízení a tak paralyzovat fyzicky i psychicky protivníkovi jednotky.

Americký Společný štáb náčelníků štábů druhů vojsk definoval v *Doktríně informačních operací* [59] informační válku jako „*operaci k dosažení informační převahy pro podporu národní bezpečnosti ovlivněním a působením na protivníkovi informace, informační systémy a počítačové sítě, za současného zajištění ochrany vlastních informací, informačních systémů a sítí*“. Tato definice je, podle Bellamyho [9], důležitá, ze dvou důvodů. Rozlišuje totiž tři různé aspekty informační války – informace, informační systémy a počítačové sítě. Zahrnuje proto široké spektrum operací, počínaje nasazením počítačových virů a konče pumovým útokem na rozhodující komunikační centra. Zahrnuje rovněž útočná i obranná opatření a není zcela zjevně omezená pouze na ozbrojené síly.

Polní manuál amerického pozemního vojska [60] definuje informační operace „*Information operations (IO)“*[6] jako „*nasazení klíčových kapacit elektronického boje (EW), 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*“. Tato definice je komplexní, je však, na rozdíl od předcházející limitovaná na ozbrojené síly. V tomto případě to ale není nedostatek, protože je určená pro pozemní vojsko.

Ostatní definice

Zástupce české vojenské odborné komunity Josef Nastoupil [89] definuje informační válku jako „*souhrn veškerých opatření pro a) ochranu vlastních informací a procesů na nich*

[6] Termín informační operace se někdy používá, zejména ve vojenských předpisech, aby se zdůraznil široký rozsah použitých prostředků při vedení informační války, a aby se uživatel nedopouštěl záměny termínů warfare a war (k čemuž může dojít při používání termínu informační válka). Pro účely této práce lze termíny IW a IO chápat jako synonyma.

založených, jakož i pro ochranu informační techniky; b) pro působení na nepřátelské informace a procesy na nich založené, jakož i pro působení proti nepřátelské informační technice“. Informační válka je tedy vedení války s využitím útočných opatření proti nepřátelské informační infrastruktuře a opatření k ochraně vlastní infrastruktury. Taková definice je značně obecná, míra pochopení a porozumění frázi „na informacích založené procesy“ záleží pouze na představivosti čtenáře.

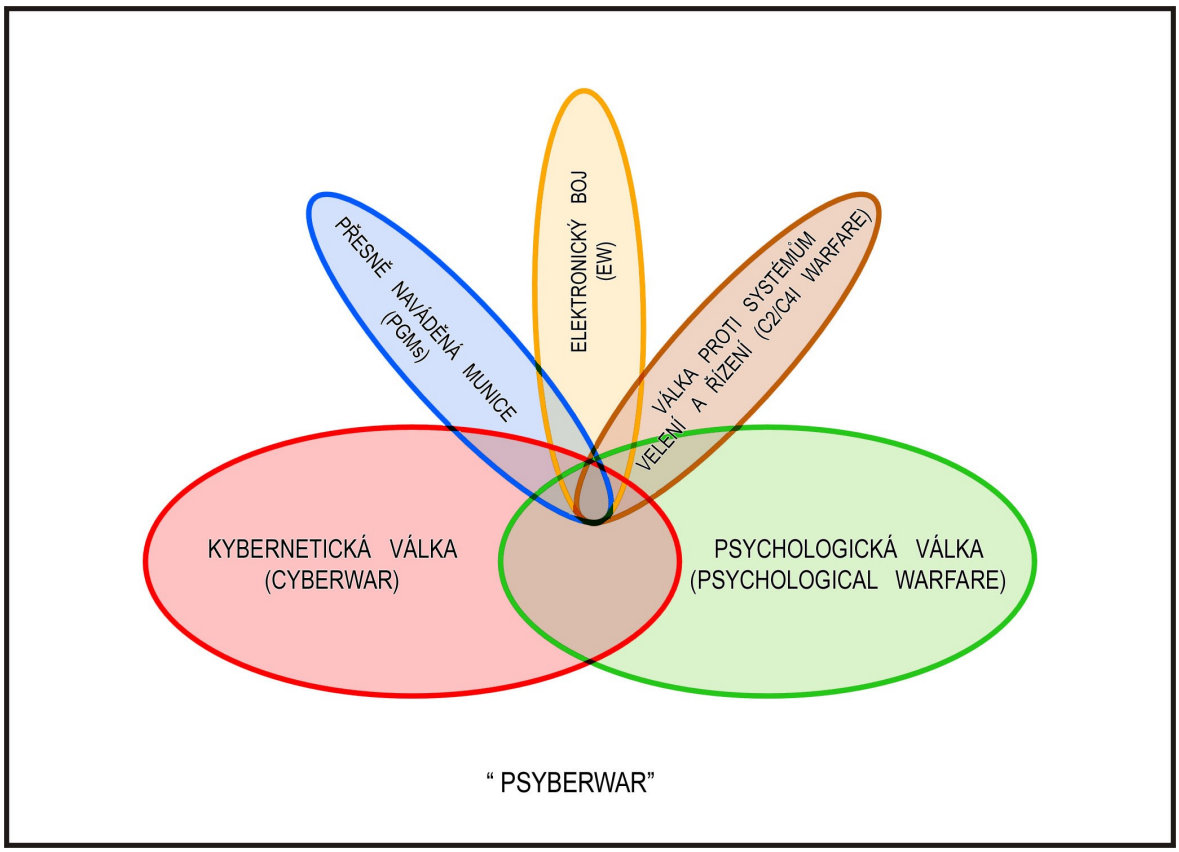
Zástupci ruského generálního štábu definovali informační válku na operačně – strategické úrovni jako „*souhrn speciálně plánovaných a koordinovaných opatření jednotek a zpravodajských služeb, systémů včasného varování, prostředků velení a řízení, spojení, klamání a elektronického boje, jejichž účelem je zajistit dosažení stanovených cílů bojové operace*“. [126] Z definice vyplývá, že informační válka je považována za jeden z podpůrných prvků bojové operace. Možnost samostatného použití informační války k dosažení určitého cíle definice nepřipouští. Rusové však význam informací v žádném případě nepodceňují. Vyplývá to z prohlášení analytika ruského ministerstva obrany Tsymbala, podle něj nebude z vojenského hlediska považována informační válka vedená proti Rusku za nebojovou fázi konfliktu, nehledě na skutečnost zda dojde ke ztrátám na životech či nikoliv. Protože by jednostranné vedení informační války mohlo mít katastrofální dopady na hospodářství, řízení státu, prostředky velení a řízení nebo na vlastní vedení bojové činnosti, ponechává si Rusko právo prvního jaderného úderu proti nepřátelským prostředkům a silám a potom proti protivníkovi samotnému. [126]

Bývalý příslušník finských ozbrojených sil Sakari Ahvenainen vytvořil vlastní definici, podle ní je „*informační válka nepřátelské působení, kterého je dosaženo z více jak 50 procent pomocí informačních prostředků*“. [1] Může být dále umocněna např. účinky konvenčních zbraní nebo ovlivněním elektromagnetického spektra. Jeho definice musí nutně vyvolat pochybnosti. Bylo by velmi obtížné zjistit kdy se informační prostředky podílely na ovlivnění protivníka 51 procenty a kdy méně. Není ani známa metoda, jak by tento účinek bylo možné zjistit. Na rozdíl od zbraňových systémů určených k fyzické likvidaci, kde je možné kvantitativně účinnost zjistit, je použití působení informačních prostředků pravděpodobně jen těžko měřitelné.

Zajímavou definici použil ve své analýze Christopher Bellamy z Royal Military College of Science z Velké Británie. Termín informační válka by, podle něj, mohl být vhodným

označením pro kybernetickou válku, za předpokladu využití informace k likvidaci, poškození nebo využití protivníkovi informace, protivníkových informačních systémů a počítačových sítí. Vystihuje rovněž útoky proti smýšlení velitelů (ovlivnění rozhodování) - tzn. psychologická válka, klamání a zvrat mysli. Informační válku, by šlo v této souvislosti nazvat novým termínem - psychokybernetickou válkou „*psyberwar*“. [9] Kromě těchto dvou oblastí se však informační válka překrývá i s válkou proti systémům velení a řízení, elektronickým bojem a informace jsou samozřejmě klíčové i při nasazení přesně naváděné munice (viz. obr. 7).

Obrázek 7. Psyberwar



Zdroj: Upraveno a převzato z BELLAMY Christopher. What is Information Warfare?

Zvláštní pojetí informační války má Čína, která byla zprvu ovlivněna sovětskou vojenskou vědou a později transformovala na své podmínky americké definice. Pozornost začali čínští odborníci věnovat informační válce v polovině 80. let minulého století, intenzivně se však na ni zaměřili po první válce v Perském zálivu. Po jejím vyhodnocení dospěli totiž k závěru, že Čína by v případě přímé konfrontace se Spojenými státy válku prohrála. [79]

Proto se čínští vojenští odborníci začali zaměřovat na asymetrickou válku, včetně informační války, jako na možné řešení. Její zvládnutí by, podle nich, umožnilo slabšímu (Čína se tradičně sama označuje jako „slabší stát“) porazit silnějšího protivníka. Podle tchaj-wanského odborníka na čínský vojenský vývoj Lin Chonga se Čína zabývá informační válkou tak intenzivně, že by mohla dokonce v brzké době na čele priorit vystřídat jaderné zbraně. [43] Za šest pilířů informační války považuje čínský generální štáb psychologické operace, klamání a maskování, elektronický boj, počítačovou válku, fyzické ničení a operační bezpečnost (počítačových sítí). V tomto duchu i definoval generál Dai informační válku jako „*soubor operací vedených v podmínkách informačního prostředí, jakožto bojiště, s použitím vojenských informací a informačních systémů, které jsou zároveň cílem operačního působení, dále s využitím elektronického boje a počítačové války*“. [125] Nejedná se o jedinou čínskou definici, ani ostatní se však v pojetí informační války příliš neliší.

ZÁVĚR

V řadě zemí v současné době probíhá a v těch nejvyspělejších již pravděpodobně proběhla přeměna průmyslové společnosti ve společnost informační. Tento proces je určován informační a komunikační technikou, jakož i stoupající potřebou komunikace nejen civilních, ale i vojenských institucí. Používáním nových metod a využíváním závislosti i nových možností ovlivňovat lidi a stroje se vytváří situace, která jako tak zvaná informační válka překračuje vojenskou oblast a může být účinně vedena i mimo rámec ozbrojeného střetnutí.

Informační válka představuje rychle se rozvíjející, avšak dosud jen nepřesně definovanou oblast rostoucího zájmu resortu obrany a politických činitelů. V odborné literatuře existuje řada definic tohoto pojmu, shody však dosud dosaženo nebylo. Nemá smysl všechny definice uvádět, ani některé z nich odsuzovat. K objasnění pojmu by to více nepřispělo. Přestože se všechny definice různou mírou liší, shoda existuje, podle Nastoupila, v tom, že informační válka je formou vedení války pomocí informací a informační techniky proti informacím a informační technice. [89]

V posledních letech se informační válkou intenzivně zabývá Čína a pravděpodobně její možnosti až přeceňuje. Čínští odborníci dokonce předpokládají, že konflikty brzké budoucnosti ovládne informační válka a určí i jejich rozsah a intenzitu. Čína prohlašuje, že si je vědoma tohoto trendu a proto je prý zvládnutí informační války určujícím faktorem čínských vojenských kapacit a bojové připravenosti. [6] Některé její definice zmiňují také důležitou roli lidí (lidského faktoru)[7] a čínské studie zdůrazňují nutnost vychovat mladé schopné lidi, vhodné pro informační válku – informační odborníky. Tím se odlišují od ostatních pojetí a definic. [43]

[7] Zdůrazňování lidí vyplývá, podle západních vojenských odborníků, z tradiční vojenské doktríny tzv. lidové války ještě z dob Mao Ce-tunga.

. KLAMÁNÍ A DEZINFORMACE

ÚVOD

Každá vojenská síla, ať má, podle Nastoupila, jakoukoli převahu a bojové kapacity, nebude–li používat lstí a klamání, riskuje neúspěch. [90] Klamání zahrnuje, pokračuje Nastoupil, plánovaná opatření pro poskytování pravdivých nebo falešných informací, tedy dezinformací, týkajících se strategických plánů, síly vojsk, sestavy, operací nebo taktiky, což vede protivníka k nesprávnému hodnocení, a proto k nesprávnému jednání. Tím lze dosáhnout překvapení v čase, prostoru, způsobu či intenzitě boje a využít ho k dosažení vítězství. Umění využít lstí a klamání k vítězství není považováno ve válce za nemorální, naopak bylo vždy z vojenského hlediska vysoce ceněno. Již Sun Tzu[8] považoval vítězství dosažené lstí za vítězství nejcennější - první třídy, vítězství dosažené prostřednictvím diplomacie řadil do druhé třídy a vítězství dosažené použitím síly cenil pouze jako vítězství třetí třídy. [118]

PRINCIP KLAMÁNÍ

Klamání je proces uplatnění triků nebo podvodu a lze ho považovat, podle Gerwehra a Glenna zčásti za umění a zčásti za vědu. [47] Obecně se jím rozumí přimět někoho věřit něčemu co není pravda; zmást někoho nebo vlákat do léčky. Teorie klamání „*Deception*“ vychází z analýzy dvou hlavních, ale zcela odlišných oblastí, kde se tato činnost využívá. Jedná se o magii (kouzla) a vedení války. Zatímco pod pojmem magie se rozumí předvádění triků zpravidla pro pobavení obecenstva, klamání je záměrná činnost na oklamání protivníka. Podle americké doktríny je vojenské klamání definováno jako „*záměrně prováděné operace s cílem donutit protivníkovo velení ke špatnému rozhodnutí, které bude však bude příznivé pro vlastní jednotky, záměry a operace; činnost kterou povede protivník tak přispěje k úspěšnému splnění stanoveného cíle*“. [83] Magie ani klamání však nejsou zázrakem, ani nadpřirozenou mocí, ale aplikovanou psychologií, psychologií špatného pochopení vstupní informace. Je to tedy, jak zdůrazňuje Barton Whaley, psychologický jev. [141] Všechny procesy klamání se totiž odehrávají v lidském

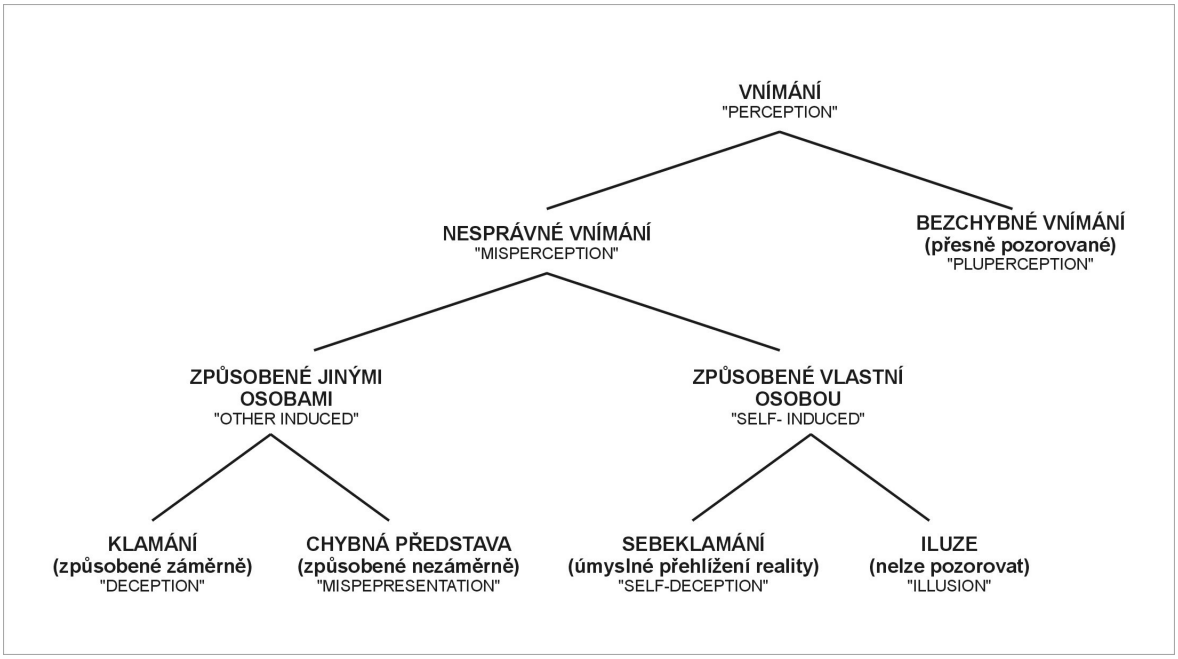
[8] Sun Tzu – starověký čínský stratég a vojenský teoretik, podrobněji je představen v kapitole o historických informačních operacích.

vědomí, ne v reálném fyzickém světě. Od tohoto faktu se odvíjí i úspěšnost magie či klamání. Splnění cíle jedné válčící strany, jenž se snaží přimět druhou ke špatnému výkladu reality (produkuje proto nepravdivý obraz reality) bude záležet na tom, jestli vůbec druhá strana nepravdivý obraz, tj. záměrně zkreslenou informaci přijme.

Proces vnímání

Ke správnému pochopení procesu vnímání[9] okolní reality, správného nebo nesprávného je nejprve vhodné sestavit typologii vnímání (viz. obr. 8). Z ní je zřejmé, že klamání je jednou z forem vnímání a lze ho nazvat jako nesprávné vnímání[10].

Obrázek 8. Typologie vnímání



Zdroj: Upraveno a převzato z WHALEY Barton. Toward a General Theory of Deception.

Pokusy vysvětlit proces, jak se dostane informace do lidského vědomí, se objevily již v minulosti. Vnímáním reality se zabýval např. v 18. století pruský filozof Immanuel Kant ve své teorii poznání. V roce 1970 přišel britský neuropsycholog Gregory s názorem, že procesy vnímání jsou hypotézy. [141] Dospěl k němu na základě důkazů získaných

[9] Jde o autorův překlad anglického termínu „perception“.
[10] V anglickém originálu „misperception“; autor pro účely této práce zvolil překlad „nesprávné vnímání“. Lze ho vykládat i jako „nesprávné pochopení“.

z výzkumů z oblasti neurologie, psychologie a filozofie. Proces vnímání se, podle něj, skládá z několika fází:

1. Okolní prostředí nepřetržitě vysílá doslova chaotický proud signálů, či široké spektrum nespojitých dat (bitů informací).
2. Lidské smysly, jako např. oči, uši – zrak a sluch, jsou schopny část těchto signálů (informací) zachytit.
3. Takto přijaté bity a útržky informací jsou předávány do lidského vědomí – do mozku.
4. Většinu dat lidský mozek vyřadí, ale některá zpracuje a uloží do paměti.
5. Mozek vytvoří hypotézu o okolním prostředí dedukcí z nově přijatých dat i z dat uložených v paměti.

Proces vytvoření hypotézy je tedy závislý na uložených datech, které jsou na základě podobných charakteristik a souvislostí seskupeny do určitých souborů a na nově přijímaných datech. Ta jsou porovnávána s jednotlivými soubory dat a poté vnímána jako vhodná, či shodná, nebo jako nevhodná (nepoužitelná). Právě tato spojování dat (informací) a vyřazování dat vede k vytvoření hypotézy o okolí. V souvislosti tímto procesem vnímání a chápání, jak uvádí Whaley, lze vysvětlit i proces nesprávného vnímání. Nesprávná hypotéza totiž může vzniknout ve dvou případech. Za prvé, vstupní senzory, tj. lidské smysly nepracují správně; nebo za druhé, je chybná lidská kognitivní strategie vytvářející hypotézu o obrazu okolí. V prvním případu jde o fyziologickou poruchu, ve druhém o psychologickou. [141] V této souvislosti je nutné zdůraznit, že schopnost správně vnímat, v tomto smyslu myšleno „přesně pochopit“, je výzvou dokonce i za příznivých okolností. Vzájemná komunikace i při nerušném spojení může být špatně srozumitelná a význam přenesených informací nejasný (např. při zanedbání zásad spojení). V takové situaci, i za předpokladu správné funkce smyslů a kognitivní strategie, bude výsledek – vytvořená hypotéza značně nejistá. [47]

Podstata klamání

Klamání je zkreslení či deformace reality. Provádí se záměrným pozměněním charakteristických rysů předmětů, které vnímají lidské smysly, jako např. tvaru, velikosti,

barvy apod. Cílem je, jak již bylo řečeno předložit klamný obraz reality a zmást tak druhé osoby. Mistři magie tuto činnost nazývají kouzlem, trikem nebo iluzí. Z hlediska vojenství se nazývá klamáním, někdy také zastíráním nebo krytím. Někteří vojenští teoretici dokonce používají, jak zdůrazňuje Urbanovský, ne příliš jasný termín „strategické maskování“. [128] Klamání je zpravidla výsledek záměrné lidské činnosti, může však za ním stát i sama příroda. Případy přirozeného klamání (zcela nezávislé na lidech) vznikají v přírodě buď bez jakéhokoliv účelu, nebo za specifickým účelem. V prvním případě jde o fyzikální jevy, jako např. fata morgána nebo zdánlivé zalomení tyče ve vodě. Ve druhém případě jde o výsledek evolučního procesu živočichů. Ty příroda obdařila takovými vlastnostmi, že vysílají do svého okolí klamné informace (zelená kůže splývá s porostem džungle a vyvolává dojem – vysílá informaci - jakoby se jednalo o list) a tak jsou buď schopni přežít útok predátorů, nebo jsou naopak schopni se nepozorovaně přiblížit ke kořisti a živit se jako predátoři. [47] V obou případech jde o vlastnosti, které jim umožňují přežít. Rozdíl mezi člověkem a přírodou je v tom, že člověk sice provádí někdy klamnou činnost nevědomě (oklame sám sebe, nebo neúmyslně i ostatní), ale zpravidla klame vědomě s cílem získání výhody nad ostatními. Podle Whaleyho však „*příroda klame vždy nevědomě*“ [141] (nezáměrně).

Možné způsoby klamání

Každá činnost mající za následek klamání, ať se již jedná o přirozené působení přírody nebo záměrnou operaci vojenských jednotek, se skládá ze dvou hlavních částí. Jsou to disimulace a simulace. [141] Disimulace je záměrné zastírání skutečného stavu. Cílem je utajit pravdu (informace) o skutečnosti nebo alespoň znesnadnit její rozpoznání (způsobit co největší nesrozumitelnost informací). V praxi to znamená zakrýt jednu nebo ЪЈЬÿ význačných charakterových vlastností ukrývaného předmětu, které je jednoznačně odlišují od jiných předmětů; např. skrytí některých součástí raketového kompletu. Právě získání informací o nich může být klíčovým faktorem pro vyhodnocení bojových kapacit protivníka. Mistři magie hovoří v tomto případě o metodě, o způsobu nebo postupu, jakým trik provedli, a kterým oklamali obecenstvo. Ve vojenství se tento způsob nazývá utajování, ukrývání a někdy i negativní maskování.

Druhá část, simulace je předstírání, tzn. záměrné zviditelňování, avšak nesprávného obrazu reality. Cílem je vnutit protivníkovi nesprávné informace, donutit ho, aby nabyl dojmu, že získal všechny potřebné informace k zahájení vlastní operace. Jedná se např. o rozmístění maket bojové techniky, simulování rádiového provozu, koncentrace jednotek na jiném (nesprávném) místě, než bude vedena operace. Získání a hlavně vyhodnocení takové informace jako pravdivé může mít v průběhu vedení bojové činnosti, podle Whaleyho, fatální následky. [141]

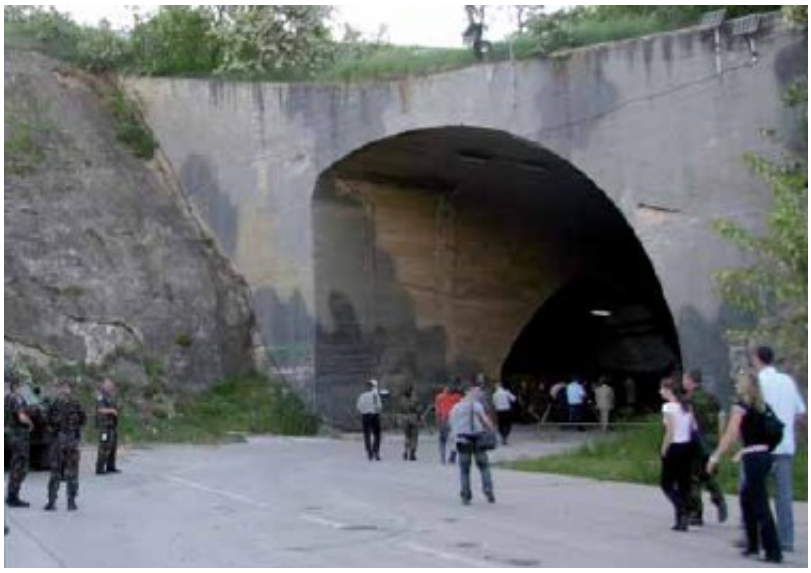
Formy disimulace

V zásadě lze rozlišit tři základní formy disimulace, nebo také pasivního způsobu klamání, jak jí nazývá Nastoupil [55]. Jedná se o ukrytí „*hide*“ pomocí maskování „*masking*“; změna vnějšího vzhledu přestrojením „*repacking*“ a vizuální zmatení „*dazzling*“. [141] Tyto způsoby spočívají primárně v utajení a maskování ke skrytí našich záměrů a možností, tzn. zatajit informace tak, aby jich protivník získal co nejméně.

Cílem maskování je v ideálním případě dosáhnout „neviditelnosti“. Provádí se skrytím všech komponentů, které by mohly prozradit rozmístění jednotek a techniky, např. do umělých nebo přírodních úkrytů. Druhou možností je imitace, tzn. přizpůsobení vnějšího vzhledu okolnímu prostředí. Mistři magie používají při předvádění triků v tomto případě ukrývaní za pódium, zrcadla, stůl a další předměty, nebo dokonce ukrývají „vykouzlenou věc“ v ruce. Ve vojenství se využívá různých prostředků maskování a krytí. Srbské vojenské letectvo např. využívalo během zásahu NATO v roce 1999 upravené skalní jeskyně, které sloužily jako letecké hangáry[11] (viz. obr. 9). [75] Běžně se používá kouřová clona, elektronické rušení pozorovacích prostředků protivníka a samozřejmě různé techniky maskování, včetně maskovacích sítí a nátěrů.

[11] Vstupní prostor do hangárů měl tvar písmene „S“, aby technika uvnitř byla maximálně chráněná před poškozením i v případě zásahu hangáru. Tento tvar měl nejen zabránit proniknutí střepin do nitra, ale i tlumit případnou tlakovou vlnu způsobenou explozí v těsné blízkosti vstupní brány. V principu se nejednalo o žádnou novinku, jejich konstrukce však byla velice důmyslná a technicky zdařilá.

Obrázek 9. "Skalní letiště"



Zdroj: Letiště s hangáry ve skále. *A-report*.

Ke změně vnějšího vzhledu se používá přestrojení. Tím se v tomto případě rozumí změna vnějšího obalu. Toho lze docílit konstrukčními úpravami nebo deformačními nátěry. Mistři magie mají k tomuto účelu různé kostýmy a převleky. Ve vojenství lze tuto taktiku využít ke zmatení protivníka, který nesprávně vyhodnotí informace, např. o použité technice. Ta díky vnějším úpravám může na první pohled připomínat známou, běžně využívanou, o které je mnoho informací samozřejmě k dispozici. Ve skutečnosti se však bude jednat o utajenou, „pod starým kabátem“ ukrytou nově vyvinutou zbraň, která zcela změní poměr sil na bojišti. [141]

Vizuální zmatení vysvětluje Whaley jako „*vyvedení protivníka z míry; ten je doslova ohromen, zmaten a popleten tak, že není schopen s jistotou vyhodnotit informace o reálném světě*“. [141] Provádí se různými technickými úpravami velikosti nebo barvy techniky, předstíráním jiné činnosti, jako např. jiného druhu bojové činnosti nebo času zahájení operace. Historickým příkladem je simulace Pattonovy armády rádiovými prostředky jednotek generála Bradleyho po vylodění v Normandii. Tím získali Němci zcela rozdílné informace o poloze (předstírané) Pattona než měli a než předpokládali. Rovněž všechny kódy a šifry způsobující nečitelnost informací a tím jejich utajení lze považovat za tuto formu disimulace.

Formy simulace

V případě použití simulačních technik se obvykle používá imitování, napodobování jiných věcí „*mimicking*“; dále výmyslů „*inventing*“ a nástrah nebo léček „*decoying*“. V prvním případě se jedná o zviditelnění věrohodných napodobenin (replik). Tento způsob použil v roce 1914 generál von Emmich při útoku na belgickou pevnost v Liége s pouhými šesti brigádami (přibližně 20 tis. osob). Jeho jednotky použily stejnokroje pěti různých sborů, Belgičané navíc získali klamné informace od uprchlých zajatců, které Emmichovy zpravodajští důstojníci přesvědčili o armádě o 150 tis. vojácích. Dalším příkladem je dvojník generála Montgomeryho v roce 1944, který oficiálně navštívil britského guvernéra Gibraltaru. [85] Německé zpravodajské služby tak získaly nesprávné informace o jeho činnosti, neboť skutečný Montgomery se podílel na přípravách k vylodění v Normandii.

Používání výmyslů – klamných objektů je podobné předcházejícímu způsobu, ale na rozdíl od něj (imituje věci existující), cíle této simulace je předstírat něco, co ve skutečnosti vůbec neexistuje. Používají k tomu makety různých předmětů a využívají je mistři magie i vojenští odborníci. Jedná se, v případě vojenství, o gumové tanky, dřevěněné kanóny, letouny z látky apod. Za tuto formu simulace lze považovat i klamné rádiové vysílání v místech, kde ve skutečnosti žádná jednotka není. Tyto techniky využili spojenci při přípravě vylodění v Normandii [123] a rovněž Srbové při alianční vojenské operaci v Kosovu. To potvrzuje skutečnost že jednoduchým a laciným způsobem lze oklamat i pokročilé informační technologie. Dřevěná děla byla totiž považována za skutečné zbraně. Vstupní data (informace) přijatá průzkumnými senzory totiž chybně vyhodnotila analytická zařízení a mylně na ně navedla bojové letouny.

Poslední formou simulace je nástraha nebo léčka. Jejím cílem je odvrátit nebo odlákat pozornost protivníka od připravované, nebo již probíhající informace. [141] Tedy zaměřit jeho akvizici informací jinam, než by skutečně měl. Tuto formu představuje jakýkoli klamný útok vedený z odlišného směru, než je veden skutečný úder. Byla a je používána po celou dobu historie vojenských operací. Příkladem je operace Inchon generála MacArthura z Korejské války, kdy se námořní pěchota vylodila na jiném místě, než byl simulován námořní útok na pevninu. [123]

PODSTATA A FORMY DEZINFORMACE

V situacích, kdy diplomatické prostředky nemají naději na úspěch a vojenská operace by byla příliš radikální, používají se jiné možnosti, včetně utajených zpravodajských operací, jejichž součástí jsou zpravidla také dezinformace. Kučerová charakterizuje dezinformaci ve *Výkladovém slovníku informační vědy a knihovnictví* jako „*záměrně nepravdivou (falešnou, lživou, nesprávnou, zkreslenou) informaci sdělovanou s cílem uvést v omyl a ovlivnit příjemce tím, že ji bude považovat za pravdivou a důvěryhodnou*“. [106] Dále rozlišuje dezinformace pasivní (zatajení, zadržení, zpoždění informace) a aktivní (tvorba nepravdivé informace, modifikace původní informace či jejího kontextu). V obou případech se jedná, zdůrazňuje Zadražilová, o akt přímo závislý na svém původci, v žádném případě nejde o nevědomé ponechání někoho v omylu. [145]

Podobně jako výkladový slovník vysvětluje termín dezinformace i *Encyklopedie špionáže*: „*dezinformace je účelová (klamná) informace, která cíleně směřuje k ovlivnění určité skupiny lidí nebo celé populace*“. [39] Ve zpravodajské práci jde o jednu ze základních operativních metod, která slouží k ovlivnění činnosti protivníka tak, aby se choval ve prospěch zpravodajské služby, uvádí dále encyklopedie. Podle povahy plánů a záměrů lze rozlišit dezinformace strategické (dlouhodobé) a operativní, které se vytvářejí na základě aktuální situace.

Z hlediska vojenského definuje dezinformace americký předpis FM 3-13 pro informační operace jako „*informace rozšiřované zejména zpravodajskými službami nebo jinými tajnými službami s cílem zkreslit realitu, oklamat nebo ovlivnit nejvyšší představitele Spojených států, americké ozbrojené síly, koaliční partnery, klíčové politiky nebo jednotlivce pomocí nepřímých nebo nekonvenčních prostředků“*. [60] Dezinformace je forma propagandy, dále pokračuje předpis, která je namířena na vedoucí představitele s rozhodovací pravomocí a jejím cílem je zmást je, aby přijali nesprávná rozhodnutí. Na taktické úrovni může dezinformace zmást velitele a způsobit plýtvání silami a prostředky na ochranu proti neexistujícím hrozbám. Může rovněž negativně ovlivnit existenci koalice záměrným oživováním historicky etnických, rasových a kulturních předsudků u jednotlivých členů koalice. Dezinformace šíří protivník zpravidla nepřímo, prostřednictvím vysílacích prostředků třetí strany (nezúčastněných států nebo organizací),

ale může využívat i nekonvenčních způsobů, mj. poznámky na předmětech běžného použití jako např. krabičky od sirek, nebo na věcných darech.

Nejpodrobněji se však věnuje dezinformacím a propagandě Ladislav Bittman; dezinformaci definuje jako „*úmyslně zkreslenou informaci, kterou pachatel tajně vsune do informační soustavy oponenta s cílem oklamat ho a ovlivnit jeho politické, hospodářské či vojenské akce*“. [11] Termín dezinformace je, uvádí Bittman, německého původu a Německo bylo také první zemí, která v době první světové války založila dezinformační odbor, jehož úkolem bylo systematicky klamat. V dějinách nejsou dezinformace spolu s operacemi strategického klamání a černou propagandou ničím novým. Masovou produkci dezinformací však přinesla do oblasti mezinárodních vztahů, podle Bittmana, až studená válka. Bittman rozlišuje dezinformace, podobně jako americké vojenské předpisy, na dva základní druhy. Jednak jsou to dezinformace propagandistické, v podstatě tzv. černá propaganda, jejichž úkolem je oklamat a ovlivnit veřejné mínění. Jejich úspěch je závislý na slabinách a omylech protivníkovi politiky a na předsudcích veřejného mínění. Dalším druhem dezinformací jsou tajné operace, které mají oklamat nebo ovlivnit vládní představitele protivníka nebo jeho politickou, hospodářskou či vojenskou elitu. V tomto případě není dezinformační kanálem tisk (tento typ dezinformací se publicitě vyhýbá), ale tajný nebo anonymní kanál, např. agent nebo anonymní dopis.

Propaganda

Cílem propagandy je, zdůrazňuje Bittman, záměrná snaha ovlivnit široké publikum informacemi bez ohledu na to, jsou-li pravdivé, či zkreslené nebo falešné (klamné). Propagandu lze definovat jako „*úmyslný pokus jednotlivce či skupiny formovat, kontrolovat či měnit názory jiných společenských skupin pomocí komunikačních kanálů a prostředků tak, aby výsledek byl v souladu se zájmy propagandisty*“. [11] Z této definice je zřejmé, že se jedná o jeden z možných způsobů psychologické manipulace s cílovou skupinou populace, nebo s jednotlivci. V současné době je technika propagandy natolik vyspělá, že většina lidí si často neuvědomuje, že je obětí cílevědomé manipulace. V případě, že je propaganda jako jedna z možných technik využita při vedení psychologické války, není ani žádoucí, aby cílová skupina zjistila, že je manipulována. V takovém případě by mohla být dokonce kontraproduktivní a pokud by se jednalo

o mírovou misi, civilní obyvatelstvo by pravděpodobně ztratilo důvěru k mírovým jednotkám a začalo by se chovat nepřátelsky. V souvislosti se zdrojem a pravdivostí obsahu se propaganda obvykle dělí do tří hlavních kategorií: bílé, černé a šedé. [11]

Bílou propagandu vytváří a rozšiřuje zdroj (organizace, stát, agentura), který nezakrývá svoji totožnost. [32] Sovětský svaz např. rozšiřoval, uvádí Bittman, v době studené války ve Spojených státech prostřednictvím firmy Imported Publications sídlící v Chicagu široký sortiment propagandistických materiálů. Typickou ukázkou bílé propagandy je rozhlasové vysílání pro zahraniční posluchače. Masového rozmachu se dočkala po druhé světové válce a mezi nejznámější patřily/patří stanice Hlas Ameriky, Rádio Svoboda/Svobodná Evropa, Radio Moskva nebo BBC.

Černá propaganda je propagandistická dezinformace, která má nejen ovlivnit, ale také oklamat širokou veřejnost, zdůrazňuje Bittman. [11] Pochází z jiného zdroje, než se prezentuje na veřejnosti (vyrábí se pod cizí vlajkou). [32] Cílem skutečného pachatele je zůstat v utajení, mj. proto, aby nebyla ohrožena jeho pověst. Černá propaganda je velkou lží, uvádí dále Bittman, jejími nejčastějšími producenty jsou zpravodajské služby, polotajné politické spolky a teroristické skupiny. Patří do ní zejména padělky vládních dokumentů s kompromitujícím obsahem, šíření nepravdivých zpráv tzv. „šeptandou“, podsouvání falešných zpráv tisku, publikování článků a knih pod cizím jménem a rovněž rozšiřování klamných zpráv mezinárodní počítačovou sítí.

Šedá propaganda je operací, podle Bittmana, která obsahuje prvky bílé i černé propagandy. [11] Americký slovník vojenských pojmů *Department of Defense Dictionary of Military and Associated Terms* [91] i *Terminologický slovník NATO* [91] uvádějí, že se jedná o propagandu, která neuvádí svůj zdroj. Taková definice však není příliš srozumitelná. Přesněji vysvětluje šedou propagandu přece jen Bittman. Propagandistický zdroj může, pokračuje Bittman, ale nemusí být správně identifikován, pravdivost informací je vždy nejistá. Do této kategorie patří např. zkreslování statistických informací ve výročních zprávách různých společností nebo inzeráty a sliby (nereálné) nejrůznějších pseudonáboženských hlasatelů.

Zvláštní kategorií je tzv. propaganda činem. Patří do ní, uvádí Bittman, fyzické akty, vládní rozhodnutí nebo vojenské manévry. Jako příklad lze uvést vzdušný úder amerického

a britského vojenského letectva na Berlín v lednu 1943, přesně načasovaný na okamžik, kdy Göring přednášel oslavný projev k desetiletému výročí zrodu nacistického režimu. Záměrem spojenců byla propagandistická demonstrace síly s cílem ovlivnit alespoň část německého obyvatelstva a podlomit jeho oddanost nacistickému režimu a odhodlání pokračovat ve válce. [11]

Metody a techniky dezinformace

Jednou z metod šíření dezinformací je využití tisku. V demokratických zemích je tisk nejen komunikačním kanálem, rovněž však i jako politický faktor ovlivňuje prostřednictvím zpravodajství a komentáři veřejné mínění a státní aparát. Z tohoto důvodu, uvádí Bittman, je častým terčem domácích i mezinárodních intrik, propagandistických kampaní a dezinformačních operací. Jejich cílem je ovlivnit novináře a následně oklamat veřejnost, parlament a vládní orgány. Jedním z důvodů, proč profesionální dezinformátoři v mezinárodních vztazích mnohdy uspějí, vysvětluje Bittman, je nedostatek vysoce kvalifikovaných korespondentů. V době studené války mělo dokonce každé komunistické i západní velvyslanectví k dispozici finanční prostředky na ovlivňování místního tisku. Novinář, který byl ochoten napsat pozitivní článek, byl odměněn. Tento fond využívaly i zpravodajské služby, zejména ke kompromitaci novinářů a na zabezpečení utajených dezinformačních kampaní.

Často používanou formou dezinformačních operací jsou padělky. Mají nejrůznější podobu, jako např. dokumenty vládních institucí protivníka, osobní spisy nebo dokumenty významných osobností, letáky a inzeráty skutečných nebo neexistujících organizací, výtisky novin, padělané bankovky nebo padělky autorských rukopisů. Podle Bittmana lze rozdělit padělky na tři kategorie. Do první patří padělky vyrobené za účelem zisku, jedná se tedy o kriminální činy. Padělky, které mají oklamat politické, hospodářské nebo vojenské činitele protivníka patří do druhé kategorie. Pokud nejsou odhaleny, měly by způsobit rozhodnutí, které je v souladu se zájmy pachatele. Třetí kategorií jsou propagandistické padělky usilující o širokou publicitu. Podsouvání padělků západních vládních dokumentů byla velmi populární metoda komunistických rozvědek zejména v padesátých a šedesátých letech minulého století, doplňuje Bittman. [11]

Dobře známou metodou šíření dezinformací je rozhlasové vysílání do zahraničí. Velkého významu nabyla během druhé světové války. Více než sto rozhlasových stanic se zaměřovalo na protivníkovy posluchače a zejména na vojáky. Šířily do éteru propagandistická hesla, zprávy a dezinformace s cílem podlomit jejich bojovou morálku. Ve vysílání nechyběly např. ani zprávy o nepřístojném chování manželek a přítelkyň. Jako první začalo používat metodu černé rozhlasové propagandy Německo, ne však úspěšně, protože obsah vysílání byl zjevně proněmecký. Mnohem větších úspěchů dosáhli Britové a rovněž americká zpravodajská služba Office of Strategic Services (OSS)[12]. [11]

K propagandistickým účelům je možné využít, podle Bittmana, rovněž filmového média. Již v minulosti se o to pokoušelo mnoho vlád a organizací, ale často, pokračuje Bittman, bez velkého úspěchu. [11] Podle Taylora však kino během druhé světové války plnilo roli velmi důležitého média k rozšiřování propagandy. Důležitým předpokladem úspěšnosti však byla i přitažlivost pro diváka z hlediska zábavy. Orientovala se výhradně na domácí publikum, využitelnost tedy byla jen v zázemí, ale významně přispívala k vlastenectví a k posílení protinacistických nálad. [123]

Dobře zneužitelné komunikační médium k dezinformačním účelům je fotografie. Tvrzení že „fotografie hodnotu tisíce slov“, a „že kamera nikdy nelže“ jsou naprosto klamná tvrzení, uvádí Bittman. V současné době mají pachatelé k dispozici řadu technik, počínaje „režií“ snímku tak, aby podporovala autorův záměr, a končíce fotografiemi, které jsou „vylepšeny“ počítačovou technikou, zdůrazňuje Bittman. Komunistické režimy běžně používaly metodu vymazávání „nežádoucích“ osob z veřejně dostupných fotografií, jako např. Trockij nebo Dubček. Avšak i v demokratických státech se používá „diskrétní“ naaranžování, jako v případě bývalého amerického prezidenta Roosevelta. [11]

Možnou technikou využitelnou k šíření dezinformace jsou i pověsti a tzv. šeptandy. Pověstí se rozumí neprověřená zpráva, která se může potvrdit, nebo ukázat jako zcela nevěrohodná. Pokud se šíří ústní komunikací, hovoří Bittman o šeptandě. V současné době elektronických komunikací šíří neprověřené informace masová média, což ještě znásobuje jejich vliv na veřejné mínění. Pověsti se mohou vynořovat spontánně, ale mohou být

[12] OSS byla předchůdkyně americké Ústřední zpravodajské služby (CIA), během války zřídila dvanáct rozhlasových stanic, které předstíraly, že jsou německé.

i výtvorem zákulisních manipulátorů. Techniku rozšiřování klamných pověstí používaly s oblibou zpravodajské služby bývalého sovětského bloku. [11]

Zcela odlišnou technikou, ve srovnání s předešlými, jsou tajné operace. Provádějí je především civilní a vojenské zpravodajské služby. K paralyzování nebo alespoň oslabení protivníka využívají zvláštní prostředky. Pokud jsou dobře naplánovány, jejich účinek může být pro protivníka téměř zničující. Příkladem je izraelská operace „Láhev“ ze šedesátých let minulého století. Izraelským příslušníkům speciálních jednotek se podařilo vybudovat síť překupníků, která dodávala egyptským jednotkám množství marihuany s cílem podlomit jejich bojovou připravenost. Získané finanční prostředky navíc sloužily k financování jiných operací. [11]

Dezinformační kampaně vedou rovněž krycí organizace. Ty se v kontextu mezinárodní propagandy a dezinformací označují jako organizace mezinárodního charakteru (charitativní, humanitární, atd.). Předstírají ideologickou, politickou a finanční nezávislost, ve skutečnosti jsou však řízeny a finančně podporovány vládou nebo organizací, které slouží. [11] V současné době působí např. v západní Evropě a na Balkáně řada organizací, které jsou údajně nezávislé, existuje však podezření, že některé z nich jsou řízeny a podporovány ze zemí Blízkého a středního východu nebo mají dokonce napojení na al-Káidu. [26]

Nejnovějším prostředkem k šíření dezinformací a propagandy je celosvětová síť internet. V souvislosti s dostupností, rozšířeností a oblíbeností je zcela exkluzivní a využitelná pro jednotlivce, organizace, orgány státní správy i koalice. Její využití je finančně nenáročné, což velmi rychle zjistily zejména teroristické skupiny, které ji využívají ve stále větší míře. Podrobně je však tato problematika analyzována v kapitole zabývající se informačními operacemi proti teroristickým skupinám.

ZÁVĚR

Termínem klamání, je nazýván souhrn opatření, jejichž cílem je vnutit nepříteli mylnou představu (informaci) o situaci a činnosti vlastních vojsk a jejich objektech. Jsou to klamné akce, demonstrační činnost, poutání nepřítele, odvádění pozornosti, zřizování klamných

objektů, šíření klamných zpráv apod. Přestože není klamání považováno vojenskými odborníky za formu informační války, lze ho z hlediska informačního pokládat za aplikaci informační války přímo v prostoru bojiště. Jedná se totiž o záměrné ovlivňování procesu přijetí a vyhodnocení informace, tedy o způsob předkládání nesprávných informací protivníkovi tak, aby byly pokládány za pravdivé. Klamání lze provádět v zásadě dvěma způsoby, či metodami. Jsou to buď metody pasivní - disimulace, které spočívají primárně v utajení a maskování ke skrytí záměrů a možností. Mají zabránit protivníkovi získat informace, nebo alespoň množství dostupných informací maximálně zredukovat. Druhým způsobem je aktivní klamání, které zpravidla zahrnuje, jak zdůrazňuje Nastoupil, „*promyšlenou snahu o prozrazení polopravd podporovaných vhodnými důkazy, signály anebo jinými materiálními důkazy*“. [89] Nutnou podmínkou pro provedení klamání je jeho naplánování, včetně volby správné formy. Je naprosto nezbytné nejprve vyhodnotit kapacity a možnou reakci protivníka. Nutností je, aby předloženou klamnou informaci přijal jako pravdivou a přitom nepojal podezření. V případech, kdy se tento záměr nezdaří a protivník zjistí, že jde o fikci, stává se strana, která vedla původně klamání stranou oklamanou. Z informačního hlediska jde o odhalení nepravdivé informace (tedy o správné vyhodnocení vstupní informace), z hlediska vojenského o ztrátu převahy na bojišti. Odhalení klamání se nazývá protiopatření proti klamání, nebo – li „*counterdeception*“. [141]

Nedílnou součástí válečných operací jsou, jak upozorňuje Bittman, propaganda a dezinformace. Byly využívány po staletí, masivně je však válčící strany začaly využívat až během druhé světové války. Od té doby jejich význam nepoklesl, naopak se v důsledku rychlého rozvoje masových médií neustále zvyšuje. V moderní válce usilují válčící strany o dosažení vítězství nejen vojenskými prostředky a nástrahami, ale také utajeným i veřejným ovlivňováním vlastního i nepřátelského veřejného mínění. Propaganda je v podstatě forma psychologické manipulace bez ohledu na to, zda jsou iniciátorem komunisté, nacisté nebo demokratické instituce, uvádí Bittman. [11] Není to ideologie, pokračuje Bittman, ale nástroj ovlivňování, který je k dispozici politickým, náboženským nebo jakýmkoli jiným společenským organizacím všeho druhu, včetně teroristických skupin nebo nacistických spolků. Dezinformace lze přirovnat, podle Bittmana, k rakovinovým buňkám, které imunologický systém v lidském těle nedokáže rozeznat od zdravých buněk. Některé z nich mají za úkol oklamat protivníka a přinutit ho k rychlé reakci, jiné jsou naopak součástí dlouhodobých operací, mají kumulativní efekt, který se

projeví za relativně delší období. Nejsnadnějšími oběťmi dezinformací bývají osoby s vyhraněnými levicovými, pravicovými, nacionalistickými nebo náboženskými radikálními názory a předsudky. Když jsou produkty dezinformační kampaně v souladu s jejich přesvědčením, jsou často ochotni uvěřit, podle Bittmana, i bizarním obviněním a konspiračním teoriím.

S dezinformacemi se lze setkat, podle vydavatele internetového serveru Česká média Jaroslava Berky, rovněž v oboru Competitive Intelligence. [101] Boj s informacemi (jehož součástí jsou i dezinformace) je, podle něj, jednou ze součástí konkurenční strategie. Platí pro ně však určitá omezení dodává Berka, nesmí být právně napadnutelné. Vzápětí však charakterizuje dezinformaci jako záměrnou lež. Jeho výklad není příliš jasný, avšak každé záměrné šíření lží, přestože se jedná o konkurenční prostředí je nezákonné. V této souvislosti se autor domnívá, praktiky tohoto typu patří do jiné sféry než je konkurenční zpravodajství. Naopak v mezinárodních vztazích, zpravodajských operacích a psychologických válkách je z pochopitelných důvodů dezinformace akceptovanou taktikou kdekoli na světě.

. TYPOLOGIE INFORMAČNÍCH OPERACÍ

ÚVOD

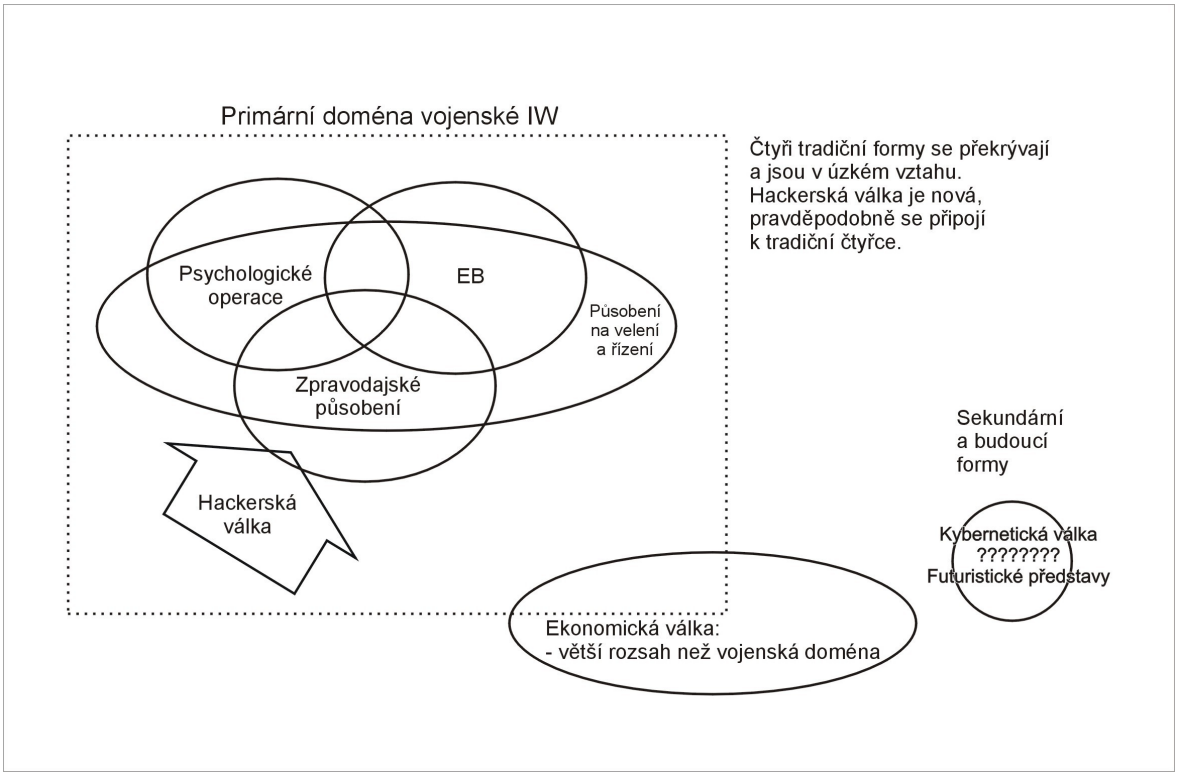
V posledních letech se v souvislosti s taktikou velmocí opouštět tvrdé techniky vedení bojů (s ohledem na případné ztráty v řadách vojáků nebo civilního obyvatelstva) začal přesouvat důraz na takzvané měkké formy války. „*Proto došlo k masivnímu rozvoji jednotlivých forem vedení informační války*“, uvádí Hodický. [52] Informační válku, tj. informační operace je možné vést letálními nebo neletálními prostředky, hrubou silou či nesmrtícími prostředky. Dále je lze členit na obranné nebo útočné – podle toho, zda je cílem informace ochraňovat vlastní síly a prostředky, nebo působit na protivníka. Takové rozdělení je však velmi hrubé, protože odpovídá pouze základnímu rozdělení bojové činnosti na obranu a útok.

Informační válka jako separovaná technika zatím neexistuje, existuje však několik typů, či forem informačních operací, které se navzájem prolínají a doplňují. V současné době lze rozlišit, jak uvádí Martin Libicki [78], nejméně sedm typů informačních operací (viz obr. 10):

1. Působení na velení a řízení „*command-and-control warfare*“.
2. Zpravodajské působení „*intelligence-based warfare*“.
3. Elektronický boj[13] „*electronic warfare*“.
4. Psychologická válka „*psychological warfare*“.
5. Ekonomicko-informační válka „*economic information warfare*“.
6. Hackerská válka „*hacker warfare*“.
7. Kybernetická válka „*cyberwarfare*“.

[13] Pro anglický výraz Electronic warfare se v české vojenské terminologii používá termín elektronický boj, ne doslovný překlad - elektronická válka.

Obrázek 10. Jednotlivé typy informačních operací podle tradičního pojetí



Zdroj: HAWKINS Charles. Coming to Grips With Information Warfare.

V některých případech se uvádí ještě např. politická informační válka a legální informační válka, jak píše Ahvenainen. [1] Tyto pojmy se však spíše vztahují ke způsobům vedení informační války a ke stupni, na který je její působení zaměřeno, než aby byly považovány za další typy informačních operací.

PŮSOBENÍ NA VELENÍ A ŘÍZENÍ (C2W)

Zneškodnění velitele je už po staletí jedním z cílů k získání nadvlády na bojišti. Obtížnější však vždy byla vlastní realizace tohoto záměru. Posun ovšem nastal v okamžiku vytváření velitelských center. Ta jsou snadno identifikovatelná podle základních rysů jako jsou například viditelná komunikace, výpočetní zařízení (spojené s elektromagnetickým vyzařováním) nebo přesuny tištěných dokumentů a logistického materiálu, a hlavně, jak zdůrazňuje Hodický, podle netypických aktivit, které jsou naprosto odlišné od standardní činnosti u ostatních jednotek [52]. I přes jasnou nevýhodu centrálního bodu velení z hlediska snadné zranitelnosti není zatím tento způsob velení překonaný. Informace musí

být někde shromažďovány a na základě jejich analýzy distribuovány jednotkám pro vytvoření celkového operačního pohledu.

Účelem působení je zničení nebo narušení prostředků velení a neutralizace velení. Tím se přeruší informační tok od velitelských struktur k výkonnému prvku – bojovým jednotkám, které tím ztratí přehled o celkové situaci a nebudou mít mj. informace kde zasáhnout, kdy zasáhnout, ani jak zasáhnout. Účinnost těchto opatření jsou však, podle Nastoupila, značně závislá na míře centralizace umlčované struktury velení. [89] Redundatní, decentralizované spojení představuje problém při výběru cílů, na něž se musí působit. To byl také problém, uvádí Hodický, během druhé války v Perském zálivu[14] - západní ropné společnosti zanechaly v Iráku propracované komunikační sítě, které pak používala irácká armáda a pomocí nich získávala redundantní spojení. [52]

Fyzická neutralizace míst velení

Jednou z možností neutralizace velení a jednou z nejstarších forem je jeho fyzická likvidace (destrukce). Podle amerického polního řádu je v tomto případě „*fyzická destrukce aplikací bojové síly ke zničení nebo oslabení nepřátelských jednotek, zdrojů informací, systémů velení a řízení a míst velení*“. [60] Úder na místa velení lze provést pomocí různých prostředků, mezi nejčastější patří použití dělostřelectva, letecký úder nebo operace speciálních sil. V tomto případě, i když se jedná o nasazení bojových jednotek ke zničení cíle, jde o podpůrnou akci ve prospěch informační války. [63] Neutralizace míst velení je z hlediska informačního totální zastavení informačního toku, včetně fyzického zničení úložiště informací ve velitelském objektu; nebo alespoň jeho ochromení a zničení většiny uložených informací. V obou případech se jedná o likvidaci „informační instituce“.

Neletální neutralizace míst velení

Letální (smrtící) působení není jediným možným účinným prostředkem. Systémy velení a řízení lze paralyzovat například přerušením dodávek elektrické energie, pomocí elektromagnetického záření nebo nasazením počítačového viru. Ani jeden z těchto způsobů

[14] Druhá válka v Perském zálivu nesla kódové označení Irácká svoboda „Operation Iraqi Freedom“, byla zahájena 20. března 2003 místního času; bojové operace byly oficiálně ukončeny 1. května téhož roku.

však není, zdůrazňuje Libicki, spolehlivý a finančně méně nákladný ve srovnání s použitím fyzického prostředku ničení, jako např. letecké pumy. [78] V případě použití „měkkých zbraní“ je totiž nutné si uvědomit, že i softwarové útoky musí předem znát místo působení, jinak jsou neúčinné, nebo trvají příliš dlouhou a tím je účinnost minimální. V tomto případě se jedná o paralyzování informační instituce, následky útoku jsou však na rozdíl od fyzické likvidace vratné a po provedení oprav lze obnovit její činnost. To se však bude odvíjet od skutečnosti, zda bude ještě vůbec někomu informační podpora prospěšná.

ZPRAVODAJSKÉ PŮSOBENÍ (IBW)

O zpravodajské formě působení v informační válce se hovoří v případě, že je zpravodajství přímo zahrnuto v bojové činnosti – například v procesu výběru a přidělování cílů „*targeting*“ nebo při určení, zda daný prostředek zasáhl cíl a byl splněn požadovaný efekt „*Battle Damage Assessment*“ – a neslouží pouze jako vstup procesu velení a řízení. Účelem zahrnutí zpravodajství do bojové činnosti je tedy získávání informací, vytváření trvalého a obsáhlého obrazu bojiště. Kromě toho však má zpravodajství za úkol také ochranu informací, tzn. zabránit nepříteli, aby se mu nepodařilo informace získat a nemohl si vytvořit plnohodnotný obraz bojiště, včetně kapacit protivníka. Tyto činnosti se nazývají jako ofenzivní a defenzivní opatření. [89] Některé americké vojenské předpisy používají pro tyto činnosti souhrnný termín zabezpečení informací. [60] Zvláštností zpravodajského působení je oproti jiným formám informačních operací skutečnost, že vždy dochází k fyzickému kontaktu s cílem. [52]

Ofenzivní opatření

Jeho cílem je získávání co nejvíce informací o protivníkovi. Rapidní snížení poměru cena – výkon u informačních technologií umožnilo implementaci decentralizovaných systémů a vytvoření nových architektur pro získávání a rozšiřování informací. Decentralizované platformy zahrnují operátora, senzory a zbraňové systémy. V této architektuře operuje každý prvek autonomně, ale je s zároveň s ostatními elektronicky propojen. Takové pojetí je zcela odlišné od vedení války v průmyslovém věku, kdy každý prvek operoval zcela odděleně, (osádka tanku např. sama zjišťovala a zaměřovala cíle; nyní může získat přesné

informace o cíli, včetně souřadnic z bezpilotních průzkumných prostředků, nebo jiných senzorů). [78] Na bojišti v informačním věku mohou operovat různé senzory, vzájemně propojené a sestavené do architektury podle aktuálních požadavků [52]:

- Rozmístěné v odstupu od bojiště (pracující na bázi prostorové, seizmické a akustické).
- Rozmístěné přímo na bojišti (průzkumné bezpilotní prostředky, bezobslužná pozemní průzkumná vozidla nebo elektronické průzkumné prostředky).
- Rozmístěné na bojišti a pracující na bázi akustické, gravimetrické, biochemické a optické.
- Zbraňové, využívající infračervené záření a laserové paprsky.

Senzory v takovém rozsahu jsou schopny pokrýt celé bojiště a zajistit dokonce redundantní akvizici informací. Právě ta je v tomto případě důležitá, protože zaručuje větší důvěryhodnost situačního obrazu bojiště. Rovněž je pro protivníka mnohem obtížnější zabránit procesu získávání informací.

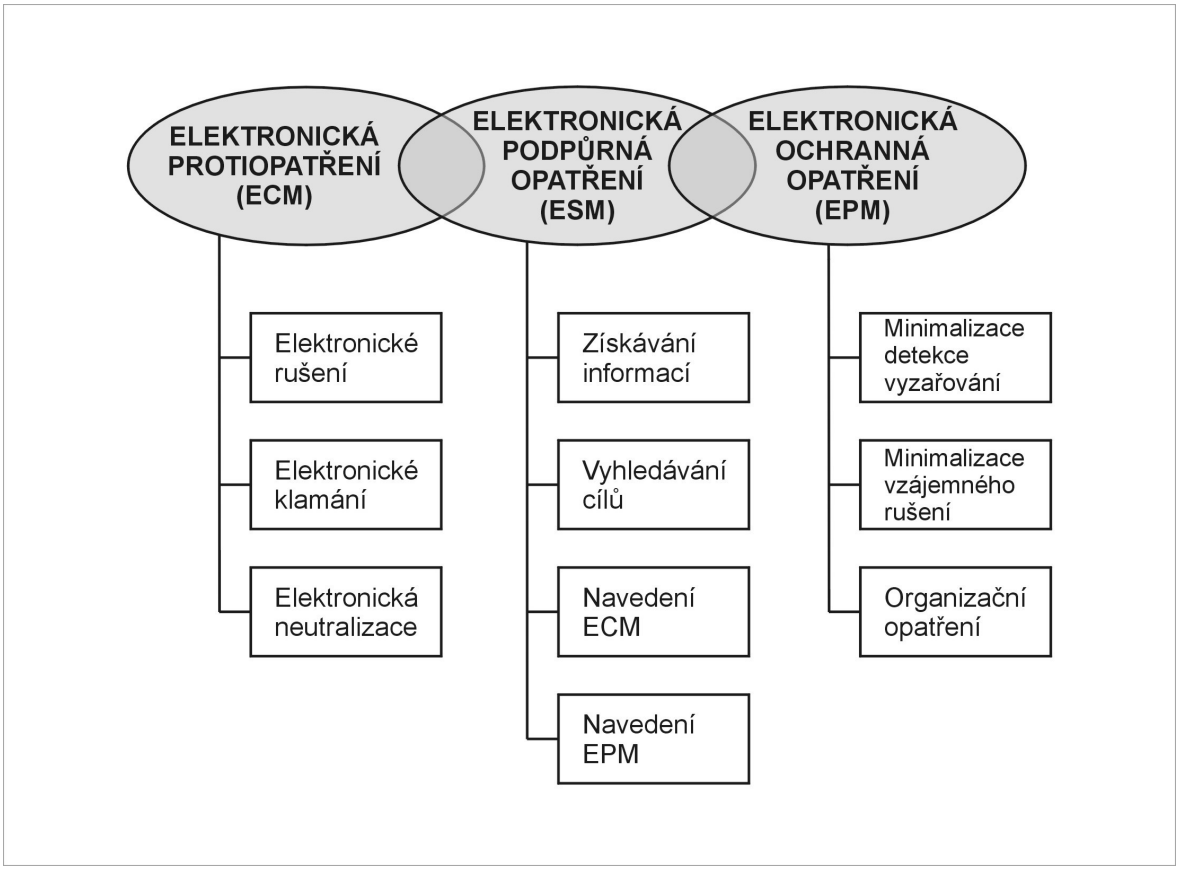
Defenzivní opatření

K defenzivním opatřením patří všechny možnosti, jak uniknout zjištění a pozorování nepřítelem, včetně klamání a používání nesnadno zjistitelných stanovišť. [89] Další možností je zásah přímo do procesu akvizice dat nepřátelským senzorem. Pokud takové opatření nelze realizovat, vzniká možnost působit na část spojení, kde senzorická část přechází do části vyhodnocovací. Jednou z nejstarších technik je předstírání vlastní nemohoucnosti detekovat činnost protivníka. [52] Jde tedy o aplikaci některé ze simulačních forem klamání. Defenzivní opatření lze také považovat za jednu z kontrarozvědných činností. Součástí defenzivních opatření je totiž i zjišťování zpravodajského zájmu protivníka, tzn. o jaké informace se vůbec zajímá. [83] Jinak by mohla být veškerá opatření zbytečná, protože by utajovala informace, kterými protivník již disponuje, nebo je vůbec nepotřebuje.

ELEKTRONICKÝ BOJ (EB)

EB je definován jako „*činnost zaměřená na využití elektromagnetického spektra, která obsahuje pátrání, zachycení a identifikace elektromagnetického vysílání, využití elektromagnetické energie včetně směrového vyzařování s cílem omezit nebo zabránit jeho využívání protivníkem proti vlastním prostředkům a zajistit jejich efektivní využití*“. [134] EB má tři součásti (viz. obr. 11) [131]:

Obrázek 11. Součásti elektronického boje



Zdroj: Autorův vlastní diagram.

- Elektronická protiopatření; zahrnující činnosti prováděné ke znemožnění nebo ztížení efektivního využití EM spektra protivníkem použitím EM energie (znemožnit mu přenos informací EM spektrem).
- Elektronická podpůrná opatření; zahrnují činnosti k vypátrání, zachycení a identifikaci EM vyzařování a zaměření jeho zdrojů. Poskytují zdroj informací pro

rozhodovací procesy, použití zbraní, elektronická protiopatření, elektronická ochranná opatření a jiné činnosti.

- Elektronická ochranná opatření; zahrnují činnosti k zajištění efektivního použití EM spektra vlastními silami v podmínkách (navzdory) použití EM energie protivníkem (zajišťují využití EM k přenosu vlastních informací).

Zjednodušeně řečeno, EB zahrnuje všechna ofenzivní i defenzivní opatření pro využívání elektromagnetického spektra. Z informačního hlediska lze považovat za základní způsoby elektronického boje působení proti komunikaci a komunikačním systémům, radiolokátorům a dalším elektronickým zařízením s cílem degradovat přenos protivníkových informací a současně zajistit přenos vlastních informací.

Působení proti radiolokátorům

Jedním ze základních způsobů elektronického boje je působení proti vyhledávacím a naváděcím radiolokátorům. Lze je umlčovat elektronickým rušením nebo protiradarovými raketami. [89] Tradiční radiolokátory generují signál na jedné frekvenci, modernější však pracují na principu rychlých změn vysílací frekvence. Antiradary musí být schopny zjistit příchozí signál, určit jeho frekvenci, přizpůsobit se jí a vyslat rušivý signál tak, aby byl minimalizován dosah a síla rušeného signálu. [52] Z hlediska informačního byl přerušen datový tok k bojovým prvkům (např. letounům) a potlačeno úsilí k získání informací o našich kapacitách. V této souvislosti ovšem nastává problém. Podařilo se sice zabránit navedení nepřátelských zbraní na místa velení nebo potlačit úsilí o vypátrání a zaměření vlastních naváděcích prostředků, rušící prostředek nicméně vysláním rušivého signálu prozradil svojí polohu a stává se tak významným cílem pro úder protivníka. [78]

Působení na komunikační prostředky a komunikace

Elektronický boj proti komunikačním prostředkům, sdílení a výměně informací je složitější a náročnější než působení proti radiolokátorům. Zatímco paprsek radiolokátoru je zaměřen přímo na určitý cíl v prostoru vlastních jednotek, při komunikaci se nepřítel snaží, jak zdůrazňuje Libicki, „*úplně vyhnout našemu prostoru, našimi jednotkami kontrolované*

části spektra“. [78] Situaci rovněž komplikuje skutečnost, že fyzikální vlastnosti šíření signálu komunikačních prostředků jsou odlišné od vlastností vyzařování radiolokátorů. Komunikační prostředky navíc používají mj. tzv. frekvenční skákání „*hopping*“ nebo rozprostřené frekvenční spektrum a technologii CDMA[15]. Jde o techniky, při jejichž využití je signál obtížně zjistitelný, lze ho obtížně rušit nebo přerušit. Satelitní komunikace využívá digitálních technologií pro příjem signálu v očekávaném směru a filtrování rušících signálů z ostatních směrů. Digitální kompresní mechanismy spolu s redundantním bitovým tokem mohou dokonce umožnit obnovení signálu při zarušení jeho části. [52] Z hlediska informačního jde během působení na komunikace o přerušení informačního toku protivníka (předávání a získávání informací) mezi jednotlivými prvky na bojišti a samozřejmě i odříznutí informační instituce, což je v tomto případě místo velení. Všechny prvky budou informačně činné, ovšem distribuované informace se nedostanou k uživatelům vůbec, nebo v nepoužitelném stavu.

PSYCHOLOGICKÁ VÁLKA (PSYW)

Psychologické operace jsou 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*“. [134] Zjednodušeně vyloženo, cílem psychologické války[16] je, podle Nastoupila, ovlivňovat nepřátelskou vůli bez použití zbraní. [89] Z informačního hlediska jde o plánovanou a systematickou distribuci informací různým cílovým skupinám, která musí být provedena v přesně stanovené období, aby informace ovlivnily jejich vědomí.

Psychologické operace a propaganda mají k sobě velmi blízko. Hranice mezi oběma činnostmi je nejasná a podle některých autorů se tyto činnosti dokonce prolínají. Obecně platí, že psychologická operace v době míru je založena na prezentování pravdivých informací, nebo alespoň pravdy jak je vnímána. Propaganda je naopak vnímána, podle

[15] CDMA – „Code Division Multiple Access“ je mnohonásobný přístup do sítě kódovým dělením. Na rozdíl od konkurenčních systémů jako GSM, který využívá TDMA, CDMA nepřiřazuje každému uživateli specifickou frekvenci. Místo toho používá každý kanál úplné dostupné spektrum. Jednotlivé hovory jsou kódovány pomocí pseudonáhodné digitální sekvence.

[16] Psychologická válka „Psychological Warfare“ bývá rovněž označována jako psychologické operace „Psychological Operations“ (PSYOPS).

autorů *Oxfordského průvodce vojenskou historií*, jako šíření lží (klamných informací) a cílovou skupinou je často vlastní obyvatelstvo. [123] Tiina Seppälä má pro propagandu umírněnější definici: „*jedná se o vědomé, metodické a plánované rozhodnutí k využití technik přesvědčování k dosažení specifických cílů, které mají sloužit ku prospěchu tomu, kdo organizuje tento proces*“. [115] V období ozbrojeného konfliktu, dále zdůrazňuje Seppälä, je však nutno vnímat propagandu zcela jinak. Tvoří totiž spolu s vojenskou frontou a finanční frontou trojici tří nejdůležitějších válečných front. Z tohoto pohledu pak jde souhlasit i s tvrzením Lískové, která uvádí, že cílovou skupinou psychologických operací nikdy není vlastní armáda nebo obyvatelstvo. [80] Tiskoviny i rozhlasové vysílání organizované československým exilovým vedením za druhé světové války a určené jako podpůrný prostředek pro vlastní jednotky lze proto považovat za propagandu a ne za psychologickou válku.

Kategorie psychologických operací

Psychologické operace je možné rozdělit na různé kategorie podle tří hledisek. Prvním je druh operace, k jejíž podpoře slouží, druhým pak a cílová skupina, na kterou se zaměřují a třetím je stupeň působení. Podle prvního kritéria, které používá i Armáda České republiky, se dělí na strategické psychologické operace (SPO), psychologické operace k podpoře bojových operací (CPO) a psychologické operace k podpoře nebojových operací (CRPO). [80] Podle druhého hlediska lze rozlišit operace proti vůli národa, proti nepřátelským velitelům, proti nepřátelským jednotkám a poslední kategorií je tzv. kulturní válka. [78] Podle posledního hlediska, který používá americká doktrína, se jedná o psychologické operace prováděné na strategické, operační a taktické úrovni. [34]

Strategické psychologické operace jsou vedeny na cílovou skupinu v době míru, krizových situací a v době válečného stavu. Jejich cílem je získat podporu a spolupráci spřátelených a neutrálních zemí a potlačit vůli a odhodlání protivníka vést válku. V době míru jsou SPO součástí uplatňování bezpečnostní a obranné politiky v souladu s národními zájmy daného státu. V případě vzniku krizové situace, SPO demonstrují odhodlání, vůli a způsob, kterým ji chtějí řešit představitelé státu a obyvatelstvo. Tyto strategické operace plánují, řídí a vedou státní orgány, zejména ministerstva zahraničí. [80] SPO jsou tedy operace zaměřené na vůli národa, jak uvádí Libicki. [78]

Psychologické operace k podpoře bojových operací jsou plánovány a vedeny v době válečného stavu jako součást bojových operací k zabezpečení obrany státu nebo kolektivní obrany podle článku 5 Washingtonské smlouvy. Jsou krátkodobého charakteru. Jejich cílem je vyvíjet psychologický nátlak na jednotky protivníka a obyvatelstvo pod kontrolou protivníka v oblasti bojové činnosti a podpořit tak dosažení operačních a taktických cílů operace. V podmínkách AČR je plánuje a řídí velitel operačního uskupení a vedou je jednotky AČR. [80] V podmínkách Spojených států se dokonce předpokládá nasměrování satelitního televizního vysílání na konkrétní zájmovou oblast. V případě, že má stát takové možnosti, je samozřejmě přísun ovlivňujících informací mnohem mohutnější a dosažení požadovaného výsledku pravděpodobnější. [52] V případě, že se působení zacílí přímo na nepřátelské velitele, jde o třetí kategorii psychologických operací, podle dělení Martina Libickiho. Jde však o značně obtížnou operaci, protože působení musí překonat zažité procesy – především povinnost dodržet rozkaz nadřízeného. Proto konečný výsledek působení, tedy zda byla předložená dezinformace přijata, záleží především na schopnosti velitelů ovládat svoje emoce a na jejich vycvičenosti. [78]

Psychologické operace k podpoře nebojových operací jsou plánované psychologické aktivity prováděné jako součást nebojových operací. Záměrem je dosáhnout spolupráce mezi vojenskými jednotkami a místním obyvatelstvem s cílem napomoci k uklidnění situace, prosazení míru, ovlivnění politického prostředí, zamezení nelegálních aktivit apod. [80]

Zvláštním případem je kulturní válka, podle některých teoretiků, není ani součástí informační války, ale samostatným druhem neletálního působení na protivníka, jak uvádí Libicki. [78] Jedná se v podstatě o kulturní invazi do odlišného prostředí s cílem „transformovat či zkulturnit danou společnost podle vlastních představ“. Rozsah kulturní války nelze přesně stanovit. Je jisté, že vůdčí zemí kulturní války jsou Spojené státy. „*Americká kulturní nadvláda nemá rovného soupeře ani historického předchůdce*“, zdůrazňuje Brzezinski. [17] Za kulturní válku, nebo již dokonce získanou nadvládu je možné považovat přijímání amerických stravovacích návyků, nadvládu na poli filmového průmyslu, populární hudby, internetu, značkového zboží, jazyka a také vysokoškolského vzdělávání a manažerských dovedností. [17] Invazi této kultury usnadňuje její přitažlivost,

současný rozmach informačních a komunikačních technologií a informovanost obyvatel zemí třetího světa o sociálních a technologických vymoženostech Západu.

EKONOMICKO-INFORMAČNÍ VÁLKA (EIW)

Ekonomicko-informační válka vznikla spojením ekonomické války a informační války. V současné době se rozlišují dvě její formy: informační blokáda a informační imperialismus. [78]

Informační blokáda

Informační blokáda bude efektivní a má smysl ji vést pouze ve společnosti, kde je životní úroveň závislá nejenom na materiálních dodávkách, ale i na přísunu informací. Je založena na potlačení přístupu k informacím (předpokládá se do určité míry i potlačení exportu informací), což může způsobit zhroucení ekonomiky nepřátelského státu. Může být proto chápána i jako varianta ekonomické blokády. Pracuje na podobném principu jako ekonomické blokády, která odřízne stát od dodávek zboží a snaží se potlačit výhody z účasti na mezinárodním obchodu. Z informačního hlediska potlačuje informační blokáda výhody výměny a sdílení informací v mezinárodním měřítku. Musí zahrnout působení na virtuální i fyzický tok informací. Za fyzický tok informací lze považovat například distribuci manuálů v tištěné formě, databáze na fyzických nosičích (CD-ROM a DVD) atd. Jedna z forem informační blokády může být narušení infrastruktury satelitních spojů a tím znemožnění komunikace a paralyzování toku dat od vysílače k přijímači. [52] Informační blokáda rovněž omezuje možnosti blokované země, dodává Libicki, vést psychologickou válku. [78] Otázkou ovšem zůstává, jak dále uvádí, do jaké míry je v současné době informační blokáda proveditelná.

Informační imperialismus

Informační imperialismus vychází z předpokladu, že mezinárodní obchod je v přeneseném významu bojiště. Jednotlivé národy si konkurují a usilují o získání dominantního postavení

ve strategickém průmyslu. Zdá se na první pohled, že jde o ryze ekonomickou záležitost. I v této oblasti však hraje informace důležitou roli. Jako příklad může sloužit americké Silicon Valley[17]. Výhoda být a pracovat v této oblasti spočívá, podle Libickiho, v jednodušším přístupu k zákazníkovi, dodavateli a v relativně snadném získání pracovníků s dobrou znalostí výpočetní techniky. [78] Firmy, které zde působí úzce spolupracují v oboru elektroniky, provádí výměnu a sdílení nejnovějších informací, mají dostatek hypermoderních technologií a „mladých mozků“. Podle některých teorií je totiž v oblastech s vysokým finančním příjmem zaznamenán i vyšší přírůstek obyvatelstva. V souvislosti s vyspělým průmyslem výpočetní techniky dochází k souhře obou těchto faktorů a proto místní populace převyšuje okolní oblasti nejenom finančně, ale i vědomostmi a vzděláním. Je tedy informačně gramotnější. [52]

HACKERSKÁ VÁLKA

Informační operace jsou často zjednodušeně považovány za válku hackerskou. Ve skutečnosti je však hackerská válka jedním z typů informačních operací, kde útoky směřují na konkrétní systémy (jejich strukturu i obsah) s využitím technologických nedostatků „děr“ v bezpečnostních opatřeních. [52] Techniky či metody hackerské války se liší podle místa, odkud útočník podniká útok, podle způsobu provedení a podle předpokládaného rozsahu škod. Všechny techniky hackerské války zde dále uváděné představují útoky proti civilním cílům. Útoky na civilní a teoreticky i vojenské cíle mají v hackerské válce společné charakteristiky. Libicki má však pravdu, že vojenské systémy jsou lépe zabezpečené než civilní [78], proto by měly i lépe odolat útokům. Vojenský systém je totiž navržen pouze pro vnitřní přístup a od okolí (například internetu) je fyzicky oddělen. Téměř vždy jsou v něm uchovávány utajované informace, jejichž sdílení s veřejností nepřichází v úvahu. Hackerský útok na vojenské systémy typu C2I je proto podstatně složitější. Z hlediska informačního se jeví vojenský systém jako uzavřený informační systém, který propojuje neveřejné a navíc střežené informační instituce.

Útoky na civilní systémy se rozlišují z operačního hlediska zpravidla na útoky na fyzickou úroveň, syntaktickou úroveň a na sémantickou úroveň. Útok na fyzickou úroveň je

[17] Nejjižnější část sanfranciského pobřeží v Severní Kalifornii ve Spojených státech amerických. Je zde neobvykle vysoká koncentrace společností zabývajících se vývojem a výrobou křemíkových mikročipů a počítačů.

zaměřen na konkrétní fyzickou součást. Tento druh útoku se vyskytuje zřídka, i když Schwartau uvádí možnost útoku s využitím mikrovlnného paprsku, který způsobí náhodné chyby zasaženého počítače. [114] Cílem syntaktických útoků jsou, podle Libickiho, části informace – bity a jejich pohyb; sémantické útoky mají ovlivnit a změnit význam či smysl informací přijímaných počítačem (vstupních dat). [78] Hackerská válka lze rovněž rozdělit podle toho zda je útočná nebo obranná. Tedy, zda je cílem poškodit cizí informační systémy, nebo zda jsou přijímána obranná opatření proti případnému hackerskému útoku.

Zda je hackerský útok opravdu válka, zůstává dosud otázkou. Jisté však je, že hackerský útok na vojenský informační systém může sloužit jako podpůrná činnost při vedení konvenční vojenské operace a při vedení jakékoliv jiné formy (typů) informačních operací. Zcizení, nebo znehodnocení dat může změnit rovnováhu sil na bojišti (na operační a taktické úrovni), nebo může mít dokonce strategický význam (technologie strategického významu). Cliff Stoll uvádí příklad, kdy se v minulosti podařilo hackerům proniknout do informačního systému americké Ústřední zpravodajské služby (CIA) a získat informace o technologiích, které měly strategický význam pro Sovětský svaz. Získané informace potom údajně hackeři předali za značný finanční obnos sovětskému Výboru státní bezpečnosti (KGB). [117]

KYBERNETICKÁ VÁLKA

Termín kybernetická válka pro mnoho lidí navozuje představu ničivých, zákeřných programů, které způsobují, že počítačové systémy zamrzají a zbraňové systémy selhávají, a využívají tak zázraků technické zdatnosti k nekrvavým vítězstvím. Tento obraz, ve kterém je kybernetická válka izolována od širšího konfliktu, odvíjí se v prostředí zcela odlišném od tradičního vedení boje a nabízí nekrvavou alternativu nebezpečí a nákladnosti moderní války, je sice atraktivní, ale nerealistický. Skutečnost bude zcela rozdílná, zdůrazňuje Dunlevy: „k*ybernetický boj bude mít téměř jistě reálný fyzický dopad*“! [36]

Kybernetická válka je považována za zcela specifickou oblast informačních operací; zahrnuje informační terorismus, sémantické útoky (prolíná se s hackerskou válkou), simulovanou válku a Gibsonovu válku.[78] Předpokládá se, že některou z těchto forem bude působit na vyspělé vojenské systémy. Počítačová technologie se totiž od jiných

vojenských prostředků liší v tom, že je integrální součástí všech ostatních prostředků používaných v moderních armádách. Z tohoto pohledu je právě tou klíčovou součástí, na které mnohé moderní armády závisejí, a této závislosti jsou si potenciální nepřátelé dobře vědomi. Kybernetická válka zatím nebyla v žádné své formě proti vojenským prostředkům použita, stále častěji se však o ní diskutuje a její formy jsou předmětem zájmu vojenských odborníků.[52] Některé její formy proto již nejsou zdaleka futuristickým jevem, jak uváděl ještě v roce 1998 Waltz [135], ale představují v současné době naprosto reálnou hrozbu. V květnu 2007 se staly cílem rozsáhlého kybernetického útoku servery estonských vládních institucí, včetně ministerstva obrany, parlamentu, sítě mobilních operátorů a dokonce i komunikační síť záchranné služby. [15] Následky útoku mohly být v případě souhry přírodní nebo průmyslové katastrofy tak vážné, že ho estonské ministerstvo obrany přirovnalo k teroristickým útokům ve Spojených státech v září 2001. Severoatlantická aliance a Spojené státy vyslaly v této souvislosti do Estonska své odborníky, identifikovat přesně útočníka, přestože estonská vláda obvinila Rusko, se nepodařilo. Útoky (s cílem zahltit servery a tím je paralyzovat) byly vedeny z počítačových terminálů z nejrůznějších světových destinací, včetně Spojených států, Brazílie nebo Vietnamu. [71]

Informační terorismus

Informační terorismus je součástí počítačového hackingu, který se zaměřuje ne na narušení systémů, ale na využití osobních dat důležitých osobností, včetně vojenských velitelů, k následnému působení přímo na ně nebo na jejich blízké. V počítačových úložištích, včetně vojenských, jsou totiž v mnoha souborech údaje o zdravotním stavu, vzdělání, finančních náležitostech, zájmech, příbuzných, kontaktech na jiné osoby a různé státní i nestátní organizace. V případě informačního terorismu je ovšem problém vědět přesně, jak nakládat s takto získanými informacemi. Ne všichni lidé budou pod hrozbou zveřejnění, nebo zneužití shromážděných informací reagovat stejně a ne každého lze tímto způsobem donutit k vyvíjení požadovaných aktivit [78], jako např. odvolat nebo pozměnit plánovanou vojenskou operaci. Základním způsobem ochrany proti informačnímu terorismu může být mj. zavedení restriktivních podmínek pro uchovávání citlivých informací.

Sémantický útok

Sémantický útok je podobný hackerské válce. Při ní ovšem dojde k náhodným nebo systematickým chybám systému, včetně výpadků; nakonec napadený systém přestane pracovat úplně. Při sémantickém útoku počítačový systém pracuje dále, navenek bezchybně, ale generuje výstupy, které se různou mírou rozcházejí s realitou (chybné výstupy). Útok tohoto typu na bojové letouny by mohl mít fatální následky. Bez fungujícího systému - hardware, bez pracujícího software, nebo s poškozeným software je moderní letoun téměř neovladatelný, není schopen plnit bojový úkol, ani se bránit proti napadení.[3] Mechanické ovládání se totiž stalo minulostí a zbraňové systémy i pohonná jednotka je řízena pomocí informací z palubního počítače, který komunikuje s pozemním řídícím střediskem.

Simulovaná válka a Gibsonova válka

Věrohodnost počítačových aplikací založených na simulačních technologiích se neustále zvyšuje. Simulace jsou běžnou součástí vojenského výcviku i výzkumu. V této souvislosti by mohl využít protivník, podle Libickiho, simulaci vojenského konfliktu a zaměnit ho s realitou. Podle něj by zvítězil, v rozporu s realitou, nad některými jednotkami a donutil velení k nesprávným rozhodnutím. Druhou možností je, že by v simulovaném vojenském konfliktu demonstroval, že bojovat proti jeho kapacitám nemá smysl, protože by porážka byla nevyhnutelná.[78]

Gibsonova válka předpokládá existenci umělé inteligence, vychází z konceptu dvojí reality (fyzické a virtuální). Obě na sobě závisí, přičemž vítězství ve virtuální realitě postačuje k definitivní porážce protivníka.[52] Obě tyto formy kybernetické války jsou z hlediska informačního jen těžko proveditelné, z hlediska vojenského patří do oblasti sci-fi a jejich realizace není pravděpodobná ani v dohledné budoucnosti.

ZÁVĚR

Informační operace se obvykle člení podle způsobu vedení na sedm základních typů, počínaje působením na velení a řízení a kybernetickou válkou konče. Někdy odborná literatura uvádí méně forem, někdy naopak více. Jedná se však buď o dílčí způsoby vedení některé ze základních forem, nebo naopak o spojení blízkých forem do jedné. Clay Wilson například uvádí tzv. operace v počítačových sítích „*Computer Network Operations*“. [143] Jedná se však o sloučení hackerské války a kybernetické války do jedné formy.

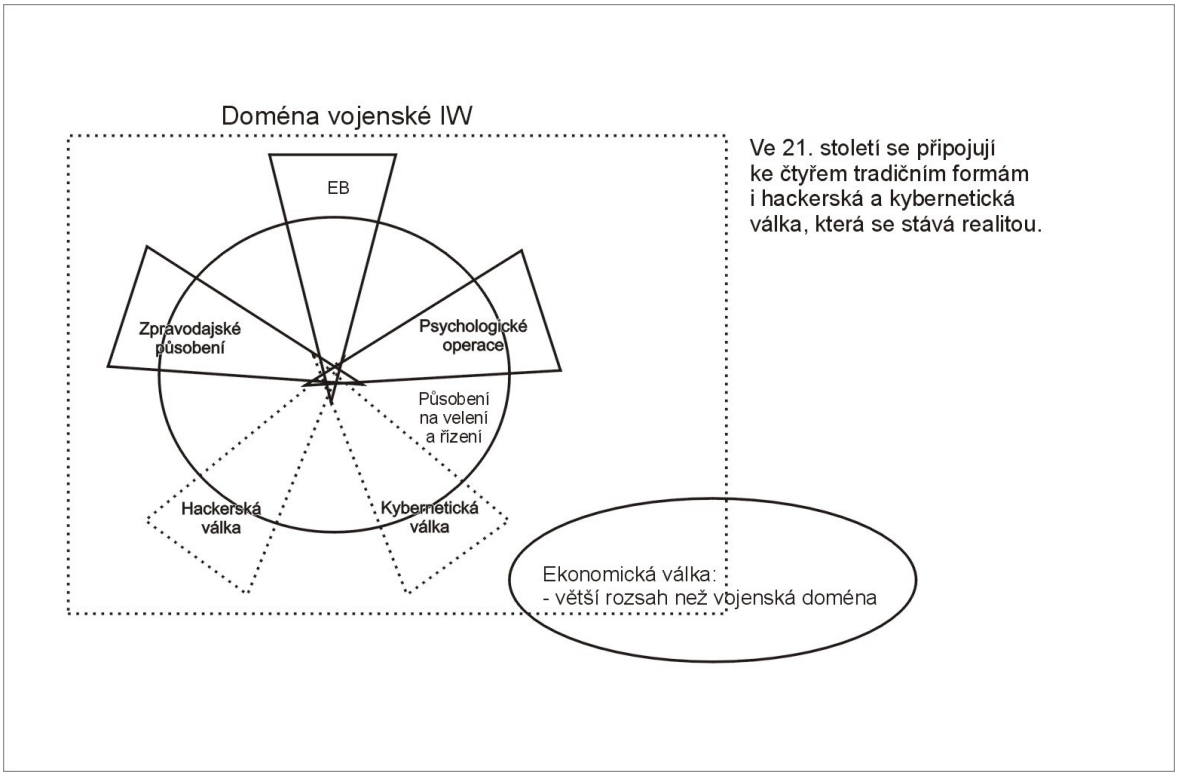
Některé typy informačních operací byly používány již v dávné minulosti, i když nebyly nazývány dnešními názvy. V tomto směru je nutné uvést na prvním místě použití zbraní proti místům velení. Neutralizace velení se používala po staletí k získání nadvlády na bojišti. Dávno známé je i psychologické působení na protivníka. Tento typ informačních operací lze vést v rámci bojových i nebojových operací.

Zpravodajské působení má za úkol vytváření obrazu bojiště a zároveň zabránit protivníkovi, aby udělal totéž. Při defenzivní činnosti se provádí opatření, jak uniknout zjištění a pozorování s využitím různých technik klamání. Relativně mladou formou informační války je elektronický boj. Kromě původního poslání – ovládnutí elektromagnetického spektra se prostředků EB začíná využívat i jako elektromagnetických nekinetických zbraní založených na vysílání krátkých elektromagnetických impulsů. Ty jsou údajně schopné zničit protivníkovu výpočetní techniku a dokonce paralyzovat vystřelenou raketu. [143]

Ekonomicko-informační válka, hackerská válka a kybernetická válka se vztahují spíše k civilnímu sektoru, ale zvláště posledně jmenovaná je v poslední době hodně diskutovaným typem informačních operací. V této souvislosti poukazuje Nastoupil na nebezpečí, které hrozí při jejím podcenění: „*její útoky, nemusí být ihned zpozorovány, nýbrž mohou probíhat po dlouhá období, dříve než se projeví prvé škody*“. [89] V takovém případě však může být během ozbrojeného konfliktu již pozdě. Americké vojenské letectvo šlo v tomto směru dokonce tak daleko, že vytvořilo Velitelství pro kybernetickou válku. [143] Následky kybernetického útoku mohou mít samozřejmě vážný dopad i v době míru a čím více bude instituce, organizace nebo samotná vláda, jako např. „e-government“ Estonska, závislá na výpočetní technice, tím bude rozsah škod závažnější. [40] Případ

kybernetického útoku proti Estonsku je jedním z mnoha podobných útoků, jejichž počet v posledních letech stoupá. To potvrzuje, že kybernetická válka již vystoupila z futuristických představ a stala se realitou. Ve svém rozsahu se rovněž značně překrývá s hackerskou válkou a mnohdy se oba typy operací zjednodušeně nazývají (poněkud zavádějícím termínem) kyberterorismus. V této souvislosti lze proto s trochou nadsázky částečně poopravit Hawkinsův model jednotlivých typů informačních operací [50] (viz obr. 12).

Obrázek 12. Jednotlivé typy informačních operací ve 21. století



Zdroj: Autorův vlastní diagram odvozený z HAWKINS Charles. Coming to Grips With Information Warfare.

Rostoucí význam jednotlivých typů informačních operací potvrzuje i rostoucí význam informace jako zbraně ve vojenství. Úroveň informačního zabezpečení vojsk a ochrany vlastních informací se stala činitelem podmiňujícím úspěšnost vedených bojových i nebojových operací. Je zřejmé, že některé formy informační války mají v současné době civilní charakter. Existují hluboko pod prahem dosud označovaným jako válka. Je zcela zřejmé, že v budoucnu bude rozhraní mezi mírem a válkou stále méně zřetelné. V této souvislosti je jasné, že účelná kooperace a koordinace vojenských a civilních aktivit pro ochranu před útoky informačních operací je nezbytná.

. PLÁNOVÁNÍ INFORMAČNÍCH OPERACÍ

ÚVOD

Každá vojenská operace musí být před vlastním zahájením pečlivě naplánována a připravena. Informační operace mohou být součástí bojových operací v době ozbrojeného konfliktu, nebo součástí mírových misí určených ke stabilizaci bezpečnostní situace a udržení míru v určité oblasti kdekoli na světě. Jejich naplánování je jednou z dílčích částí plánovacího procesu celé vojenské kampaně. Musí být provedeno vždy v počátečním stadiu plánovacího procesu a nezbytnou podmínkou je, aby bylo vždy jeho součástí, nikdy ne, zdůrazňují americké předpisy, pouze doplňkem nebo přílohou. [59] Naplánování informačních operací samozřejmě vyžaduje včasnou a podrobnou přípravu. Její součástí je tzv. zpravodajská příprava bojiště. Tou se rozumí analytické vyhodnocení celkové situace v prostoru předpokládaného působení, včetně vyhodnocení kapacit a možností protivníka, terénu, klimatických podmínek a všech dalších faktorů, které mohou ovlivnit vedení operace. Zahrnuje proto nejprve sběr informací, jejich zpracování a vytváření rozsáhlých databází pro každou oblast kde by mohly být potenciálně nasazeny síly a prostředky. Takto roztříděné a uložené informace jsou pak vyhodnocovány s cílem předvídat dopad zamýšlených operací na místní prostředí, včetně sil protivníka a místního obyvatelstva. Zpravodajská příprava bojiště není jednorázový proces a nekončí zahájením operace, to by byla fatální chyba. Naopak musí to být vždy průběžný proces, na jehož základě je nutné opravovat a aktualizovat operační plány a tedy i přizpůsobovat činnost jednotek skutečným cílům a potřebám. [32] Úspěšnost plánovacího procesu je závislá na shromážděných informacích, jejichž kvalita a včasnost je předpokladem k získání informační nadvlády nad protivníkem. To potvrzuje i prohlášení amerického generála Gordona Sullivana, podle kterého „*jsou informace měnou vítězství na bojišti*“. [58]

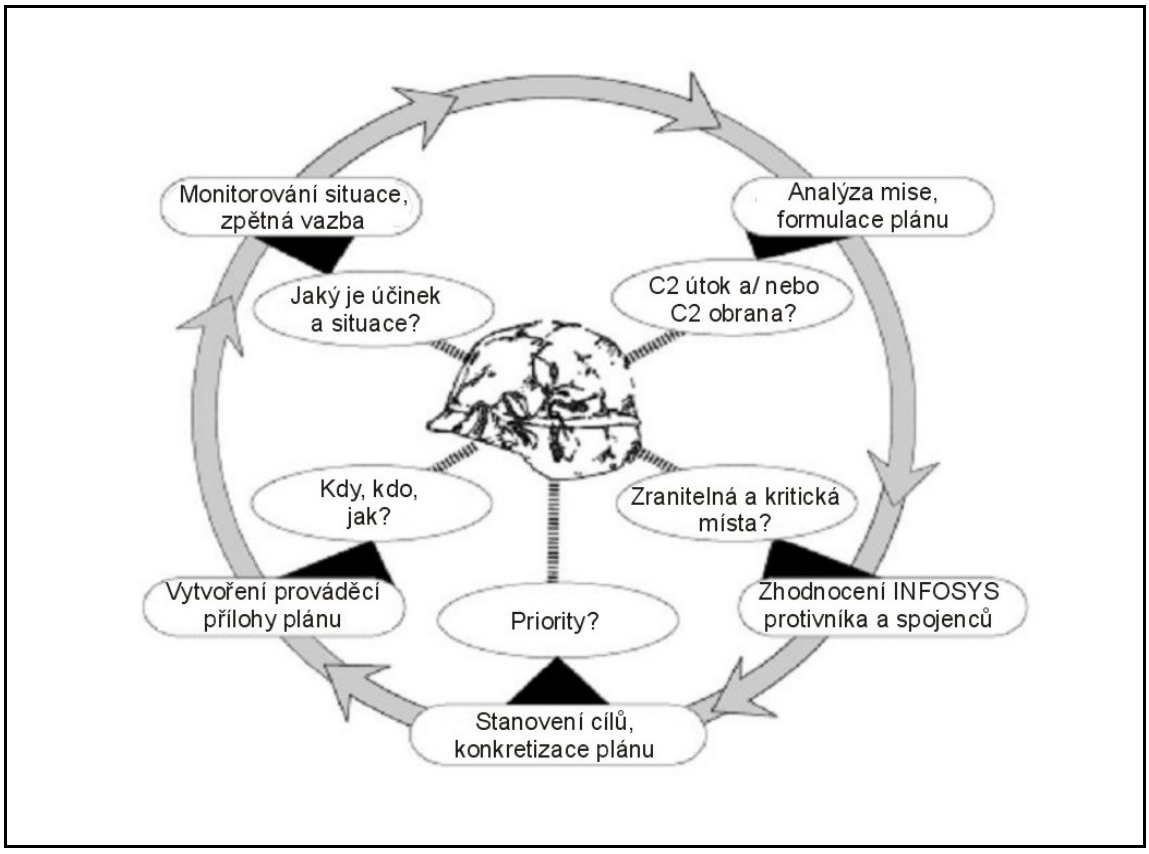
PLÁNOVACÍ PROCES IO

Plánovací proces informačních operací je závislý na úrovni, na které bude vlastní operace vedena, tj. na strategické, operační nebo taktické úrovni. [58] Podle toho budou odlišné cíle, způsoby provedení, ale i předpokládaný dopad na protivníkovy jednotky. V zásadě

však lze shrnout proces plánování informačních operací (viz obr. 13) do pěti základních kroků [66]:

- Stanovení cílů informační operace
- Vypracování úkolů k dosažení stanovených cílů
- Identifikace nepřátelských cílů
- Určení prostředků k provedení IO, stanovení jednotlivých úkolů a příprava seznamu konkrétních nepřátelských cílů
- Zpětná vazba, kontrola, verifikace jednotlivých úkolů

Obrázek 13. Plánovací proces IO



Zdroj: Upraveno a převzato z *Information Operations.* FM 100-6.

V průběhu první fáze je nutné stanovit reálné, skutečně dosažitelné cíle, na které stačí kapacity vlastních sil a prostředků. Dále je nezbytné na základě analýzy aktuální situace určit cíle, jejichž splnění bude mít skutečně požadovaný efekt a bude mít vliv na protivníka, aby nedocházelo k plýtvání silami, které mohou být nasazeny k plnění jiných úkolů. V této souvislosti je rovněž nutné vyhodnotit slabé stránky protivníka, protože bude

efektivní zaměřit se právě na ně. V této plánovací fázi je také důležité rozhodnout, jaké typy informačních operací budou vedeny a jaké techniky k tomu budou použity. [66] Rovněž je nutné vyhodnotit spojenecké jednotky, jednak aby neměla plánovaná informační operace negativní dopad na jejich činnost a jednak způsob jak se na jejím vedení budou podílet. Zahrnuty musí být i nevojenské faktory, jako např. stav místních nebo regionálních komunikačních sítí, rádiové a televizní stanice v prostoru zamýšlené operace, zvyklosti a postoje místního obyvatelstva. [58] Posledně zmíněné faktory hrají velmi důležitou roli především při plánování informačních operací v prostoru mírové mise.

Během druhé fáze jsou vyhodnocovány pravděpodobné protivníkovy aktivity a působení na ně pomocí informačních operací. Odhadován je účinek tohoto působení a celkový vliv na změnu činnosti protivníka, aby byla v souladu s našimi záměry. Jedině pak je informační operace úspěšná. K dosažení stanovených cílů musí být rozpracovány dílčí úkoly pro jednotlivé jednotky a zvolen nejefektivnější způsob jejich provedení (např. klamání, dezinformace, likvidace míst velení, přerušení spojení nebo kombinace různých technik). Při sestavování úkolů je nutno stanovit priority. Ty jsou závislé na zranitelných místech protivníka a na důležitosti potenciálních cílů útoku (které budou paralyzovány nebo zničeny). Zároveň musí být naplánována obranná opatření, protože protivník by mohl odpovědět protiútokem na stejné cíle, např. na místa velení a prostředky spojení. Útočná i obranná opatření by měla být vyvážena, aby byla míra zranitelnosti vlastních sil a prostředků minimalizována. [58]

Ve třetí plánovací fázi probíhá identifikace (určování) konkrétních nepřátelských cílů, proti kterým bude veden útok. Cílem útoku jsou samozřejmě síly a prostředky protivníka, konkrétními cíli však může být mj. informační systém, výpočetní technika, počítačový program, příslušníci nepřátelských jednotek, ale rovněž mysl (vědomí) nepřátelských velitelů nebo vojáků a rovněž protivníkova data. [66] Právě jejich znehodnocení může hrát důležitou roli a nepřátelské jednotky nebudou disponovat potřebnými informacemi, nebo záměrně zkreslenými a pozměněnými. V této souvislosti je opět nutné pokračovat ve stanovení priority, tentokrát již ve vztahu k jednotlivým objektům (cílům) útoku. Tento krok je důležitý, protože útoky proti nepřátelským objektům nemusí být nutně vedeny ve stejný časový okamžik, ale záměrně v časovém sledu. Tato fáze je někdy také nazývána konceptem nebo-li pojetím, protože jde již o to jak konkrétně provést operaci. [58]

V předposlední čtvrté fázi nastává úkolování vlastních (případně i spojeneckých, pokud se budou na vedení operace podílet) sil a prostředků. Důležitý je výběr vhodných jednotek, aby měly potřebné kapacity a disponovaly potřebnou technikou ke splnění daného úkolu. Při nesprávné volbě by mohlo dojít k zbytečnému vyčerpání vlastních kapacit, neočekávaným ztrátám a případně i k ohrožení informační operace. To by mělo samozřejmě negativní dopad i na vedení celé bojové nebo nebojové operace. Výsledkem této fáze je sestavení seznamu nepřátelských cílů a k nim připojený seznam jednotek a techniky odpovědných za jejich ovlivnění, paralyzování nebo úplnou eliminaci. Tento seznam je zároveň vztažen k časové ose a součinnost mezi jednotkami synchronizována. [66]

Následuje provedení operace, monitorování jejího průběhu, kontrola plnění dílčích cílů, průběžné vyhodnocování a aktualizace a oprava předběžného odhadu. V této souvislosti může dojít i k přehodnocení některých úkolů, jejich změně a v případě neočekávaných změn k případnému stanovení úkolů nových. Celý plán musí být flexibilní, schopen reagovat na nenadálé změny situace a v záloze musí být pro tyto účely ponechán přiměřený počet sil a prostředků, aby bylo možné pozměněné a nové úkoly splnit. [66]

Omezení a překážky IO

Plánování a vedení informačních operací je omezeno nejenom kapacitami vlastních jednotek a technickými možnostmi. Je nutné respektovat i zákony a právní normy. Tím se rozumí ústava země která vede kampaň a její platné zákony, které do různé míry omezují možnosti nasazení jednotek. Dále je nutné ve vlastním zájmu dodržovat mezinárodní právo, zejména právní normy vztahující se k ozbrojenému konfliktu (LOAC[18]). V případě, že se jedná o koaliční operaci, mohou (často s negativním dopadem) vstupovat do hry i zákonné normy spojenců, pokud není výhradně stanoveno jinak. Některý z typů informačních operací nebo způsob jejího provedení může být považován za zcela legální právním řádem jedné země, ale jinou zemí za nepřátelský akt. [59] Kromě toho, zejména během mírových operací jsou omezující i zákony a zvyklosti země na jejímž území je operace vedena. V tomto případě se jedná v podstatě o pomoc a každé porušení by bylo

[18] LOAC – Law of Armed Conflict; soubor mezinárodně platných a uznaných právních ustanovení, které je nutno při vedení bojových operací dodržovat. V opačném případě je činnost jednotek považována za nelegální.

kontraproduktivní a hrozilo by vypovězení ze země. Při plánování je proto nutné vyhodnotit i zákony a normy o používání vysílacích frekvencí, přístupu veřejnosti k informacím, o působení zpravodajských služeb (v souvislosti s vedením špionážních aktivit), o využívání informačních a komunikačních sítí. Všechny tyto skutečnosti mohou ovlivnit zejména vedení psychologických operací, které jsou k podpoře mírových misí nezbytné.

Trvalou překážkou je při vedení a plánování každé operace, včetně informační určitý stupeň neurčitosti. Z hlediska informačního se jedná o typický případ neuspořádanosti systému (entropii). Dostupné informace získané před a v průběhu plánování operace nejsou nikdy úplné a naprosto věrohodné. Přetrvává zde „*válečná mlha*“, jak o ní hovoří Clausewitz. [24] Podle schopností průzkumných jednotek a prostředků a analytiků jí lze „*její hustotu pouze snížit, úplně však nezmizí nikdy*“. [58] Velitel bude mít vždy před sebou tuto překážku a bude záležet na jeho důvtipu a válečném umění. Do hry zde proto významným způsobem vstupuje lidský faktor.

Plánování propagandy

Příkladem plánovacího procesu IO je možný způsob naplánování psychologické operace s využitím technik propagandy. Jedná se o opět o nepřetržitý proces, který vyžaduje kromě úsilí i určitou dávku představivosti. Plánování musí být flexibilní a schopno zareagovat na aktuální změny situace nebo změny okolností ovlivňujících cílové obyvatelstvo (na které je působení psychologické operace zaměřeno). Při přípravě plánu je vhodné kalkulovat s možnými situacemi, které mohou nastat a přizpůsobit jim alternativní verze plánu operace.

Při zpracování plánu je nutné vzít v úvahu následující skutečnosti a limitující faktory [104]:

- Stanovení reálných cílů operace
- Analýza aktuální vojensko-politické situace
- Zdroje informací

- Konkretizace dílčích cílů (útoku) a jejich dosažitelnost
- Způsoby (působení), kterými budou splněny cíle psychologické operace
- Způsoby (působení), které jsou v dané situaci nevhodné (kontraproduktivní)
- Média, které budou využita
- Nutnost koordinace plánu s výkonnými složkami

Plánování má, podle manuálu pro psychologické operace, obecnou posloupnost (v reálném prostředí se mohou postupy a kroky lišit v závislosti na situaci a její proměnlivosti) [104]:

- Definování mise, jejího poslání a určení (co je vlastně cílem, čeho je potřeba dosáhnout)
- Zhodnocení situace ve vztahu k psychologické operaci (bude sloužit k podpoře mise), včetně odhadu účinku psychologické operace
- Příprava vlastního plánu – nařízení jednotkám k přípravě provedení propagandy (propagandistických úkolů)
- Výběr vhodných médií (jakým způsobem budou rozšiřovány informace tak, aby je cílová skupina byla schopná přijmout); např. v případě výběru televizního vysílání musí místní obyvatelstvo disponovat přijímači
- Vývoj propagandy – proces přípravy informací, které budou rozšiřovány (ve formě textu, jednotlivých slov, symbolů nebo prostřednictvím akce – v případě propagace činem)
- Vyzkoušení propagandy, tj. ověření zvolené propagandistické techniky na cílové skupině obyvatelstva (tato fáze je diskutabilní, informační operaci, ať se jedná o psychologickou, kybernetickou nebo jinou nelze pravděpodobně již v průběhu reálné vojenské kampaně „otestovat“; došlo by téměř jistě k jejímu prozrazení, protivník by použil protiopatření a obyvatelstvo by se stalo vůči zvolenému typu psychologického působení resistentní)[19].
- Řízení propagandy (psychologické operace s prvky propagandy)
- Zpětná vazba a vyhodnocení psychologické operace (získané poznatky budou zahrnuty do plánování jakékoli další operace s cílem minimalizovat zjištěné nedostatky)

[19] Poznámka autora: vhodnější by bylo uvést „vyladění propagandy“ – tzn. zahájení propagandistické činnosti a v případě zjištění nedostatků jejich bezodkladná náprava.

Zásadou vedení každé propagandy je důraz na její srozumitelnost a přesvědčivost. Struktura šířených informací se proto liší podle cílové skupiny obyvatelstva. Ta musí být schopna tyto, v souladu Vickeryho pojetím informace z hlediska informační vědy, informace pochopit, vstřebat a dále si je mezi sebou předávat (komunikací). V této souvislosti je vhodné vztáhnout sdělovanou informaci ke každodennímu životu, aby cílovou skupinu zaujala. Naopak je mj. zcela nevhodné používat nejasná, protichůdná prohlášení, neznámá či nefrekventovaná slovní spojení, slangové, odborné a cizojazyčné výrazy.

ZÁVĚR

Plánování tvoří důležitou součást informačních operací. Předchází samotnému vedení informační operace v jakémkoli prostoru působnosti (bojiště, prostor mírové operace nebo virtuální bojiště). Jedině pečlivé a důkladné naplánování může zajistit úspěch informační operace. Špatné vyhodnocení situace, podcenění protivníka nebo přecenění vlastních sil se nevyplácí a informační operace je v takovém případě neúspěšná. Fiaskem skončily německé pokusy vést informační propagandistické operace v první světové válce. Propaganda namířená do zahraničí byla nedostatečně připravená, amatérská a spočívala hlavně v různých článcích a prohlášeních akademiků a novinářů. Cílem bylo vysvětlit (podat veřejnosti informace), proč mají západní mocnosti vinu na rozpoutání války. Propagandě však chyběla, zdůrazňuje Bittman, pevná organizační struktura a morální zaujatost. Mezinárodní tisk ji ignoroval. [11] Dalším neúspěšnou informační operaci ilustruje příklad psychologické operace Spojených států ve válce ve Vietnamu. Americké jednotky podcenily odhodlání severovietnamských jednotek a partyzánského Viet Congu a přes značné úsilí nedokázaly jejich vůli po dosažení vítězství zlomit. Nepomohly ani tisíce letáků shozených z letadel, ani nasazení bojové techniky, kterou nepřítel neměl, jako např. bojové vrtulníky typu Cobra, nebo bombardovací letouny B-52. Naopak, byli to Vietnamci, kteří byli, podle Valleyho, lepšími psychologickými válečníky než Američané. [130] Jako neúspěšné, především z důvodu zkostnatělosti a nepružnosti, lze hodnotit dlouhodobě vedené propagandistické a dezinformační akce bývalého Sovětského svazu. Sověti vydali, podle Bittmana, např. v roce 1981 na tyto účely, včetně nákladů na rozhlasové vysílání stanice Rádio Moskva v 82 jazycích s 2 000 vysílacími hodinami týdně

přibližně 3,3 mld. USD. Přes veškeré snahy však Sovětský svaz nakonec tuto bitvu se Západem prohrál. Stereotypní domácí propaganda, které přestali věřit i ortodoxní komunisté, vážné hospodářské problémy, byrokracie a morální rozklad vyústily v hlubokou krizi, která v roce 1991 skončila zhroucením sovětského režimu. [11]

. VÝZNAMNÉ HISTORICKÉ INFORMAČNÍ OPERACE

ÚVOD

Na historii války lze nahlížet z různých pohledů. Jedním z možných je využití Tofflerovy teorie tří vln a rozlišovat podle období válku agrárního věku, průmyslového věku a věku informační společnosti. [65] V této souvislosti lze charakterizovat agrární války jako války motivované především územními zisky a charakterizované krvavými střety armád vyzbrojených ručními zbraněmi. To se změnilo s převratnými technologickými změnami v 17. století. Proti sobě válčily národní armády a profesionální vojáci jednotně vyzbrojení standardizovanými zbraněmi. Ekonomická nadvláda, totální porážka protivníka nebo jeho bezpodmínečná kapitulace byly rysem válek průmyslového věku. S nástupem informačních technologií, včetně telefonů, faxů a počítačů však i společnost prodělala zásadní změny. Masovou produkci vystřídala výroba využívající inteligentní technologie a přizpůsobená požadavkům různých trhů. Změnilo se i pojetí války, do výzbroje byla zařazena přesně naváděná munice, autonomní pozorovací prostředky, prostředky elektronického boje, apod. Tato zařízení byla navíc postupně integrována s využitím výpočetní techniky do zbraňových systémů, které dnes přijímají, zpracovávají a vyhodnocují informace z různých zdrojů a ještě je téměř v reálném čase sdílí s dalšími zbraňovými systémy a zařízeními. V tom spočívá síla moderně vybavené armády. Dnešní jednotky jsou včas informovány a nepřetržitě řízeny z velitelských stanovišť. Bojová činnost je proto charakterizována nepřetržitým tokem informací všeho druhu a různého utajení mezi pozemními, vzdušnými a námořními platformami. Významným rysem je i úsilí zabránit zbytečným ztrátám. Toho je možné dosáhnout jedině s využitím informací - kdy zasáhnout, kam zasáhnout a čím zasáhnout. Mohlo by se tak zdát, že informační operace jsou fenoménem informační společnosti a zcela nový způsob vedení boje. To by však byl velký omyl, informační válka není výlučně něco nového, naopak, jak zdůrazňuje Požár, je stará jako válka sama. [102] Získávání informací, jejich interpretace, rozšiřování a provádění protiopatření k zabránění využití informací protivníkem bylo a je klíčovým faktorem vedení války po celou dobu její historie.

INFORMAČNÍ OPERACE V HISTORICKÉM KONTEXTU

Již v desátém století před naším letopočtem zdůrazňoval izraelský král a vojevůdce Šalamoun důležitost získání poznatků o nepříteli (vojenské zpravodajství), řízení (strategické a operační plánování) a poradenství (analýza získaných informací). Jedině ten, kdo si uvědomí tyto tři faktory, může zvítězit ve válce. [135] Ve čtvrtém století před naším letopočtem čínský stratég Sun Tzu (viz. obr. 14) dokonce rozpracoval ve svém díle *The Art of War* tehdejší pojetí informačních operací. [118] Stručně ho lze shrnout do čtyř základních bodů.

1. Informace je nezbytná během procesu pozorování, vyhodnocení situace, rozvoje strategie a pro vyhodnocení alternativních rozhodnutí a s tím spojených rizik.
2. Nejlepší velitelé se odlišují od ostatních tím, že mají zpravodajské informace a na jejich základě jsou schopni vyhodnotit budoucí vývoj operace.
3. Klamání, maskování a využití momentu překvapení může přispět k vítězství. Proto je nutné oklamat protivníka záměrným poskytnutím zkreslených a nepravdivých informací.
4. Nejvyšší formou válečného umění je schopnost využít informací ve svůj prospěch k ovlivnění protivníkovy mysli takovým způsobem, že ztratí vůli k odporu a dobrovolně se podřídí. Vítězství je pak dosaženo bez zbytečných ztrát.

Obrázek 14. Sun Tzu

Zdroj: *Biographical Dictionary*, http://www.s9.com/Biography/Sun-Tzu

Z výše uvedeného vyplývá, že Sun Tzu dokonale pochopil v čem spočívá síla informace, když je k dispozici včas, je správně vyhodnocena a využita v procesu rozhodování. Tento proces se dosud nezměnil a je v současné době nazýván jako zpravodajský cyklus. Sun Tzu tak v podstatě zvládl umění informační války, již před mnoha staletími a dokonce rozpoznal některé typy informačních operací, včetně principů klamání.

Jedním z vojevůdců, kteří prokázali velký talent ke strategické lsti a vojenským dezinformačním trikům byl Hannibal. Jeho vítězství nad římskými vojsky v období 218 až 216 před naším letopočtem bylo spojeno s důmyslnými nástrahami a klamavou taktikou. V bitvě u Kann rozmístil své nejslabší jednotky do středu, nejsilnější na křídla. Střed jeho vojsk se pod úderem Římanů zhroutil, tím je však vlákal do pasti. Hannibalovy křídelní jednotky římskou armádu obklíčily a zničily. Kromě lstí na bojišti používal Hannibal také agenty plynně hovořící latinsky, kteří jeho jednotkám usnadňovali pronikání do měst přes vstupní střeženou bránu. Jeho největší soupeř Quintus Fabius Maximus používal rovněž různé klamné hry, noční manévrování a dezinformační triky. Právě proto byl nazýván „uhýbavý“. Někteří mocní Římané ho neměli v oblibě a označovali ho za zrádce kvůli jeho vyhýbavé taktice. Toho využíval Hannibal, aby je utvrdil v podezření. Kdykoli dobyl nové římské území, ponechal veškeré Fabiovy nemovitosti nepoškozené a ostatní zničil. [11]

Přibližně 1500 po válečníkovi Sun Tzu se proslavili jako mistři informačních operací Mongolové. Využívali mj. obchodníky a velvyslance k získávání informací o svých potenciálních nepřátelích. Ve své době dosáhli dokonalé informační převahy nad všemi svými protivníky, jejich strategické plánování založené na kvalitním zpravodajství nemělo konkurenci. Kromě toho byli i odborníci na psychologickou válku. Využívali jí především ke zlomení odporu obyvatelstva na dobytých územích. Záměrně požívali kruté praktiky, veřejně masakrovali obyvatelstvo a tak šířili strach a ovlivňovali mysl porobeného obyvatelstva, které pak ztrácelo jakoukoliv vůli k odporu. [9]

Informační operace v období před druhou světovou válkou

Příkladů využití některých z typů informačních operací by bylo možné zmínit mnoho. Každá armáda v historii používala maskování a krytí vlastních jednotek před nepřítelem, ať již pomocí kouře nebo využitím přírodních materiálů. Princip byl vždy stejný - vnutit

nesprávné informace protivníkovi tak, aby byl přesvědčen že jsou pravdivé. Rovněž působení na morálku a vůli protivníka i obyvatelstva v dobytých územích praktikovala téměř všechna vojska podobně jako dříve mongolští válečníci.

Za skutečně vojenského novátora a průkopníka nové organizace a taktiky, včetně využívání informací lze považovat Napoleona Bonaparte. Vytvořil hierarchickou organizační strukturu jednotek, která se používá dodnes. [123] Hlavním přínosem z hlediska informačního bylo, že na úrovni divize byly jednotky soběstačné, tvořené všemi druhy zbraní, včetně lehké kavalérie, která působila jako průzkumné a zpravodajské jednotky. [109] Jejich úkolem bylo postupovat skrytě před vlastním vojskem, získávat co nejvíce informací o síle, pohybu a plánech protivníka a co nejrychleji je doručit na velitelská stanoviště. Právě dokonalá akvizice informací a jejich sdílení a využití v rozhodovacím procesu stála, podle některých odborníků, za jeho vítězstvími. Napoleon mohl díky informační převaze zahájit překvapivý útok z místa a v době, kdy to jeho protivník neočekával. Typickým příkladem byly bitvy u Marenga, Ulmu nebo Jeny.

Pozadu za Napoleonem ovšem nezůstali ani jeho protivníci a během války na Pyrenejském poloostrově (1808 až 1814) dokázal anglický vojevůdce Wellington získat nad francouzskou armádou informační převahu. Dokázal vytvořit dokonalou síť zpravodajských důstojníků, získat přesné informace o záměrech a plánech bojové činnosti Francouzů. Výsledkem bylo vítězství Angličanů nad mnohem početnější, avšak informačně hůře zabezpečenou francouzskou armádou. [9]

V době Napoleonských válek se zabýval vojenským uměním i známý švýcarský teoretik a filosof Antoine-Henri Jomini. [116] Přestože se nezabýval přímo informační válkou, jeho přínos vojenské vědě je významný. Jomini byl zjevně ovlivněn Napoleonovými operacemi. Ve svém nejslavnějším díle *Summary of the Art of War* zdůrazňoval, že nejprve je nutné protivníka dokonale poznat, tzn. shromáždit o něm dostupné informace a vyhodnotit je. Ve svém díle se dokonce zmiňuje o provedení kalkulací, tzn. analýzy vojenských informací. Pak teprve lze vést útok na jeho slabé místo. Kromě toho považoval za důležité ovlivňovat morálku vlastních i protivníkových vojsk, tzn. doručit potřebné informace přesně stanoveným uživatelům. V tomto případě se jedná o psychologickou válku. Na rozdíl od něj další vojenský teoretik Karl von Clausewitz [24] nepřikládal využití zpravodajských informací velkou váhu. Považoval je totiž za nepřesné, zkreslující celou situaci. Uznával

tzv. totální válku, kdy je nutné zapojit všechny dostupné síly a prostředky. Tím však připouštěl i nasazení průzkumných a zpravodajských jednotek, jejichž úkolem bylo právě informační zabezpečení. Dokonce považoval za velmi důležité psychologickou podporu bojových operací, tzn. rozvíjel jednu z forem informační války – psychologickou válku.

Během dalšího vývoje a rovněž v průběhu první světové války došlo k útlumu vojenského umění a v té souvislosti i k útlumu taktik, které lze považovat za určité formy informační války. Rozvoj technologií byl rychlejší než organizační a doktrinální změny, proto byla válka převážně statická. Z hlediska informačního došlo k pokroku v oblasti získávání informací, bylo poprvé využito průzkumných letounů. Rovněž se provádělo rozhazování letáků z letounů – distribuce informací novým způsobem, kromě toho sloužily letouny jako prostředek psychologického působení na jednotky v zákopech, tzn. byly využity ve smyslu psychologické války. [123] Tyto praktiky byly využívány až v průběhu druhé poloviny války.

Dobrým příkladem klamání je dezinformační operace proti Stalinovi, kterou provedla ve 30. letech minulého století německá tajná služba s cílem odstranit maršála Tuchačevského. Specialisté nacistické tajné služby SD (Sicherheitsdienst) na přímý rozkaz svého velitele Reinharda Heydricha zfalšovali spisy o spiknutí Tuchačevského proti Stalinovi. Němci chtěli maršála zkompromitovat a odstranit, protože v případě válečného konfliktu by mohl být nebezpečný. Rovněž Stalin toužil po zámince, která by mu umožnila zlikvidovat tohoto nadmíru ctižádostivého a oblíbeného vojevůdce, který kdyby měl úspěch v budoucí válce, se mohl stát jeho rivalem. Spisy o zradě Tuchačevského získal Stalin od československého prezidenta Beneše. Někteří znalci však uvádějí, že údajné spisy od Beneše k likvidaci Tuchačevského pouze přispěly, zatímco usvědčující materiály přišly odjinud. Beneš se, podle Pacnera, *„dozvěděl pravděpodobně od říšskoněmeckého průmyslníka Fritze Thyssena, že německý generální štáb má zprávy, že Tuchačevskij se uchází o jakousi dohodu s německým generálním štábem a byl by ochoten za německé pomoci udělat v Sovětském svazu převrat*“.[99] Dezinformační operace byla z pohledu Německa úspěšná, neboť Stalin dal v červu 1937 Tuchačevského a dalších sedm vysokých důstojníků popravit.

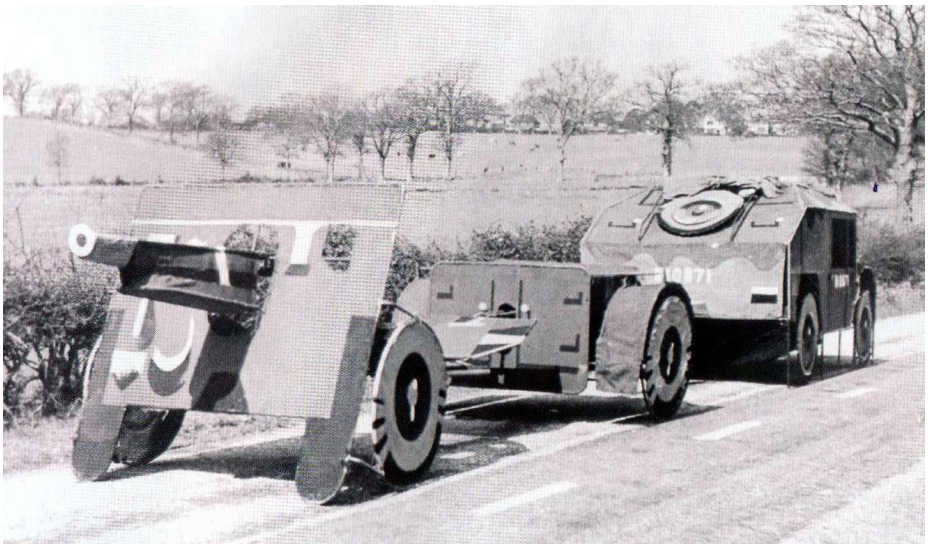
Zkušenosti s dezinformačními a tajnými operacemi mají však i Rusové. Zálibu v nich našli, zdůrazňuje Bittman, ještě dlouho před revolucí roku 1917. Již Lenin v době své

ilegální podzemní činnosti zdůrazňoval, že je důležité tajně pronikat do důležitých vládních a společenských institucí a propagandy a klamného manévrování používat jako součásti strategie komunistické strany. Ve dvacátých letech minulého století založili příslušníci sovětských zpravodajských služeb na území Sovětského svazu v rámci operace „Trust“ fiktivní opoziční organizaci, která postupně navázala kontakt s několika emigrantskými skupinami v zahraničí a také se západními zpravodajskými službami. Pod tímto krytím přiměli stovky oponentů komunistického režimu, aby se začlenili do tohoto hnutí. Postupně pak identifikovali a eliminovali sítě, které západní tajné služby vybudovaly na území Sovětského svazu. Tím získali téměř úplnou kontrolu nad veškerou protisovětskou činností. Opozice, která se do akce zapojila s cílem podkopávat autoritu sovětského režimu se tak stala pouhou součástí dezinformační hry. [11]

Informační operace ve druhé světové válce

Ve druhé světové válce se informační operace rozšířily, díky použití nových technologií do nové oblasti – elektromagnetického spektra. Všechny německé tanky nasazené na východní frontě byly vybaveny rádiovými spojovacími prostředky. Tím získaly Guderianovy tankové jednotky převahu nad početnějšími a mnohdy technicky lepšími sovětskými tanky. Rádiovým spojovacím prostředkem byl u sovětských jednotek vybaven pouze velitelský tank. [9] Opět se projevil význam informace a převaha válčící strany, která informacemi disponovala a mohla je distribuovat uživatelům – v tomto případě tankovým osádkám. Informační operace dokonale ve druhé světové válce zvládli Spojenci během operace v Normandii. Geniální plán Fortitude na oklamání německé armády byl jedním z klíčových faktorů úspěšnosti operace Overlord (vylodění v Normandii). [123] Spojenci rozmístili makety kolové (viz. obr. 15) a obrněné techniky na jihovýchodě Britských ostrovů a navíc u pobřeží shromáždili vyřazená plavidla, která simulovala válečnou flotilu. V prostoru vedli spojenci také klamnou rádiovou komunikaci a simulovali neexistující 1. americkou armádní skupinu (FUSAG). Operace byla navíc umocněna šířením dezinformací diplomatickou cestou a prostřednictvím médií. Německým zpravodajským službám i průzkumným letounům tak byly záměrně předkládány klamné informace z různých zdrojů. Úspěch byl takový, že Němci vůbec nepředpokládali vylodění v Normandii, ale v úžině Pas de Calais. [41]

Obrázek 15. Makety kolové techniky; jihovýchodní Anglie 1943 - 44

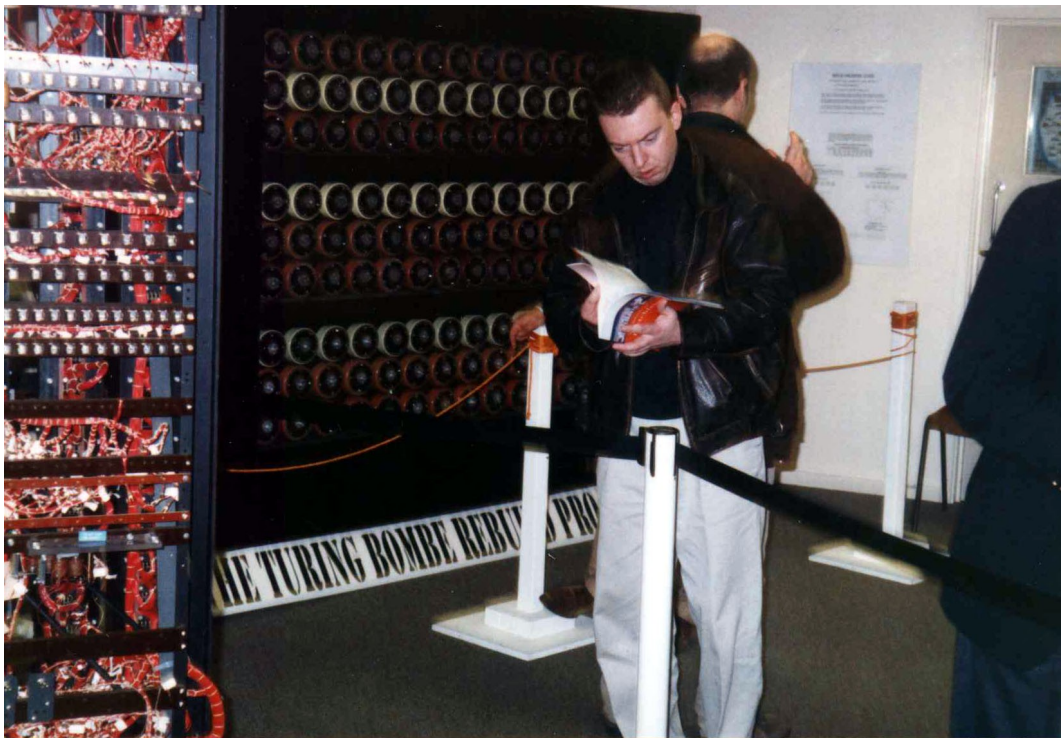


Zdroj: HOLMES Richard. *The D-Day Experience*.

Důležitým momentem z hlediska vojenského i informačního byla skutečnost, že se Britům podařilo úspěšně provést operaci Ultra a prolomit (dešifrovat) německé kódované zprávy, které používali při spojení na operační a taktické úrovni. [124] Jednalo se o prolomení přístroje Enigma pomocí elektromechanického dešifrovacího přístroje Bombe[20] (viz. obr. 16). Získali tím výraznou informační převahu, protože měli informace o německých plánech, přípravě a pohybu jednotek. Operace měla však i druhou stránku věci – ochranu vlastních informací, tedy aspekt obranných informačních operací. Němci totiž nesměli zjistit, a ani skutečně nezjistili, že k prolomení kódu došlo. V praxi to znamenalo připustit určité lidské i materiální ztráty, jinak by nepřítel operaci odhalil. Prolomení německých zakódovaných informací zásadním způsobem ovlivnilo bitvu o Británii a přispělo k porážce Rommelových jednotek v Africe. Kromě toho předávali Britové část takto získaných informací Sovětům ve Švýcarsku v rámci operace pod kódovým názvem Lucy. [123] Sověti tak získali informace o plánovaném útoku na Sovětský svaz (operace Barbarossa) ještě před zahájením, Stalin však tyto informace odmítal jako podvrh.

[20] Přístroj Bombe zkonstruovali Britové podle plánů polských kryptoanalytiků. Název Bombe v tomto případě neznamená pumu či bombu, ale zmrzlinu.

Obrázek 16. Autor práce u modelu "Bombe"; Bletchley Park 2003

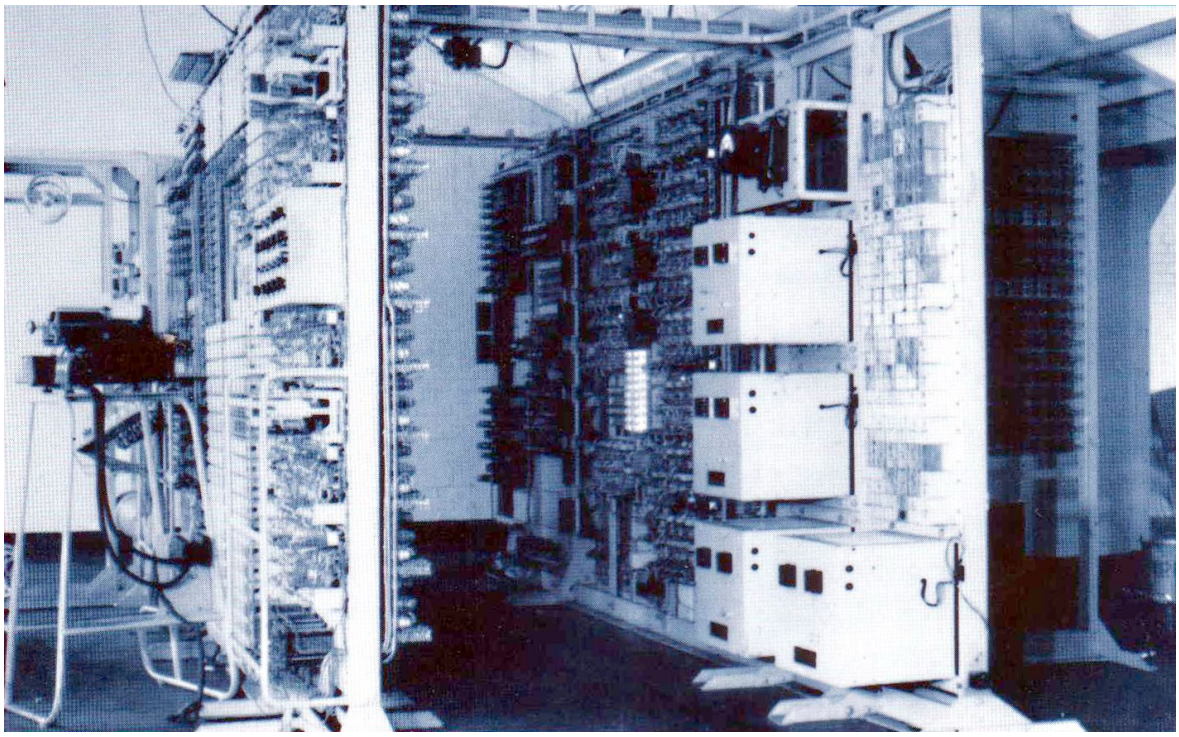


Zdroj: Autorova soukromá sbírka.

Kromě Enigmy dešifrovali Britové i další německý prostředek - Lorenz, který byl používán na strategické úrovni. Pracoval na podobném principu jako Enigma. Z informačního hlediska je důležité, že kromě vlastního dešifrování informací byl v roce 1943 použit, podle Britů, první programovatelný elektronický počítač na světě – Colossus[21] (viz. obr. 17). [124] Později v průběhu války se ještě podařilo Spojeným státům úspěšně dokončit operaci Magic a dešifrovat i japonské zprávy. [123] Tím byla informační převaha Spojenců nad státy Osy dokonána.

[21] Britové se o prvenství v oblasti počítačové techniky přou se Spojenými státy. Ani jedna strana nechce uznat argumenty druhé, zůstává neoblomná a pouze opakuje „důkazy“ proč právě její přístroj je skutečně prvním počítačem, ne pouhým elektromechanickým strojem.

Obrázek 17. Britský programovatelný počítač Colossus



Zdroj: *The Secrets of Bletchley Park*. Souvenir Guide.

Informační operace se pokoušelo vést i Německo, ne však úspěšně. Na grand – strategické úrovni se pokusili realizovat Goebbelsův plán „Nostradamus“ – psychologickou válku a přesvědčit na počátku války britské vedení, že je bez šancí na úspěch. Odpor by prý vedl pouze k rozsáhlým ztrátám na životech a v konečném důsledku by znamenal i rozpad Britského impéria. Operace se nezdařila a naopak britské královské letectvo rozhazovalo letáky na Německem a informovalo obyvatelstvo, že naopak prorok Nostradamus předpověděl pád Německa. [9] Další neúspěšnou německou informací byl pokus využít britského kolaboranta Williama Joyce k přesvědčení obránců Tobruku, aby se vzdali. Výsledkem bylo, jak uvádí Klapálek, že dostal posměšnou přezdívku Lord Haw Haw, když křičel na obránce perimetru „*krysy vylezte ze zákopů a vzdejte se*“. [72]

Ve spolupráci s britskými piloty vedlo, podle některých odborníků informační operace, podle jiných propagandu, i exilové československé vedení v Londýně. Britští piloti rozhazovali nad protektorátem letáky připomínající obyvatelstvu významné dny československé státnosti (viz. příloha č. 3) a tak podporovaly morálku a vůli k odporu. Kromě toho podporovalo finančně a materiálně exilové vedení v Londýně i v Moskvě vydávání periodik u československých jednotek. Vedlo tak systematickou „psychologickou

propagandu“ cílenou na podporu vlastních vojsk. Noviny totiž neobsahovaly jen běžné informace z prostoru jednotek, ale i informace od zpravodajských služeb o aktuálním dění v protektorátu, o rodinách vojáků a o situaci na dalších frontách. [127] Psychologickou podporu jednotek zajišťovalo denně i československé vysílání z Káhiry, [110] pro jednotky na Blízkém východě. Československé rozhlasové vysílání bylo organizováno i z Moskvy, dokonce již od dubna 1939. Komentátor Zdeněk Nejedlý [92] apeloval především na slovanskou sounáležitost a přinášel informace o úspěších Rudé armády na východní frontě. Podporoval tím morálku v protektorátu a zároveň působil proti psychologické válce nacistů, kteří ve sdělovacích protektorátních prostředcích situaci záměrně zkreslovali. Z Londýna zase hovořil v rádiu Jan Masaryk, který se ve svých relacích zesměšňoval nacistické pohlaváry a samozřejmě informoval i o situaci na západní frontě. [81]

Informační operace ve druhé polovině 20. století

V období mezi druhou světovou válkou a začátkem 21. století proběhla řada regionálních konfliktů. Míra využití jednotlivých typů informačních operací v nich byla různá. Z hlediska informačního i vojenského však stojí za zmínku Vietnamská válka. V jejím průběhu používali Americké jednotky samozřejmě psychologickou válku, elektronický boj k rušení komunikace – toku informací mezi piloty severovietnamského letectva a jejich základnou, ale nejvýznamnějším faktem bylo použití přesně naváděné munice. [9] I když její použití není přímo součástí informačních operací, bezprostředně s ní souvisí a z hlediska informačního jde o využití pertinentních informací při navedení této munice[22] na cíl. V této souvislosti nelze nezmínit ani význam médií, které válku ovlivňovaly. Podle Christophera Bellamyho „*Vietnamská válka byla první válka v přímém přenosu*“. [9] Společnost nebyla na takový typ informací připravena a proto jejich dopad, přestože nešlo o informační válku, byl doslova devastující. Protiválečné demonstrace ve Spojených státech negativně působily na psychiku vojáků a negativně ovlivňovaly bojeschopnost jednotek. Do Vietnamu totiž doslova proudil nepřetržitý tok informací o dění ve vlasti. Média v tomto případě vedla psychologickou válku. Z hlediska vojenského není takové tvrzení správné, ovšem z hlediska informačního je zcela na místě.

[22] Někdy bývá také označována jako inteligentní munice. To z důvodu, že se při navádění na cíl může měnit trajektorie jejího letu. Munice se chová „inteligentně“, protože dostává upřesňující informace během letu.

Velmi důležitým mezníkem v historii byla první válka v Perském zálivu „Desert Storm“[23]. Jednalo se, podle Jensena, [65] o válku „třetí vlny“[24], pokud by byla na ozbrojené konflikty aplikována Tofflerova teorie tří vln. Stály v ní proti sobě dvě rozdílné armády. Zatímco irácká vedla klasickou konvenční válku dvacátého století, Spojenými státy vedená koalice vedla informační válku. Přestože koaliční síly kvantitativně Iráčany nepřečíslily, na bojišti dominovaly. Porazily iráckou armádu díky informační technologii. Informace byla poprvé v dějinách hlavní a rozhodující zbraní ozbrojeného konfliktu, koaliční síly měly dokonalou informační podporu díky dobře rozvinuté zpravodajské síti, která dokázala zabezpečit včasné a relevantní informace. Ty byly rozšiřovány k jednotkám pomocí nepřetržitého spojení, které bylo zároveň zabezpečené elektronickými obrannými opatřeními proti zneužití nepřítelem. Zatímco irácké letectvo a protivzdušná obrana byly paralyzovány informační válkou proti místům velení a řízení (použitím elektronického rušení informačního spojení i přesně naváděné munice), koaliční letouny mohly po ovládnutí elektromagnetického spektra ovládnout beze ztrát i vzdušný prostor. [10] Informační technologie v tomto případě zvítězila nad dobře vyzbrojenou armádou „druhé vlny“ během několika týdnů[25].

Odlišnou povahu měly informační operace v Bosně a Hercegovině vedené jednotkami SFOR. Jednalo se totiž o mírovou operaci, ne o bojovou. Informační operace zde vedlo oddělení pro informování veřejnosti (Public Information Office). Jejich cílem bylo ovlivňování veřejného mínění místního obyvatelstva, tedy systematické předkládání informací všem společenským skupinám se záměrem vytvořit příznivé podmínky pro fungování budoucí multietnické společnosti. Jako prostředek působení byly využívány hromadné sdělovací prostředky, včetně televizního a rádiového vysílání státních i soukromých společností. Televizní produkcí SFOR se podařilo pokrýt téměř 70% území. Jednotky SFOR měly čtyři vlastní rádiové stanice vysílající zpravidla 24 hodin denně. Převážnou část vysílacího času tvořily zpravodajské relace. Kromě vlastních stanic se k informačnímu působení využívaly i stanice místní, dále vlastní časopisy SFOR a denní tisk. Důležitá byla také činnost tiskových mluvčích. Zajišťovali informování veřejnosti o situaci v jednotlivých částech země a předcházeli šíření polopravd a pomluv o mezinárodních jednotkách. Dalším informačním prostředkem byly letáky, především k eliminování negativních postojů a projevů obyvatelstva. Podle účastníka mise Josefa

[23] Operace pouštní bouře (1990-91), které se účastnila i československá protichemická jednotka.
[24] Třetí vlnou nazývá Toffler období informační společnosti (předcházelo ho období agrární a průmyslové).
[25] Obvykle se uvádí šestitýdenní letecká kampaň, po které následovala 100 hodinová pozemní operace.

Procházky, však *„měly omezený časový interval působení a naopak dlouhodobý měly plakáty vyzývající obyvatelstvo ke smířlivému postoji k návratu uprchlíků, k odevzdávání nelegálně držených zbraní, k účasti ve volbách, apod*“. [103]

Uvedené příklady jsou vybrané informační operace světového významu. Kromě nich však byla provedena řada méně významných, nebo méně známých operací. Jako příklad lze zmínit československou informační operaci s kódovým označením Neptun ze šedesátých let. Ve spolupráci se sovětskou KGB ji provedl v období 1964 až 1966 tehdejší 8. odbor První správy ministerstva vnitra - dezinformační odbor. V těchto letech zpřístupnila československá vláda oblast šumavských jezer a při této příležitosti plánoval filmový štáb Zvědavé kamery Československé televize ve spolupráci se skupinou sportovních potápěčů natočit pořad o pověstech kolem Černého jezera. Tohoto záměru chtěl využít dezinformační odbor a do jezera vhodit několik beden s nacistickými dokumenty, které potápěči objeví. Takto vyvolaná senzace měla být využita k intenzivní propagandistické kampani proti Spolkové republice Německo. [11] Novinářům a veřejnosti měly být podstrčeny takové informace, které by vyvolaly zájem i zahraničních sdělovacích prostředků. Právě způsob jejich podstrčení nic netušící veřejnosti hrál významnou roli[26] v jejich ocenění. Skupinu potápěčů infiltroval příslušník dezinformačního odboru Ladislav Bittman alias Brychta [98] (viz obr. 18), aby úspěšnost operace byla zajištěna. Nalezené bedny v červnu 1964 však byly ve skutečnosti prázdné nebo naplněné pouhým čistým papírem. Vhodnou náplň – dokumenty totiž v domácích archivech ministerstvo vnitra nemělo. Musely být proto dodány z Moskvy. To se po určitém zpoždění podařilo, ministr vnitra Štrougal uspořádal tiskovou konferenci a domnělé materiály z úřadoven Říšského hlavního bezpečnostního úřadu (RSHA) se dostaly na veřejnost. [12] Vybrané soubory „neptunovských“ dokumentů byly předány velvyslanectvím Spojených států, Velké Británie, Francie a Nizozemska. V důsledku jejich „objevu“ prodloužila také bonnská vláda původní dvacetiletou lhůtu ke stíhání nacistických zločinců o dalších pět let. Mezi další dopady mj. patřilo důkladné „proprání“ některých exponentů sudetoněmeckého hnutí nebo německých poslanců – bývalých příslušníků gestapa nebo SS v tisku. Jak zdůrazňuje Bittman, obětí „neptunovské“ dezinformace však bylo i samo Československo. S výjimkou prezidenta Novotného a ministra vnitra Štrougala totiž nikdo z vládního kabinetu netušil, že šumavský nález je historický podvod. [11]

[26] Pokud by tyto informace nebyly podstrčeny „senzačním způsobem“ – nálezem, pravděpodobně by jim nebyla věnována zdaleka taková pozornost.

Obrázek 18. Ladislav Bittman v akci

Zdroj: BITTMAN Ladislav. *Špionážní oprátky*.

ZÁVĚR

Význam informačních operací rozpoznali vojenští odborníci již dávno před naším letopočtem. Čínský stratég Sun Tzu předběhl svou dobu, když dokázal tehdejší vládce přesvědčit o významu informační nadvlády nad protivníkem. Přestože některé typy informačních operací používali i jeho následovníci, zdaleka nedosahovali jeho důvtipnosti a geniality. Ve středověku se důraz spíše kladl na fyzickou likvidaci nepřítele, což vedlo ke krutým konfliktům se ztrátami na straně vítězů i poražených. Význam informací a sílu informační nadvlády si uvědomil Napoleon Bonaparte, což byla cesta k jeho vítězným tažením. Získání a vyhodnocení informací o protivníkovi v kombinaci s využitím klamání a momentu překvapení bylo mj. klíčovým faktorem i při jeho vítězství ve známé bitvě u Slavkova. [123]

Informační operace byly dlouhou dobu používány pouze jako podpůrný prostředek ke konvenčnímu vedení války. V první světové válce bylo např. použito rozšiřování letáků vyzývající vojáky protivníka k zanechání odporu. Skutečného rozmachu se dočkaly až za druhé světové války, kdy byly klíčovým faktorem mj. v bitvě o Británii nebo při vylodění spojenců v Normandii. Přestože byly informační operace rozvinuty v nebývalém rozsahu, pronikly do elektromagnetického spektra a byly využívány různé typy operací, včetně rozšiřování informací k psychologickému ovlivnění občanů protektorátu a byly

v maximální míře používány techniky klamání, stále se jednalo o podporu bojových operací. Nový fenomén se objevil za války ve Vietnamu, z hlediska vojenského měla přínos přesně naváděná munice, která byla závislá na dodaných informacích; z hlediska informačního se projevila síla médií. Jak se ukázalo, právě informace v rukou médií měly rozhodující vliv na morálku jednotek a následně i na úspěchy vojenských operací. Válka v přímém přenosu předběhla dobu a ani politici, ani vojenští velitelé nebyli na tento nový jev připraveni.

Za historicky první ozbrojený konflikt, který je možné nazvat informační válkou lze považovat první válku v Perském zálivu – operaci Pouštní bouře. Ovládnutí informačního spektra vedlo k nadvládě koaličních jednotek na vzdušném i pozemním bojišti a k úplné eliminaci irácké obrany. Vítězství dosáhla kvalitativně vyspělejší válčící strana nad kvantitativně silnějším protivníkem. Zvláštní, a dosud ne zcela zvládnutou problematikou jsou informační operace v podmínkách mírových misí. Důraz je kladen zejména na rozšiřování informací mezi obyvatelstvo vhodnou formou. Cílem je psychologické ovlivnění populace. Protože se jedná o nebojovou operaci, nelze k dosažení cíle použít silové prostředky. Právě proto má informační operace v těchto podmínkách prioritu.

. SOUČASNÉ INFORMAČNÍ OPERACE

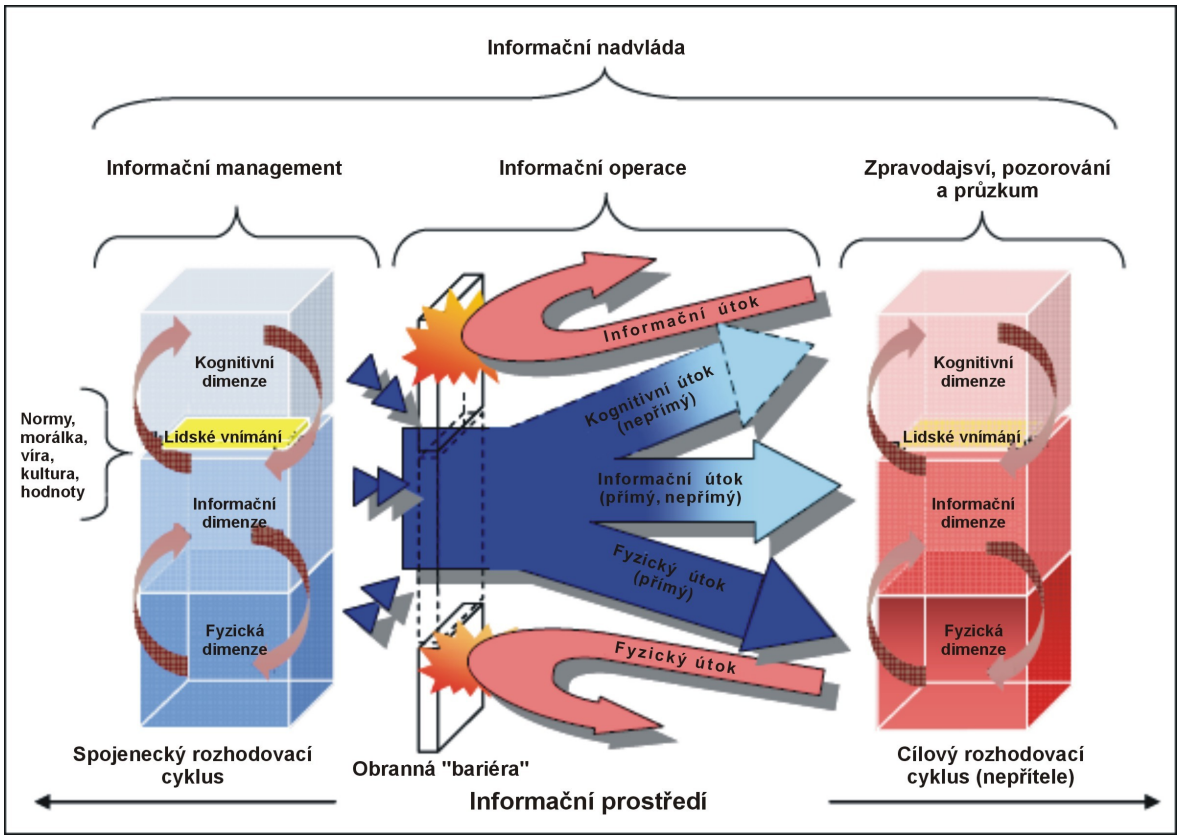
ÚVOD

Informační operace jsou v současné době nedílnou součástí jakýchkoli vojenských kampaní. Vlastnímu plánování informačních operací předchází zhodnocení celkové situace, tzn. vyhodnocení dostupných informací o protivníkovi, geografických, klimatických a případně i demografických podmínkách bojiště. Cílem je vytvořit virtuální obraz bojiště, který by se co nejvíce podobal reálné situaci. V případě, že se bude jednat o bezpečnostní operace, jejichž cílem je nastolit demokratickou vládu v zemi a zajistit jí podporu, tzn. že bojové operace budou mít omezené trvání, pak bude samozřejmě nezbytné vyhodnocení i politické a ekonomické situace. Teprve na základě těchto poznatků je možné naplánovat informační operace. V případě zanedbání tohoto kroku by pravděpodobně jejich úspěšnost by byla velmi omezená nebo dokonce žádná. Podle aktuální situace je nutné zvolit příslušný typ informační operace a vyčlenit na něj vlastní síly a prostředky. V současné době by měly informační operace plnit, jak uvádí Bloom [14], zejména tyto funkce:

- Odstrašovat, omezovat a usměrňovat protivníka, a tím narušovat jednotu jeho velení a jeho záměry, a to při zachování vlastního záměru.
- Chránit vlastní plány a zmařit plány protivníka, což umožní soustředit účinky pro dosažení maximální výhody, zatímco protivník spotřebuje svoje prostředky s malým účinkem.
- Ovládnout spojení a sítě protivníka, a to při ochraně vlastního spojení a vlastních sítí, a tím ochromit možnost protivníka řídit organizovanou obranu a zachovat účinné velení vlastním silám.

V obecném pojetí lze tyto funkce shrnout do srozumitelnější formulace - získání informační nadvlády nad protivníkem (viz. obr. 19), zabránit mu šíření jeho informací a zároveň zajistit vlastní nepřetržitý informační tok. Kromě toho se předpokládá i informační působení na místní obyvatelstvo.

Obrázek 19. Informační nadvláda



Zdroj: Upraveno a převzato z *Information Operation Primer*, http://www.carlisle.army.mil/usacsl/publications/IO-Primer-AY06.pdf

OPERACE V KOSOVU

V průběhu zimy 1999 zvýšila používání násilných prostředků tehdejší jugoslávská vláda proti kosovským Albáncům do takové míry, že hrozilo vypuknutí humanitární krize. Ta by pravděpodobně dosáhla takových rozměrů, že by destabilizovala bezpečnostní situaci na celém Balkáně. [30] V této situaci se Aliance rozhodla zasáhnout. Do oblasti nebyly vyslány pozemní jednotky, protože hrozily značné ztráty na životech, byla však provedena letecká kampaň – vzdušné údery proti vybraným cílům. Cílem bylo zastavit ozbrojené akce proti Albáncům, které posoudilo mezinárodní společenství jako nelegální a donutit Miloševiče stáhnout vojenské jednotky z Kosova. [123]

Informační operace před kampaní a v průběhu kampaně

Severoatlantická aliance vedla propagační kampaň v souvislosti s Kosovem ještě v letech před vypuknutím konfliktu. Plánování a příprava informační strategie probíhala současně s plánováním letecké kampaně. Informační operace byla zaměřená proti Miloševičově vládě. Jejím cílem, před zahájením vzdušných úderů bylo, jak zdůrazňuje Tiina Seppälä, prezentovat veřejnosti prezidenta Miloševiče a jeho příznivce, včetně jugoslávské armády jako agresora a překážku demokratických změn v Evropě. [115] Jednalo se tedy z informačního hlediska o šíření informací, které mělo vyvolat u veřejnosti negativní smýšlení o jugoslávské vládě. V této souvislosti je nutné podotknout, že úsilí bylo v této fázi zaměřeno hlavně na „evropskou veřejnost“, ne na srbské obyvatelstvo. Aliance zdůrazňovala odpovědnost mezinárodního společenství za události a rovněž již předem oznamovala, že případný zásah bude legitimní a jak dodává Haines, v souladu s mezinárodním právem. [49] Po zahájení kampaně byla celá operace medializována, aby veřejnost mohla sledovat její průběh „v reálném čase“.

Jednalo se tedy o využití zejména psychologických operací, jako jednoho z typů informačních operací. Na strategické úrovni byli cílem těchto operací političtí představitelé, na operační a taktické úrovni srbské vojenské jednotky a místní obyvatelstvo. Tiina Seppälä uvádí pět hlavních záměrů psychologických operací v Kosovu [115]:

- Přesvědčit o legitimitě zásahu NATO; cílovou skupinou těchto informací bylo zejména obyvatelstvo spojeneckých zemí a zemí neutrálních.
- Zdůraznit vojenskou převahu NATO; tyto informace byly určeny srbským jednotkám a srbskému obyvatelstvu se záměrem podlomit vůli jakkoli vzdorovat Alianci.
- Ukázat celkovou převahu Aliance, která má podporu mezinárodního společenství. Jednalo se o informace určené především srbské vládě, která se tak měla cítit osamocená a zodpovědná za lidské oběti v případě, že se postaví na odpor.

- Přesvědčit veřejnost, že za násilí v Kosovu a následný úder proti Srbům je odpovědný Miloševič. Záměrem těchto informací bylo omezit podporu Miloševiče u srbského obyvatelstva.
- Přesvědčit veřejnost, že jedinou možností je vzdát se a neklást odpor mezinárodním jednotkám. Tyto informace byly určené k demoralizaci srbského obyvatelstva a armády.

V průběhu leteckého úderu používaly alianční letouny grafitové pumy k paralyzování infrastruktury, zejména k přerušení dodávek elektrické energie. Jejich použití lze, jak uvádí William Church, rovněž považovat za součást informačních operací, protože cílem bylo vystupňovat tlak na politické vedení, aby rezignovalo. [22] Další kampaní byla rozsáhlá hackerská válka proti jugoslávské protivzdušné obraně s cílem potlačit její bojové kapacity tak, aby nebyla ohrožena bezpečnost aliančních letounů. Kromě toho obě strany, Aliance i Jugoslávie, vedly rozsáhlou psychologickou válku. Ta se neomezovala v případě NATO na šíření letáků a mediální působení, ale byla kombinovaná i s hackerskou válkou proti webovým doménám. Tímto způsobem byly mj. rozšiřovány informace (nepravdivé) o zahájení pozemní kampaně NATO. O vedení hackerské války se pokoušela i Jugoslávie, větší úspěch však měla v psychologické válce. Velmi dobře byl mj. hodnocen z psychologického hlediska (a tedy i informačního) krátký propagační videozáznam o připravenosti druhů vojsk jugoslávských ozbrojených sil k obraně státu, který vysílala jugoslávská televize bezprostředně před zahájením konfliktu, a který mj. odvysílala v roce 1999 i Česká televize.

Jednou z psychologických operací, kterou provedly americké zpravodajské služby s cílem oslabit domácí podporu Miloševiče, bylo šíření zpráv o švýcarských kontech prezidentova syna. Tyto, i další dezinformace o jeho synovi byly šířeny zejména prostřednictvím novinářů. Měly za cíl v pravé chvíli poukázat na finanční situaci a životní úroveň prezidentské rodiny v době, kdy prezident vyzýval strádající obyvatelstvo k podpoře vládní politiky.

Informační operace jednotek KFOR

Součástí působení jednotek KFOR v Kosovu je vedení informačních operací. Jedná se zejména o psychologické operace. Vzhledem k tomu, že v prostoru operace žijí dvě odlišné národnostní komunity – Srbové a Albánci, informační operace jsou zaměřené na posilování myšlenky vzájemné tolerance a soužití v multietnické prostředí. Cílem je vysvětlit oběma etnikům, že jedině tato cesta může vést k lepším životním podmínkám a zlepšení bezpečnostní situace. Jednotky zodpovědné za vedení psychologických operací, tzv. týmy PSYOPS šíří tyto informace prostřednictvím rádiového vysílání, časopisů, plakátů, letáků a komerčních televizních stanic. [103]

Během svého působení musely týmy PSYOPS čelit, zejména po zahájení mise, určitým skupinám obyvatelstva, které měly k psychologickým operacím koaličních jednotek negativní postoj. Jednalo se, podle Davisové, o tři skupiny obyvatelstva. První byly srbské obranné organizace, jejichž posláním bylo chránit kosovské Srby. Při spolupráci s koaličními jednotkami usilovaly pouze o prosazování svých zájmů a odmítaly jakékoli návrhy na spolupráci a soužití. Vůdčí představitelé těchto organizací, jak dále uvádí Davisová, „*se vyznačovali velmi antagonistickým postojem k Albáncům a rétorikou buď my nebo oni*“. [30] Jejich postoj se podařilo změnit a kosovští Srbové se zapojili do práce v kosovských vládních institucích. Druhou skupinu obyvatel tvořily skupiny organizovaného zločinu. Neměly zájem na úspěchu NATO v Kosovu a stabilizaci bezpečnostní situace, což by jim znemožnilo činnost. Snažily se proto šířit nepravdivé informace o působení koaličních jednotek, o potlačování civilistů a obětech na životech. Třetí skupinou byly nacionalistické albánské organizace, které šířily v médiích informace o nutnosti separace a vytvoření albánského státu.

V souvislosti se snahou některých skupin obyvatelstva šířit negativní informace o jednotkách KFOR je nutné vést i obranné informační operace. Jsou namířené proti vedení propagandy prostřednictvím zejména regionálních a místních sdělovacích prostředků. Zahrnují rozšiřování informací o skutečném stavu v jednotlivých oblastech provincie pomocí vlastních informačních produktů a místních médií, rovněž osobní setkání s místními vedoucími představiteli. K obranným informačním operacím patří také zvýšené hlídkování v dané lokalitě s cílem demonstrovat svoji přítomnost a psychologicky působit na obyvatelstvo. [108]

OPERACE V IRÁKU

Na rozdíl od Kosova byla v Iráku provedena letecká i pozemní operace a došlo k bojovému střetnutí koaličních a iráckých jednotek. Z hlediska vojenského je invaze do Iráku považována za tzv. preventivní válku[27]. Cílem bylo donutit iráckou vládu, aby respektovala rezoluce Rady bezpečnosti OSN a odstranit z vlády tehdejšího prezidenta Saddáma Husajna. Spojené státy totiž podezřívaly irácký režim, že vyvíjí zbraně hromadného ničení. V médiích byla vedena masová propaganda o tajném iráckém zbrojním programu. Zda šlo o omyl, nebo dobře vedenou psychologickou operaci zaměřenou na mezinárodní společenství, není zcela jasné. Z hlediska informačního však mediálně prezentované informace měly nesporně požadovaný dopad na veřejnost, která převážně souhlasila s invazí do Iráku.

Operace Irácká svoboda

Ještě před zahájením operace v březnu 2003, zahájily Spojené státy masivní informační operaci – proti iráckým obyvatelům a proti příslušníkům iráckých ozbrojených sil. Od ledna 2003, kdy probíhaly poslední přípravy k zahájení bojových operací probíhala psychologická operace prostřednictvím emailové pošty. [82] Tomu předcházela zpravodajská operace, jejímž úkolem bylo zjištění co největšího množství privátních emailových adres. Záměrem bylo zlomit odpor irácké armády ještě před zahájením operace a přesvědčit irácké obyvatelstvo o nutnosti odstranění Husajna. Pravděpodobně byla ještě před operací vedena rovněž kybernetická válka proti iráckým jednotkám s cílem paralyzovat velení. Veřejně přístupné informace však o ní nejsou zatím k dispozici.

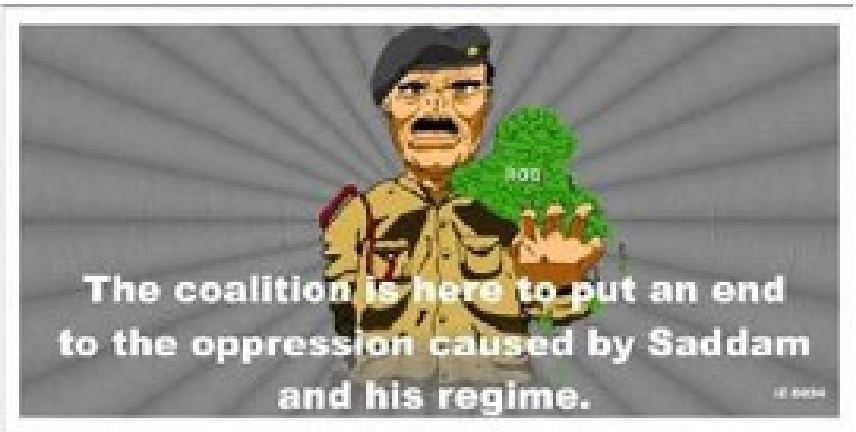
Současně se zahájením bojové operace 19. března 2003 zahájily americké jednotky i informační operaci - na vojenských rádiových frekvencích proti příslušníkům iráckých jednotek. Vysílání mělo ovlivnit irácké vojáky a přimět je ke kapitulaci. Jak uvádí Joseph Cox, zároveň s těmito akcemi „*provedly americké bojové letouny vzdušný úder na farmu, kde v té době měli pobývat Husajn a jeho dva synové*“. [29] Ten lze považovat za informační operaci proti místům velení na strategické úrovni, protože Husajn řídil jako

[27] Preventivní válka, tzv. pre-emptive war. Čeština má bohužel stejný výraz i pro preventive war nebo anticipatory war. Z hlediska mezinárodního práva se však jedná o zcela rozdílné vojenské konflikty, respektive preventivní zásahy.

vrchní velitel operace iráckých ozbrojených sil. Z hlediska informačního se jednalo o snahu přerušit informační tok od nejvyššího stupně řízení k podřízeným prvkům.

Kromě psychologického působení na irácké vojáky vedly koaliční jednotky rovněž psychologickou operaci zaměřenou na irácké obyvatelstvo. Americké letouny (Commando Solo, Compas Call a Prowler) vybavené prostředky EB byly schopny působit nejen proti iráckým místům velení, ale i pokrýt rádiovým a televizním vysíláním téměř 90 % iráckého území. Další letouny shazovaly před zahájením a v den zahájení operace letáky (viz. obr. 20) oznamující, že koaliční jednotky přijely skoncovat se Saddámem a jeho represivním režimem. Celkem jich bylo shozeno více než 40 milionů. [25]

Obrázek 20. Leták shazovaný z letounů při zahájení operace Irácká svoboda



Zdroj: COLLINS Steven. Mind Games.

Spojené státy očekávaly hackerské útoky Iráčanů na vojenské systémy a vládní instituce jako pokus o odvetu, nic takového se však nestalo. Jak se později ukázalo, irácká „internetová infrastruktura“ byla zastaralá a podobné útoky, podle McWilliamse, neumožňovala. [82] V průběhu března byla navíc fyzicky poškozena (informační válka pomocí fyzického působení) údery leteckých pum.

Během operace Irácká svoboda působil spolu s pozemními koaličními jednotkami v Iráku rovněž 600členný „novinářský kontingent“. Jeho úkolem bylo zabránit šíření dezinformací, zveřejňovat fakta o skutečném stavu koaličních jednotek, hlavně jejich bojových kapacitách; poskytovat veřejnosti reálný obraz bojiště a předcházet falešným informacím o ztrátách na civilním obyvatelstvu. [100] Z hlediska vojenského dosavadní koncept informačních operací takovou akci nepostihuje, mezi odborníky panují spory, zda se jedná

o typ informační operace, nebo ne. Z informačního hlediska šlo o informační podporu vojenské operace s cílem psychologicky ovlivnit veřejnost.

Informační podpora bezpečnostní operace v Iráku

Po oficiálním ukončení válečného konfliktu v Iráku sice pokračují bezpečnostní operace téměř na celém území, ale protivníkem jsou nyní iráčtí povstalci, ne irácká armáda. Z vojenského hlediska je tato situace, tzv. období konfliktu s nízkou intenzitou, mnohem složitější. Cílem je odhalit protivníka a potlačit jeho schopnost vést útoky proti koaličním a iráckým vládním jednotkám. [38] Povstalci se však dokáží vmísit mezi civilní obyvatelstvo, používají taktiku guerillového boje a zpravidla se vyhýbají přímé konfrontaci s početnějšími a mnohem lépe vyzbrojenými koaličními jednotkami. V této situaci se mění nejenom plánování a vedení vojenských operací, ale i informačních operací. Účinnou formou jsou především psychologické operace. Americký informační důstojník Norman Emery zdůrazňuje, že „*nejdůležitější je ovlivnit irácké kmenové vůdce, překonat jejich národní pýchu a přesvědčit je o nezbytnosti dočasného rozmístění koaličních jednotek v jejich zemi*“. [38] Cílem je získat spojence z řad místního obyvatelstva v boji proti povstalcům. Nejsložitější je podat jim přesvědčující informace a potlačit protiamerický postoj. Úspěch byl zaznamenán mj. v provincii Anbár, kde se na stranu koaličních a vládních jednotek postavilo přibližně 30 tis. bojovníků z místních kmenů. [56]

Dalším úkolem psychologických operací je ovlivňování obyvatelstva, aby neposkytovalo pomoc a zázemí povstalcům, ale naopak spolupracovalo s koaličními jednotkami. Podávané informace musí být srozumitelné a musí informovat i o stavu koaličních jednotek. I zdánlivě nepodstatné věci, jako např. vysvětlení použití přístrojů pro noční vidění, hrají v Iráku důležitou roli. Povstalci totiž šířili dezinformace o schopnosti pozorovat pomocí těchto přístrojů irácké ženy, což je v muslimské zemi zcela nepřípustné. [29]

Vláda Spojených států, uvádí americký generál Rendon v rozhovoru pro časopis *Rolling Stone*, si byla hned o začátku operací v zemi vědoma důležitosti získat Iráčany na svojí stranu, a proto rozhodla o vedení PSYOPS všemi dostupnými prostředky. Jedná se především o rádiové a televizní vysílání, ale i rozesílání krátkých textových zpráv na

mobilní telefony a šíření zpráv prostřednictvím internetu. [8] Podle amerického deníku Washington Post dokonce vyčlenily v roce 2005 Spojené státy finanční prostředky v hodnotě několika set tisíc USD na opravy a modernizaci zařízení vybraných irácký televizních stanic. Rovněž pronajímají část vysílacího času komerčních televizí k vysílání pořadů, které pozitivně hodnotí podíl koaličních jednotek na obnově místní infrastruktury. [44]

OPERACE V AFGHÁNISTÁNU

Operace v Afghánistánu s kódovým názvem Trvalá svoboda byla zahájena v říjnu 2001 s cílem podpořit afghánskou vládu a Severní alianci v boji proti hnutí Talibán, které ovládlo téměř celou zemi a poskytlo území Afghánistánu jako základnu teroristické skupině al-Káida. Jednalo se tedy o pomoc místní vládě proti povstaleckému hnutí, které sice ustanovilo svojí vlastní vládu, ale ta nebyla mezinárodním společenstvím nikdy uznána jako legitimní. Z hlediska vojenského a mezinárodního práva, byl vojenský zásah legitimní, protože al-Káida představovala reálnou hrozbu a rozsah útoku 11. září 2001 lze považovat, co do rozsahu škod, za vojenský, i když nebyl proveden vojenskými prostředky. [112] Talibán na výzvy vydat organizátory útoku (představitele al-Káidy) a zastavit jim podporu nereagoval, proto zbývala poslední možnost – vojenská podpora svržené vlády.

Informační operace k podpoře vojenské operace Trvalá svoboda

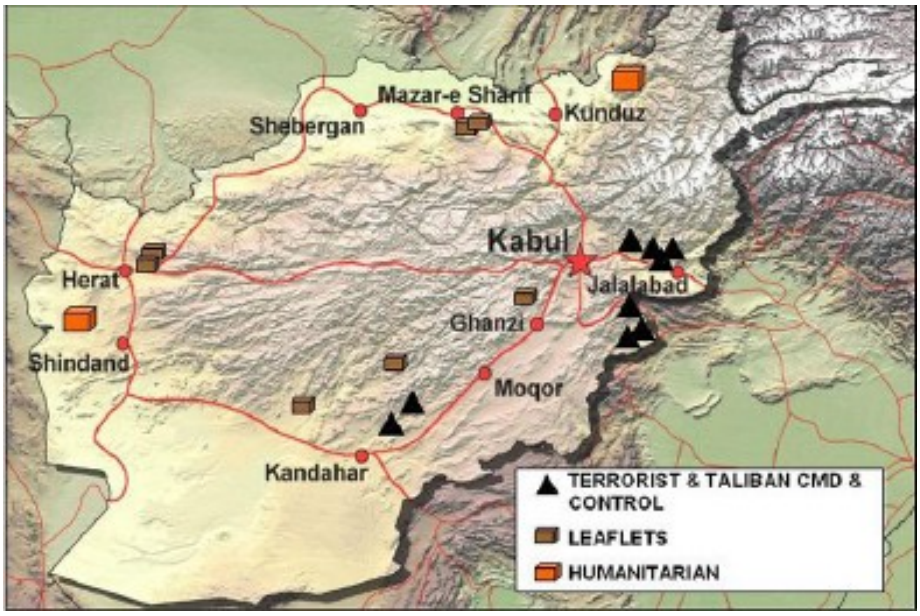
Celou operaci bylo nejprve potřeba medializovat, aby získala podporu veřejnosti. Bylo nutné zdůraznit, že koaliční jednotky provádí útoku proti Talibánu s využitím přesně naváděné munice, aby byly minimalizovány civilní ztráty. Dále bylo nezbytné, jak uvádí Cox, v médiích prezentovat, že původní vláda, které koaliční jednotky pomáhají, nepodporuje teroristické skupiny. Po zahájení pozemních operací začaly koaliční jednotky masivní informační kampaň oznamující, že americké a britské jednotky vstoupily na území Afghánistánu. Psychologická operace dále zahrnovala shazování informačních letáků (viz. příloha č. 4) a rozhlasové vysílání z amerických letounů. Šířené informace vyzývaly obyvatele k zastavení podpory Talibánu, oznamovaly zahájení humanitární pomoci

a rovněž žádaly Afghánce o poskytnutí informací, které by vedly k zadržení velitelů Talibánu a al-Káidy. [29]

Talibán a spřízněné povstalecké skupiny však kontrovaly protikoaličními informačními operacemi, a jak uvádí Davisová, „*vyzvaly naopak afghánské obyvatelstvo ke svaté válce proti Američanů a jejich spojencům*“. [30] Výzvy šířili povstalci skrytě, pomocí tzv. nočních dopisů, způsobem, který je paradoxně naučila americká Ústřední zpravodajská služba v 80. letech minulého století. Navíc se pokoušeli finančně motivovat obyvatelstvo a vypisovali odměny za eliminaci koaličních vojáků a humanitárních pracovníků. To mělo negativní psychologický dopad na koaliční vojáky i zaměstnance humanitárních organizací. Talibán působil na obyvatelstvo i rádiovým vysíláním, především z kábulské rozhlasové stanice „Hlas šarií“. Tu však koaliční letouny v listopadu 2001 umlčely. [115]

Kromě psychologické informační kampaně zaměřily koaliční jednotky prostředky EB na místa velení Talibánu (viz. obr. 21). Současně s elektronickým rušením byly provedeny letecké údery k eliminaci prostředků protivzdušné obrany, které padly do rukou talibánských bojovníků. V omezené míře byla vedena v roce 2001 i kybernetická válka a hackerská válka, namířená proti finančním institucím, které podporovaly talibánce a proti pro-talibánským serverům. Jedním z cílů bylo získat z těchto serverů a institucí informace, které by vedly k zadržení talibánských velitelů. [30]

Obrázek 21. Místa velení Talibánu, prostory shazování letáků a humanitární pomoci; podzim 2001



Zdroj: COX Joseph. *Information Operations in Operations Enduring Freedom and Iraqi Freedom – What Went Wrong?*

Informační operace Talibánu

Od ledna 2006 převzala od Spojených států zodpovědnost za vedení bezpečnostních operací v Afghánistánu Severoatlantická aliance. Operace by se měla zaměřit více na obnovu infrastruktury, realita je však taková, že je nutné čelit zvýšenému počtu ozbrojených útoků Talibánu. Obyvatelstvo není spokojené s vládou, protože dosud nesplnila hlavní slib – zlepšení bezpečnostní situace. Toho talibánci dokonale využívají k vedení psychologické války. K šíření ovlivňujících a zastrašujících informací používají různé způsoby. Kromě výhružných letáků[28] se v Afghánistánu používá, podle ústního sdělení bývalého příslušníka mise Přemysla Horáčka, ve velké míře nápisů na zdech. Ty namalují v noci na zeď domu, kde bydlí představitelé místní správy, policie nebo další vládní úředníci. Mají výhružný charakter a jejich cílem je oslabit centrální vládu a destabilizovat bezpečnostní situaci v zemi. [54] Dalším často používaným prostředkem jsou, uvádí Horáček, „*mobilní telefony, které se šíří v Afghánistánu neočekávaně rychle, že jejich počet v zemi nelze v současné době ani odhadnout*“. Slouží k rozšiřování výhružných zpráv, hrozeb fyzickou likvidací a únosem příbuzných.

[28] V Afghánistánu nepoužívá Talibán klasickou formu letáku, ale tzv. „motáky“ – papír, nebo kus látky svinutý do malé roličky, který nerozhazují jako koaliční letouny po zemi, ale cíleně je zastrkují do oken nebo dveří v nočních hodinách.

V zemi se informace šíří dnes netradičním způsobem – ústním předáváním informace. Nákladní automobily převážející zboží a koňské povozy slouží zároveň jako dopravní prostředek, kam neustále někdo nastupuje a vystupuje. Cestující si neustále předávají informace o situaci v oblastech odkud pocházejí, nebo informace, které slyšeli. Kromě běžné konverzace si takto, jak dále uvádí Horáček, předávají informace i talibánci - jak o rozmístění a stavu koaličních jednotek, tak i o poloze, shromaždištích a síle vlastních ozbrojených skupin. Tento způsob předávání informací sice lze označit z vojenského hlediska jako „low- tech“[29], ale je velmi účinný a prakticky nepostižitelný. Informační válka Talibánu je dnes natolik propracovaná, že Horáček uvádí osobní zkušenost, s výhrůžkami rodinným příslušníkům vojáků vyslaných do Afghánistánu a žijících v západní Evropě. K těmto psychologickým operacím využívá Talibán své agenty působící mimo území Afghánistánu.

Informační operace jednotek ISAF

Snahou koaličních jednotek je především podpořit vybudování bezpečnostních složek, infrastruktury a podpora afghánské vlády. Země má sice vládu Karzáího, vzhledem ke zkorumpovanosti však nemá silnou pozici. Cílem je proto posílit vládní pozici a pomoci jí získat respekt. V této souvislosti je nutné, uvádí Horáček, „*monitorovat a podporovat právě ty členy vládního kabinetu a významné provinční představitele, kteří zastávají nekompromisní postoj proti Talibánu*“. Jedná se o tzv. měkký, nebo-li neletální targeting[30]. Vybrané cíle – vládní úředníky je nutné buď podporovat, nebo diskreditovat a donutit je odejít z politické scény. Obojí se provádí záměrným šířením informací, zejména sdělovacími prostředky. Pokud tato nenásilná forma nepomáhá, používá se anonymních zastrašujících informací, např. ve formě krátkých textových zpráv zasílaných na privátní mobilní telefony. [54] Obecně řečeno jedná se psychologické operace kombinované s propagandou k ovlivnění vládních představitelů.

[29] Low-tech = Low technology, tj. nízká technologická úroveň. Jak se však ukazuje vyspělé technologické systémy mají problémy efektivně působit proti prostředkům na nízké technologické úrovni, protože nebyly za tímto účelem vyvíjeny.

[30] Targeting je označování cílů. Ve vojenské terminologii se však stále častěji používá anglický termín. Označení cílů slouží, v případě „normálního“ targetingu k jejich přesnému zaměření a následné likvidaci, zpravidla vzdušným úderem.

Ovlivňování politických špiček samozřejmě nestačí, proto vedou koaliční jednotky i psychologické operace k ovlivňování obyvatelstva. To se provádí jednak pomocí shazovaných letáků, rádiovým vysíláním (předplacený vysílací čas u komerčních rádiových stanic), ale jak zdůrazňuje Horáček, také nasazením automobilů vybavených zvukovým zařízením – amplionem. Kromě toho se používá i „zdokonalených letáků" – jednoduchých, odolných tranzistorových přijímačů s pevně naladěnou frekvencí, které jsou shazovány z letadel a po dopadu se sami aktivují. [54] Protože koaliční vysílání probíhá u komerčních stanic na určité frekvenci je součástí IW také informovat o ni nenásilnou formou, aby úsilí nebylo kontraproduktivní. To se provádí mj. shazováním letáků s rádiovou frekvencí (viz. příloha č. 5), rozdáváním čepic nebo triček s nápisy v afghánských nářečích, aby byly pro místní obyvatelstvo srozumitelné.

Kromě těchto nenásilných způsobů informační války se však někdy musí použít k psychologickému nátlaku i demonstrace síly. Tento způsob se provádí v situacích, kdy je nutno usměrnit jinak nezvládatelný dav. Podle Horáčka má tato psychologická operace dva aspekty. Nejdříve dojde k záměrnému šíření dezinformací např. o místním starostovi, protože odmítá dostatečně spolupracovat s koaličními jednotkami. V okamžiku, kdy dojde k nepokojům místního obyvatelstva, nechá se situace vystupňovat až do okamžiku, kdy dav fyzicky téměř ohrožuje daného vládního úředníka (ten samozřejmě o pozadí operace nesmí vědět). V této situaci demonstrují, zpravidla koaliční letouny extrémně nízkým průletem, svoji přítomnost a sílu. Dav je paralyzován a šokován, vládní úředník zavázán koaličním jednotkám a ochoten např. poskytnout informace o pozicích Talibánu. [54] Jedná se o jeden příklad, existují však i další způsoby vedení psychologických operací.

ZÁVĚR

Informační operace v současné době vedou koaliční jednotky ve všech krizových oblastech. Kosovo, Irák a Afghánistán jsou nejznámější a z hlediska nutnosti vyřešení nejdůležitější krizové oblasti ve světě. Zahájení bojových operací bez předchozího zahájení informační kampaně si již dnes nelze představit. V této fázi se uplatňuje hackerská válka, kybernetická válka a především psychologická válka. V okamžiku zahájení bojových operací je nutné vést válku proti místům velení a elektronický boj proti systémům protivzdušné obrany. Ekonomicko-informační válka provází každé politické napětí,

v případech jako byl např. Afghánistán pod vládou Talibánu, však nemá požadovaný účinek. Zpravodajské působení je běžnou součástí každé operace, kde jsou nasazeny ozbrojené síly. Konkrétní informace o této činnosti však nebývají veřejnosti přítomné.

Zkušenosti z dosavadních operací dokazují, že význam informační válka stále roste. V době po oficiálním ukončení bojových operací, v této souvislosti myšleno války, jako např. v Iráku nebo v Kosovu mají informační operace větší a dlouhodobější účinek než dílčí bojové operace zaměřené na ohniska odporu. Při nich lze sice eliminovat povstalce a „vyčistit oblast“, účinek je však krátkodobý a v případě civilních ztrát dokonce kontraproduktivní. Po stažení koaličních jednotek se povstalci infiltrují zpět do oblasti a mají podporu místního obyvatelstva. V této souvislosti jsou důležité zejména psychologické operace, jejichž záměrem je ovlivnit obyvatelstvo a získat ho na vlastní stranu. K tomu slouží nejlépe sdělovací prostředky. Proto je nezbytné již v počáteční fázi operace umlčet rádiové a televizní vysílání protivníka. Vzdušné údery byly proto provedeny na rádiové i televizní vysílače v Srbsku, Iráku i v Afghánistánu. V Kábulu byla dokonce zlikvidována vysílací stanice katarské televize Al-Jazeera, která je považována za „CNN arabského světa“. [115]

Předpokladem úspěchu informačních operací je jejich pečlivé naplánování. Dosavadní analýzy totiž prokázaly, že nedostatečné vyhodnocení situace a zvolení správného typu IO přineslo během současných bezpečnostních operacích dílčí neúspěchy. Při leteckých úderech na Srbsko byla mj. paralyzována protivzdušná obrana, ale Aliance podcenila srbské schopnosti vést klamání. Řada domnělé zničené techniky, ale i některé silniční mosty se ukázaly jako klamné cíle. [30] Zpravodajské působení (vytváření obrazu bojiště) a působení na srbská místa velení (řídila klamné operace – nebyl přerušen informační tok) nebyla vedena s dostatečnou intenzitou. Menší účinek než se očekávalo měly také letáky shazované v Afghánistánu, protože velká část obyvatelstva dodnes postrádá vzdělání a neumí číst. Přehodnoceno muselo být i psychologické působení v průběhu operace Irácká svoboda. Koaliční síly totiž nesprávně předpokládaly, že nasazení zdrcující síly přiměje Iráčany k okamžité kapitulaci. [25] Příkladů existuje více, ale pro dokreslení situace není nutno další uvádět.

V post-konfliktní fázi bezpečnostních operací se ukazuje, že v islámských zemích je nutné působit, kromě vládních představitelů i na kmenové vůdce a náboženské duchovní. Kromě

toho je nutné vyvarovat se ozbrojených zásahů proti civilnímu obyvatelstvu. Důležité je rovněž nepodceňovat schopnosti povstalců vést informační operace proti koaličním jednotkám. Dokáží velmi dobře informačně působit, zejména v Afghánistánu, na civilní obyvatelstvo. Kromě toho mohou šířit informace i z televizního vysílání, arabské satelitní televizní stanice, známé protiamerickým postojem jsou v tomto smyslu jejich spojencem. [100]

. INFORMAČNÍ OPERACE PROTI TERORISTICKÝM SKUPINÁM

ÚVOD

Jednou z nejvážnějších a nejnaléhavějších bezpečnostních hrozeb dnešního světa je terorismus. Jeho akty, ať už k nim dochází kdekoli, se setkávají s téměř jednoznačným odsouzením. Ještě před čtyřiceti lety byly teroristické incidenty převážně lokální záležitostí, které měly na geopolitickou situaci minimální vliv. S postupem času se však prostředky a metody terorismu rychle mění. Jak uvádí Brzybohatý, *„mění se jeho účinnost, roste jeho nebezpečnost a počty jeho obětí*“. [18] Zásadním způsobem se tvář terorismu změnila po roce 1990, kdy došlo k rozpadu socialistického bloku a k ukončení studené války. Ke změnám došlo zejména v jeho motivaci. Ideologicky motivovaný terorismus ustoupil do pozadí a jeho místo postupně zaujímá terorismus nacionalistický a zejména náboženský, což následně vede i ke změnám teroristických cílů, metod a prostředků.

STRUČNÁ CHARAKTERISTIKA SOUČASNÉHO TERORISMU

Rozsah dnešního teroristického útoku může být srovnatelný s vojenským útokem, i když je zpravidla veden nevojenskými prostředky. [112] Důkazem toho byly útoky z 11. září 2001 proti Spojeným státům. Od této události vede mezinárodní společenství oficiálně válku proti terorismu. Dodnes však zůstává otázkou, jak uvádí bývalý ministr obrany ČR Jiří Šedivý, *„zda lze vůbec hovořit o válce*“. [121] Válka je totiž podřízena racionálně definovanému politickému cíli. Je vedena pravidelnou armádou, která používá prostředky tomuto cíli přiměřené, dodává Šedivý. Odehrává se v právním rámci, který upravuje vyhlášení a ukončení války a předepisuje pravidla zacházení se zajatci a ochrany civilistů v jejím průběhu. Do tohoto pojetí však terorismus nezapadá. Podle Eichlera je terorismus *„záměrné, politicky motivované násilí páchané na lidech, kteří nejsou ozbrojeni a nevedou bojovou činnost*“. [37] K naplnění svých cílů tedy volí jiné prostředky než vojenská vítězství. Současný konflikt má proto charakter, pro který lze těžko nalézt označení. Klasickému pojetí války se vymyká i protivník; agresorem totiž není stát definovaný územím, obyvatelstvem a uznanou suverenitou, nýbrž nestátní, globálně operující teroristická síť. Ta není hierarchicky uspořádána ani centrálně řízena. [121] Zásah proti

takovému protivníkovi komplikuje i skutečnost, že proti ní nelze použít koncepci Clausewitzova „těžiště“, tedy středisko síly a pohybu, na němž závisí celek a na něž je nutno zaměřit soustředěný úder. [24] Šedivý zdůrazňuje, *že „síla protivníka je mnohotvárná a rozptýlená. Skládá se z fanatického sebevražedného odhodlání, globálně roztroušených finančních zdrojů, horizontálně uspořádaných a volně propojených modulů místních teroristických skupin a jednotlivců. Je živena pocity křivdy a frustrace, které hýbou masami nejnižších vrstev obyvatelstva v islámských zemích*“. [121] Útočníci vycházejí z radikálního výkladu islámu a dějiny chápou jako nekončící boj dobra se zlem, přesahující životy jednotlivců, pokračuje Šedivý. Právě odtud pramení připravenost obětovat vlastní životy a ochota použít jakýchkoli prostředků. Nepřátelé vedou proti západnímu světu válku svatou, tudíž totální. Je jim cizí západní vnímání války jako odchylky od mírové normy. Boj za svaté ideály je pro ně náplní života a smrt v něm životním vrcholem. Teroristé nerozlišují mezi bojištěm a civilním zázemím. Vyplývá to z jejich požadavku totálního nasazení všech prostředků v zájmu dosažení absolutního cíle - univerzální nadvlády jejich pravdy. Bojištěm je celý svět. Nejedná se o válku světovou ve smyslu dvou konfliktů 20. století. Jde spíš o globální tažení vlastníků jediné pravdy proti hodnotám, principům, symbolům a institucím otevřené společnosti západního typu. Proti takovému nepříteli se vede velmi obtížně jakákoliv bezpečnostní kampaň a proto i informační operace. S přibývajícími zkušenostmi sice dochází k nasazení účinnějších forem působení a prostředků, teroristé však nezůstávají pozadu. Svoje metody boje neustále zdokonalují a sami vedou, mnohdy velice účinné informační operace. K jejich vedení v minulosti využívali tradiční sdělovací prostředky, v posledních letech však stále více používají sofistikovanějším a nebezpečnějším způsobem internet. [88]

VYUŽÍVÁNÍ INTERNETU TERORISTICKÝMI SKUPINAMI

Informační revoluce v arabském světě začala, jak uvádí ve své zprávě pro norské ministerstvo obrany Hanna Rogan, přibližně v 90. letech minulého století. [107] Od té doby prudce narůstá využívání internetu teroristy i počet webových stránek teroristických skupin a osob s nimi sympatizujícími. Zatímco v roce 1996 byl jejich počet odhadován na sto, v současné době je jich nejméně pět tisíc. [93] Proč využívají teroristické skupiny právě internet? Odpověď je jednoduchá. Vlastnosti internetu totiž poskytují v mnohých

směrech ideální prostor pro jejich činnost. Irving Lachow z americké Národní univerzity obrany uvádí pět vlastností internetu, které jsou pro teroristy klíčové [74]:

1. Umožňuje rychlou komunikaci, konverzaci v reálném čase, organizování webového fóra. Lze proto využít např. pro předávání instrukcí, zpravodajských informací.
2. Jeho využití vyžaduje minimální finanční náklady. Teroristické skupiny mohou v podstatě dosahovat stejných schopností jako vojenské, státní a komerční organizace – shromažďování informací, výcvik, důvtipné mediální působení na veřejnost.
3. „Všudypřítomnost“ internetu dovoluje i nejmenším teroristickým skupinám využívat kybernetický prostor ve stejném rozsahu jako jejich nesrovnatelně větším soupeřům.
4. Snadná dostupnost potřebného software umožňuje i běžným (nepokročilým) uživatelům výpočetní techniky zveřejňovat a rozesílat informace po internetu.
5. Komerční a volně dostupné prostředky pro skrytou komunikaci, skrytý přístup a anonymitu (kódování, šifrování, atd.) umožňují organizování skrytých finančních transakcí; skryté prohledávání internetu, dotyčná osoba „nezanechává stopy“, podle kterých by jí bylo možné vypátrat.

Teroristické skupiny využívají internet k aktivitám, které lze zcela bez pochyby považovat za informační operace. Podle Bruna Nordesteho z kanadského Střediska pro zpravodajská a bezpečnostní studia jsou to především psychologická válka, publicita a propaganda, dobývání informací (data mining), finanční operace, nábor nových příslušníků, vytváření sítí a kooperace v sítích (networking), sdílení informací a plánování a koordinace operací. [93] Kromě těchto aktivit přichází teoreticky v úvahu i možnost kybernetického teroristického útoku proti státní infrastruktuře, včetně vojenských systémů. Teroristé by mohli, jak uvádí Karlsson, „*ochromit informační systémy, které řídí dodávky elektrické energie pro nemocnice, střediska řízení letového provozu nebo bankovní instituce*“. [69] Takový útok, zdůrazňuje Green, však dosud nebyl zaznamenán, ani případ, že by se příslušníkům al-Káidy podařilo někoho fyzicky zlikvidovat pomocí počítače. Rovněž katastrofické scénáře, kdy se útočníkovi podařilo proniknout do vojenských systémů řídících jaderné zbraně, jsou zatím, pokračuje Green, pouze součástí filmů a ne reality. [48]

Psychologická válka na internetu

Terorismus je ve své podstatě založen na psychologické válce, podle některých odborníků, jako např. Gabriel Weimann z amerického Mírového institutu, je dokonce formou psychologické války. [139] Al-Káida a další teroristické organizace potřebují poutat pozornost veřejnosti a šířit strach mezi obyvatelstvem, především v zemích, kde operují koaliční jednotky. [37] Obyvatelstvo tak odrazují, jak uvádí Eichler, od jakékoli spolupráce s Američany a jejich spojenci. K tomu využívají zejména videozáznamy poprav unesených osob a zabitých koaličních vojáků umístěných přímo na webové stránky. Kromě nich však řada islámských webových stránek umožňuje přístup k objednávce médií (CD, DVD, video a audiopásky) se záznamy poprav a pumových útoků, fotografiemi, nebo projevy velitelů al-Káidy. Mezi producenty stránek s násilnou tematikou patří např. Globální islámská mediální fronta (Global Islamic Media Front - GIMF), která v červenci 2005 zveřejnila na svých stránkách „Deset nejlepších povstaleckých útoků v Iráku“; později rovněž vybudovala džihádský internetový televizní kanál „Hlas kalifátu“. Ten informoval týdně o nejdůležitějších událostech z Iráku, Afghánistánu a Palestiny a zveřejňoval videozáznamy z operací Talibánu, Armády Ansar al-Sunnah nebo al-Káidy v Iráku. [107] Jiná irácká povstalecká skupina Ansar al-Sunnah se pokouší vydávat elektronický časopis *Hasad al-Mujahidin*, který informuje o vojenských operacích Ansar al-Sunnah a dalších spřízněných povstaleckých skupin. Podobné elektronické periodikum vydávala v období 2006 až 2007 rovněž Islámská armáda v Iráku, některá vydání měla, podle bojových úspěchů skupiny, až 60 stránek. [70] Stejně si počínají, s různými úspěchy i další irácké povstalecké skupiny.

Publicita a propaganda

Internet značně rozšířil možnosti teroristických skupin šířit propagandistické informace. Před jeho rozmachem byly zcela závislé na televizním a rádiovém vysílání a na tištěných médiích. To pro ně samozřejmě znamenalo řadu omezení, včetně technických, která se jim často nepodařila překonat. Za pomoci internetu však tato omezení, podle Weimanna, úplně zmizela. [139] Teroristé mají v současné době přímou kontrolu nad obsahem informace, který mohou kdykoli měnit podle toho jak potřebují prezentovat sami sebe (vytvářet image) nebo své nepřátele. Tyto informace nemají zpravidla násilný obsah, mají za cíl akce

teroristů ospravedlnit. Vysvětlují proto veřejnosti, že násilí je posledním východiskem a není možnost jiného výběru. „*Je tedy jediným prostředkem slabých, jak se ubránit silnějším*“, pokračuje Weimann. [139] Snahou je zapůsobit na city a emoce veřejnosti, proto často používají výrazy jako vražda, genocida, masakr apod. Dalším rysem propagandistických materiálů je přesvědčování o právní legitimitě použitého násilí a „démonizování“ protivníka, tzn. koaličních jednotek, včetně tvrzení o jejich nelegitimním rozmístění. Právě mezinárodní jednotky jsou postaveny do role bezohledného agresora, který potlačuje lidská práva a svobody. Příslušníci teroristických skupin jsou samozřejmě, podle tvůrců těchto dokumentů, bojovníci za svobodu. Jordánský duchovní Abu Muhammad al-Maqdisi, příslušník al-Káidy a bývalý poradce zlikvidovaného nejvyššího iráckého povstaleckého velitele Zarkávího dokonce vytvořil na internetu online saláfistickou knihovnu. Ta obsahuje několik desítek básní opěvujících nespravedlivou okupaci Iráku a utrpení Iráčanů. V současné době je al-Maqdisi zadržován ve vězení, knihovna již není funkční, ale z některých džihádských webových stránek lze stáhnout její funkční aplikaci. [70] Z hlediska informačního se jedná o dezinformační materiály, které mají za cíl ovlivnit zejména mladou generaci, ženy a děti.

Dobývání informací

Na internet lze nahlížet jako na obrovskou digitální knihovnu. Samotný World Wide Web nabízí přibližně miliardu stránek plných informací. [139] Teroristé z nich mohou získat řadu detailních informací o potenciálních cílech svých útoků, jako např. zařízeních veřejné dopravy, jaderných elektrárnách, vládních budovách, letištích, přístavech a dokonce i o protiteroristických opatřeních. Podle manuálu „*Manchester Manual*“ al-Káidy nalezeného v Afghánistánu lze údajně až 80 procent potřebných informací o protivníkovi získat legálním způsobem z veřejně přístupných zdrojů. [53] To částečně potvrzují i informace v přenosném počítači al-Káidy, který se koaličním jednotkám podařilo zajistit v Afghánistánu. Obsahoval elektronické modely přehrad, vodovodních sítí, jaderných elektráren a amerických a evropských stadionů. Kromě nich však i potřebný software, umožňující simulaci nejrůznějších zásahů do těchto objektů, včetně konstrukčních změn. [48] Zda al-Káida připravovala kybernetické útoky na tyto objekty se však zjistit nepodařilo.

Finanční operace

Stejně jako mnoho politických organizací, získává al-Káida finanční podporu prostřednictvím internetu. Al-Káida byla totiž vždy závislá na finanční podpoře různých charitativních organizací, nevládních organizací a některých finančních institucí. Jednotlivé skupiny al-Káidy, jako např. Hizb al-Tahrir vyzývají příznivce z řad návštěvníků stránek, které jsou pravděpodobně na serverech po celém světě, k finančním dotacím na podporu svaté války. K tomu poskytují nezbytné údaje k provedení finančních transakcí, včetně čísel bankovních účtů. Další metodou je oslovování vytipovaných osob, které již v minulosti projevili sympatie (vyplnily různé dotazníky, zaregistrovaly se do diskusních fór, atd.), přímo zasláním zprávy na emailovou adresu. Email nemusí nutně zasílat některá z teroristických skupin, ale organizace, která teroristy podporuje. Vyskytly se již dokonce případy, kdy muslimští radikálové zřídili konto a oslovili veřejnost na internetu přímo k podpoře svaté války. [139] Velmi obtížně postižitelnou metodou finančních operací al-Káidy a dalších teroristických skupin je Hawala. Jedná se o „finanční transakce bez skutečného pohybu peněz“. Metoda, či systém spoléhá na síť dealerů Hawaly, kteří jsou v neustálém kontaktu a udržují mezi sebou „finanční rovnováhu“. Příslušník povstalecké skupiny v odlehlých oblastech Pákistánu musí pouze vyhledat místního dealera Hawaly a předat mu finanční obnos, který požaduje doručit např. do některé ze zemí střední Afriky. Dealer pouze kontaktuje dalšího člena dealerské sítě, ne fyzicky, ale mobilním telefonem, internetem nebo jiným komunikačním prostředkem a pouze mu předá informaci. Ten jí předá dalšímu, a tak se předává až k dealerovi na místě určení pouze informace o finanční hodnotě, nikoli finanční hotovost. Dealer na místě určení samozřejmě předá požadovaný finanční obnos příslušné osobě. Metoda má v islámském světě dlouhou tradici, je založena na vzájemné důvěře a je až neuvěřitelně rychlá a spolehlivá. Selhání některého z dealerů Hawaly se rovná sebevraždě. Rychlost metody umožňuje právě „pouhé“ předávání informace. Finanční rovnováhu si mezi sebou dealeři vyrovnávají později, na prvním místě je co nejrychlejší transakce. [64]

Nábor nových příslušníků

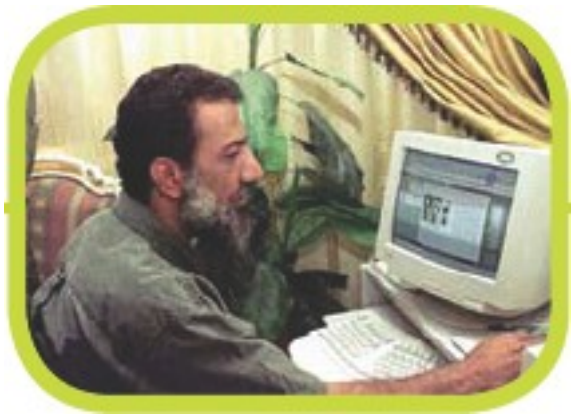
Internet lze efektivně využívat také k náboru nových příslušníků. Prostřednictvím elektronické pošty, chatu, diskusních fór, ale i bannerů na webových stránkách vyzývají

teroristické skupiny návštěvníky k větší aktivitě, než jen prohlížení obsahu stránek. Zaměřují se zejména na mladé, citově zranitelné a ovlivnitelné mladé lidi, které lákají ke vstupu do svých řad. [93] Jejich výzvy přitom nejsou zaměřeny jenom na muslimskou komunitu, ale i na potenciální konvertity k islámu. K náboru slouží, kromě oslovování jednotlivců samozřejmě také dobře propracovaná propaganda. Právě ta je např. v Saúdské Arábii v současné době nejvíce motivujícím faktorem mladých saúdských Arabů ke vstupu do al-Káidy, nebo do podobných a s al-Káidou spřízněných skupin. Jsou to videozáznamy s projevy Usámy bin Ládina a knihy o al-Káidě online, které je inspirují. Řada Arabů zadržených saúdskými bezpečnostními složkami rovněž vypověděla, že k odchodu do války v Iráku je motivovaly ideologické projevy radikálních duchovních, kteří je přesvědčili svým výkladem koránu o nutnosti boje proti nemuslimské populaci. [5] Samozřejmě, i tyto projevy lze pravděpodobně nalézt na islámských webových stránkách. V současné době je počet webových stránek, které propagují ideologii al-Káidy, podle saúdskoarabských odborníků, odhadován na více než 5,5 tisíce. Každoročně jich přibývá přibližně 900. Tato skutečnost rovněž potvrzuje, že al-Káida se zaměřila na intenzivní využití internetu a investovala do online propagace a náboru značné finanční prostředky. [4]

Vytváření sítí a kooperace

Vytvářením sítí se v této souvislosti myslí členitá síť teroristických buněk operujících na internetu, ne fyzické budování počítačových sítí. Mnoho teroristických skupin, včetně al-Káidy totiž provedlo organizační změny a v současné době již nejde o striktně hierarchicky uspořádané skupiny, ale o sdružené a vzájemně spolupracující nezávislé buňky bez centrálního velení. [7] Dokonce i sdružení různých buněk nemusí být stálé, ale může se jednat o tzv. občasné členství. [23] Teroristické skupiny totiž nemusí existovat v názorové shodě a mohou se sdružovat pouze v případě postupu proti společnému nepříteli. Tato volnost a téměř autonomní působení činí jednotlivé buňky obtížně zjistitelné pro bezpečnostní orgány. Právě internet dovolil přejít teroristům na takovou decentralizovanou strukturu a umožnil horizontální kooperaci. Operativci al-Káidy (viz. obr. 22) mohou využívat internet na veřejných místech a získávat instrukce ve formě zašifrovaných zpráv, které mohou být navíc ještě v různých nářečích. [93]

Obrázek 22. Operativec al-Káidy - příslušník palestinského Fatahu



Zdroj: LACHOW Irving and RICHARDSON Courtney. Terrorist Use of the Internet: The Real Story.

Sdílení informací

Na internetu je množství webových stránek, které poskytují informace jak vyrobit různé druhy výbušnin. Jedním nejznámějších manuálů je dokument al-Káidy, tzv. *Encyklopedie k přípravě pro svatou válku*. Jedná se o dynamický dokument online, průběžně aktualizovaný, jehož základ byl sestaven v letech 1979 až 1989, během války proti sovětským jednotkám. Obsahuje mj. detailní instrukce k používání vojenských lehkých palných zbraní, vojenské taktiky boje a k výrobě řady výbušnin v domácích podmínkách. [77] Podobných návodů a instruktážních pomůcek je internetu pravděpodobně celá řada, francouzská webová stránka organizace Société Anonyme nabízela např. ke stažení tzv. *Příručku pro sabotáže (Sabotage Handbook)* s návody na plánování vražd a způsoby jak působit skrytě a nepozorovaně. [139] Hořejší uvádí, že „*v posledních měsících se ukazuje, že al-Káida vyslala několik svých divizí i do svaté války na webu*“. [55] Elektroničtí mudžahedínové totiž nejenom verbují další radikály, ale učí je i hackerským technikám, každá webová stránka elektronických džihádistů, jako např. Hacker Boy (viz. obr. 23), obsahuje kromě instrukcí a rad i „nástěnku“ pro výměnu zkušeností a plánování útoků. Pro úplné hackerské začátečníky umístil, dnes již zadržený příslušník al-Káidy (Younis Tsouli) žijící v Londýně, dvacetistránkovou příručku „*Jak se nabourat na webové stránky*“. [55]

Obrázek 23. Webová stránka elektronického mudžahedína - Hacker Boy

Zdroj: HOŘEJŠÍ Tomáš. V éře e-džihádu.

Plánování a koordinace operací

Al-Káida využívala internet již k plánování a koordinaci útoků 11. září 2001. V zajištěném počítači strůjce celého útoku Abú Zubajdy se totiž bezpečnostním složkám podařilo objevit tisíce dešifrovaných zpráv, které byly určeny únoscům letadel. Někteří z únosců dokonce mezi sebou komunikovali a vyměňovali si informace prostřednictvím běžných soukromých emailových účtů. V současné době např. radikální palestinské hnutí Hamas, jehož velitelé mají kontakty na al-Káidu, koordinuje své operace v pásmu Gazy, na Západním břehu Jordánu, v Libanonu a v Izraeli rovněž pomocí emailové pošty. Zprávy obsahují nejenom instrukce a povely, ale i mapy, fotografie a technické údaje jak použít vhodnou výbušninu proti vytipovanému cíli. Dnes je již neposílají tak bezostyšně jako v roce 2001, ale používají metody stenografie (ukrývání dat do obrázků), aby byly nečitelné pro nepovolané osoby. [139] Dalším příkladem koordinace teroristické operace prostřednictvím internetu jsou útoky z července 2005 v Londýně. Britská policie se domnívá, že atentátníci všechny potřebné instrukce získali komunikací přes internet. [53]

Elektroničtí mudžahedíni plánují a koordinují své útoky jedině po internetu. Cílem jejich útoků nejsou zatím instituce státní správy a bezpečnostní složky, ale jak uvádí Hořejší *„jednodušší a méně zabezpečené cíle – univerzity, církve a protimuslimské soukromé blogy*“. [55] Neoperují samostatně, ale vytvářejí propojené skupiny a koordinují vzájemně čas útoků a upřesňují použití počítačových virů, jako např. Al-Jihad Al Electroni. Jednou z dalších forem koordinovaných útoků je ve stanovený čas zahltit určený server emaily s maskovanými počítačovými viry nebo ho jednoduše pouze přetíží svými vstupy a na několik minut až hodin vyřadí z provozu.

INFORMAČNÍ PROTITERORISTICKÉ OPERACE

Terorismus patří z obecného pohledu, podle Bitmanna, do kategorie propagandy činem. *„Jde o formu politického násilí, jejímž cílem je zastrašit a ovlivnit protivníka násilnými, dramatickými akcemi, které podlamují důvěru veřejnosti v zákonnost vládních institucí“*, uvádí Bitmann. [11] Novinářské zprávy o těchto akcích zaplňují první stránky novin a zpravodajské pořady rozhlasových a televizních stanic a poskytují tak teroristickým skupinám důležitou publicitu. Moderní teroristická akce je v podstatě propagandistickou akcí, která má do vědomí lidí vtisknout tvář původce a jakoby bleskem osvětlit jeho politické či náboženské cíle, pokračuje Bittman. Z informačního pohledu by proto teoreticky stačilo vyvrátit dezinformační kampaň a uvést věci na pravou míru. V praxi je ale celá věc mnohem více komplikovaná, nalézt a použít vhodné argumenty k přesvědčení veřejnosti, která je mnohdy zaujatá, není jednoduché. Situaci navíc komplikuje skutečnost, že se islámské teroristické skupiny neřídí žádnými, v západní společnosti platnými zákony a velmi rychle se dokáží poučit z vlastních chyb.

V boji proti terorismu jsou za nejúčinnější pokládány psychologické operace a použití klamání s cílem zmást protivníka. V úvahu přichází i útok na protivníkovu infrastrukturu, který zničí nebo poškodí jeho informační systémy. [95] Tyto ofenzivní operace musí být samozřejmě kombinovány s defenzivní činností, tzn. zabránit protivníkovi provést totéž. Teroristické skupiny stejně jako ozbrojené síly, uvádí Arquilla, používají informační a komunikační technologii (internet) k organizačním účelům a jako součást rozhodovacího procesu. [7] Dobrou zprávou v tomto smyslu je jejich závislost na internetu, který je „dvojsečnou zbraní“. Internet má nesporné výhody, počínaje minimálními náklady

a dostupností konče, ale zároveň jeho využívání pro tyto účely přináší nevýhody, ne-li rizika. Ostatním uživatelům stejné komunikační sítě tím umožňují monitorovat vlastní činnost, včetně používaných metod a nových trendů. Tím se zabývají zpravodajské služby, různé specializované bezpečnostní instituce, jako např. SITE Institute[31], ale i ozbrojené síly. Americké ministerstvo obrany v této souvislosti oznámilo vytvoření nové součásti MO, která se zaměří na informační a komunikační prostředky na strategické oblasti. Důvod je prostý, informační válku proti decentralizovaným a rozptýleným teroristickým skupinám nelze vést pouze na taktické úrovni v místech nasazení jednotek, jako např. v Iráku nebo Afghánistánu. [74]

Stav a úspěšnost současných informačních operací proti terorismu

V současné době vedené informační operace proti teroristickým skupinám, diplomaticky řečeno, zaostávají za očekáváním a nejsou příliš úspěšné. Proto bezpečnostní složky, zejména Spojených států, čelí značné kritice ze strany novinářů i veřejnosti. Podle některých kritiků je současné úsilí vést informační operace nedostatečné, ne-li neadekvátní. [53] Na půdě amerického ministerstva obrany a zpravodajských služeb se vedou diskuse, zda eliminovat webové stránky teroristů, či nikoli. Eliminace každé stránky by vedla současně k likvidaci určitého objemu informací, které teroristé využívají, na druhé straně je však dnes téměř nemožné eliminovat veškeré webové stránky s teroristickou tematikou. Dosavadní zkušenosti potvrzují, že kopie původní stránky se brzy znovu objeví na „jiném místě internetu“. [107] Kriticky je posuzováno i vedení psychologických operací. Jako prostředek jsou používány zejména „klasické“ sdělovací prostředky, tj. rádio, televize a tisk. K potřebnému ovlivnění příznivců teroristů a nerozhodných jednotlivců však již tyto prostředky v době internetu nestačí. [53] V teoretické rovině se jako účinný postup k potlačení terorismu nabízí uzavření islámských madras v Pákistánu a kdekoli na světě, které slouží k náboru nových členů a plní v podstatě funkci informačních a vzdělávacích středisek, kde je muslimské veřejnosti podáván radikální výklad islámu. [23] V praxi je však taková operace neproveditelná a pro demokratickou společnost nepřijatelná.

[31] SITE Institute = The Search for International Terrorist Entities. Byl založen v roce 2002 bývalými příslušníky amerických bezpečnostních složek. Úzce spolupracuje s americkým MO a dalšími silovými složkami.

Současné informační operace

Na strategické úrovni vede americké MO psychologickou operaci, která má však zatím omezený rozsah. Spravuje webové stránky v několika jazycích, včetně arabštiny, farsí a francouzštiny, které jsou určeny především pro obyvatelstvo afrických a asijských zemí. Cílem je vyvrátit nepravdivé informace o působení ozbrojených jednotek v Iráku a Afghánistánu, které na svých stránkách zveřejňují teroristé. Kromě textu obsahují i videozáznamy (mainstreamové video), aby psychologický účinek prezentovaných informací byl vyšší. [74] Kromě toho zahájily Spojené státy ambiciózní program na oslovení muslimského světa a vybudovaly televizní stanici al-Hura a rádiovou al-Sawa. Obě vysílají v arabštině a jejich společným cílem je ovlivnit muslimskou populaci. K nim se přidala i známá rádiová stanice Hlas Ameriky a zařadila do svého vysílání arabskou relaci. [53] Podobné aktivity vyvíjí i Velká Británie, vysílání BBC by se mělo zaměřit na muslimský svět.

Na operační úrovni využívají koaliční jednotky v Iráku a Afghánistánu k psychologickým operacím na ovlivnění obyvatelstva kromě letáků a místních vysílačů i speciálně upravený letoun EC-130 Commando Solo (viz. obr. 24) k rádiovému a televiznímu vysílání. [95] Kromě psychologických operací by teoreticky přicházela na operační úrovni i kybernetická nebo hackerská válka proti předpokládaným místům velení al-Káidy v horských oblastech Afghánistánu a Pákistánu. Ty sice neplní, vzhledem k rozptýlené organizaci al-Káidy, stejnou úlohu jako místa velení ozbrojených sil, jsou však pravděpodobně vybavena výpočetní technikou a datovými úložišti pro uchovávání velkých objemů dat. Podle reportérů arabských komerčních stanic, kterým teroristé umožnili přístup, jsou však vybavená ochranou proti proniknutí zvenčí. Bin Ládin si údajně k vybudování bezpečnostních bariér najal egyptské počítačové odborníky. Jeho komunikační prostředky jsou sice závislé na internetu, včetně elektronické pošty, útoku protiteroristických institucí by však měly odolat. [7] Zda jsou tyto informace od arabských reportérů pravdivé se dosud nepodařilo ověřit, protože zatím nebyla podniknuta žádná operace namířená přímo proti informačním systémům nejvyšších představitelů al-Káidy.

Obrázek 24. Letoun EC-130 Commando Solo

Zdroj: COX Joseph. *Information Operations in Operations Enduring Freedom and Iraqi Freedom – What Went Wrong?*

Na taktické úrovni provádí koaliční jednotky útoky s cílem eliminovat určitou teroristickou buňku nebo jednotlivce. Při nich se sice podaří fyzicky zlikvidovat nebo zadržet skupinu teroristů a zajistit jejich prostředky, jako např. při operaci 4. srpna poblíž irácké Samáry, kde koaliční jednotky zajistili budovu, která sloužila jako místní mediální středisko. [129] Tento způsob boje však není proti rozptýlené teroristické síti patřičně účinný. Podobné taktické operace vedou i bezpečnostní složky přímo v Evropě, kde na základě sdílení informací s jednotkami v krizových oblastech pátrají po buňkách zajišťujících nábor dobrovolníků. Tyto operace vedou se zvýšenou intenzitou především v posledních dvou letech. [35]

Defenzivní opatření

Útoky teroristických skupin namířené proti vojenským systémům přímo na bojišti zatím zaznamenány nebyly. Stejně je tomu i v případě informačních systémů ministerstev obrany a zpravodajských služeb, jako např. civilní CIA nebo vojenské DIA. Informační systémy těchto institucí nejsou dokonce fyzicky napojeny na internet, ale tvoří je samostatné interní

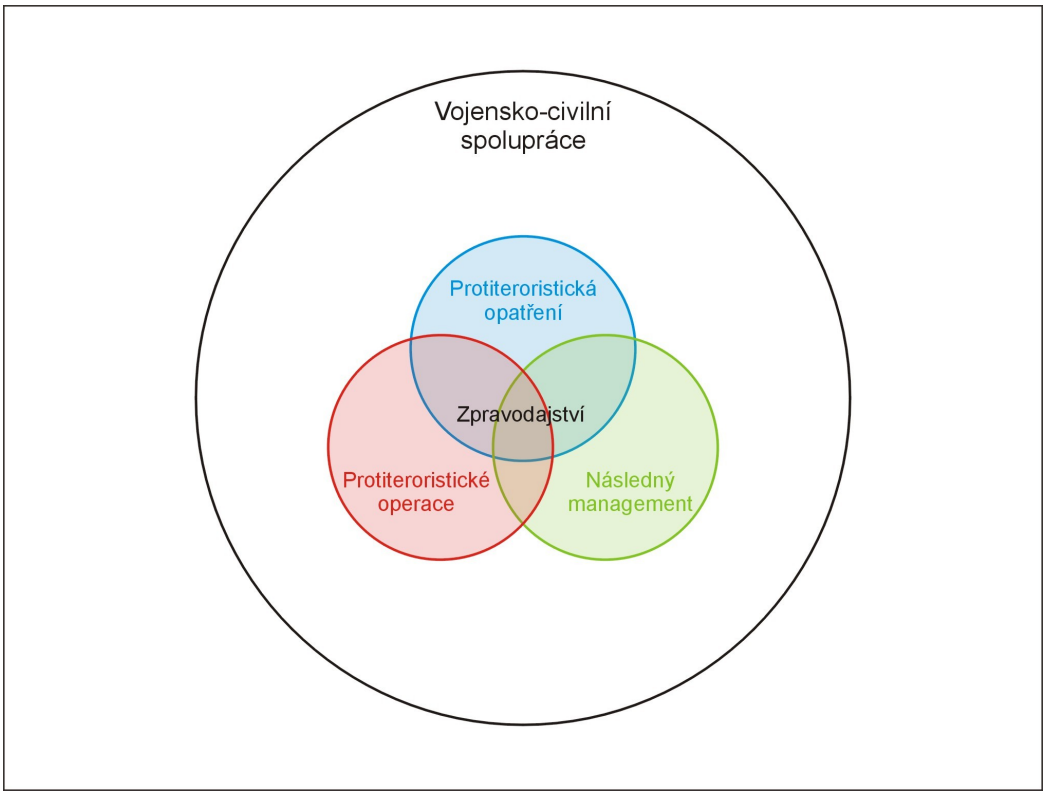
sítě, jejichž ochrana byla „předimenzovaná“ již v době studené války, kdy měly vydržet jaderný úder. [93] Jejich úplná izolace však není možná. Například pravidelná aktualizace programového vybavení těchto systémů je nutná, ale je to jedna z možností jak do systému proniknout. Proto každou instalaci nového software předchází jeho ověření národními bezpečnostními orgány. [48] Spojené státy v této souvislosti dokonce údajně uvažují i o zavedení bezpečnostního přezkoumání počítačových součástek pocházejících z asijských zemí.

Koncepce boje proti terorismu

Dosavadní zkušenosti z boje proti terorismu potvrzují důležitost kooperace a koordinace vojenských a civilních aktivit. [89] Ozbrojené síly samotné nemohou ochránit společnost před teroristickými útoky, ani bez spolupráce s civilními organizacemi nejsou schopny teroristické skupiny zcela eliminovat. Bojem proti terorismu se po útocích na Spojené státy v roce 2001 začala intenzivně zabývat Severoatlantická aliance. Na Pražském summitu v říjnu 2002 byla schválena koncepce boje proti terorismu, kterou Spojené státy přijaly za součást své vojenské doktríny. Koncepci tvoří čtyři základní, spolu související součásti/úkoly (viz. obr. 25), které jsou předpokladem úspěchu bezpečnostních operací proti terorismu [84]:

- Protiteroristická opatření – veškerá bezpečnostní opatření, včetně ochrany důležitých objektů, informačních systémů a veřejných míst, která sníží riziko teroristického útoku
- Následný management (Consequence management) – příprava na odstraňování a minimalizaci možných následků teroristického útoku. Zahrnuje rovněž pomoc jednotlivým členským státům aliance, včetně likvidace následků kybernetických útoků.
- Aktivní protiteroristické operace – ofenzivní operace bezpečnostních složek k eliminaci teroristických skupin kdekoli na světě, včetně krizových oblastí v Iráku a Afghánistánu.
- Vojensko-civilní kooperace – společné plánování operací a jejich koordinace.

Obrázek 25. Součásti boje proti terorismu



Zdroj: Upraveno a převzato z MOCKAITIS Thomas. *The „New“ Terrorism: Myths and Reality*.

ZÁVĚR

V průběhu posledních deseti let se internet stal důležitým nástrojem pro teroristické skupiny. Právě světová síť internet přispěla k tomu, že teroristické skupiny změnily svojí hierarchickou organizační strukturu na moderní, decentralizovanou a rozptýlenou strukturu. Ústřední postava al-Káidy - bin Ládin a jeho nejbližší spolupracovníci již zjevně neplní úlohu nejvyššího přímého velení nad všemi buňkami. Jsou spíše klíčovými postavami, které koordinují a podporují činnost rozptýlených teroristických buněk. [7] Ty se dnes chovají jako volná asociace, která se však v případě potřeby dokáže semknout, z jednotlivých buněk se stanou „uzlové, či styčné síťové body a rozbočovače (hubs)“, na které se napojí další a další, až spolu vytvoří navzájem propojenou síť, která je schopna vést koordinované útoky a rozsáhlé operace. [93] Teroristické skupiny se tak stále více pohybují mezi reálným a kybernetickým prostředím. To představuje, jak uvádí Nastoupil, *„pro tradiční orgány, které je pronásledují zcela nový a jen velmi obtížně řešitelný problém*“. [88] Při vytváření současných organizací a bezpečnostních složek, pokračuje

Nastoupil, totiž nikdo nepředvídal existenci rozhraní mezi reálným a kybernetickým prostředím.

Změnily se i zbraně teroristů, bin Ládin a jeho příznivci v současné době nepoužívají jen palné zbraně a výbušniny, jako dřívější generace teroristů. Do svého arzenálu začlenili minikamery, profesionálně zpracované propagační a ideologické materiály na CD a DVD, počítače, emailové účty a přístupy k internetu. [53] Dokonale se tak přizpůsobili informačnímu věku. V boji proti nim je pro bezpečnostní složky výhodou jejich závislost na internetu, kvůli jeho známým nevýhodám. Tato výhoda je však pouze relativní. Teroristé se velmi rychle učí ze svých chyb, a jak uvádí Lachow, snaží se minimalizovat nevýhody internetu a využívají čím dál dokonalejší metody, které jim umožňují skrytou výměnu informací a pohyb na internetu. [74]

Dosavadní informační operace namířené na teroristy a na jejich příznivce nedosahují požadovaného úspěchu. Jedním z důvodů je smutný fakt, že teroristé svojí online propagandou, náborem a dalšími „online aktivitami“ předběhli bezpečnostní složky. Psychologické operace vedené pomocí tradičních médií nejsou dostatečně účinné, internet jako médium v rukou teroristů je překonává. [53] Zahájit jednoduše účinnější typ informačních operací není tak jednoduché, jak se zdá. Nejdříve je totiž nezbytné, protivníka dokonale poznat, vyhodnotit jeho kapacity a podle toho zvolit způsob boje. Stále totiž platí výrok, který Sun Tzu vyslovil již před mnoha staletími: „*pokud znáš svého protivníka a sebe samého, nemusíš se obávat výsledku stovek bitev*“. [118] Potíž je právě v tom, že vojenské jednotky, ani protiteroristické instituce dokonale dnešní teroristy a jejich kapacity neznají. Ještě před 11. září 2001 řada odborníků na boj proti terorismu i vojenských specialistů považovala letecký teroristický útok za nepravděpodobný, nebo ho zcela vylučovala. To je pouze jeden z příkladů, který poukazuje na skutečnost, že bezpečnostní složky zatím pouze vyčkávají s jakou novou taktikou teroristé překvapí. Je jisté, že teroristé zatím nevyužívají internet ke kybernetickým útokům proti infrastruktuře, ale jako podpůrný prostředek zejména k plánování a provádění fyzických útoků. Takové poznání protivníka je však jen základní a k vedení účinných informačních operací nestačí. Nedostatečná je i taktika „zabít nebo zadržet“, kterou používají koaliční jednotky v Iráku a Afghánistánu. [53] Globální terorismus nezlikviduje. Bezpečnostní složky naopak čeká, podle Arquilly, v boji proti terorismu nový způsob vedení informačních operací - válka ve světové počítačové síti – „*netwarfare*“. [7]

. OBRANA PROTI INFORMAČNÍM OPERACÍM

ÚVOD

Vedení vojenských operací nezahrnuje pouze ofenzivní činnost (včetně útočných informačních operací), velitelé musí počítat rovněž s ochranou vlastních sil a prostředků, ať se jedná o operaci v rámci ozbrojeného konfliktu nebo během mírové mise. V žádném případě se totiž nevyplácí podceňovat kapacity protivníka a obranu zanedbávat. Protivník bude zcela jistě usilovat o ochromení nepřátelských (našich) jednotek odříznutím od jejich velení. Může se pokusit mj. o fyzickou destrukci míst velení, paralyzování informačních systémů, přerušení spojení nebo použije kombinaci různých způsobů. Síly vyčleněné k obraně systémů velení a řízení a dalších velmi důležitých, zranitelných míst by proto měly být v rovnováze se silami vyčleněnými k informační operaci proti citlivým místům protivníka. [58] Pro tuto činnost se někdy používá termínu „obranné informační operace“. Ty obecně definuje americká armádní doktrína jako *„ochranu a obranu vlastních a spojeneckých informací, systémů velení a řízení a informačních systémů“*. [61] Cílem efektivní obranné informační operace je umožnit velitelům získat přesný obraz bojiště (prostoru působnosti) se všemi vojenskými prvky a rovněž nevojenskými faktory, které mohou situaci v prostoru působnosti jednotek ovlivnit. Přesný obraz prostoru působnosti je nezbytný k pochopení a správnému vyhodnocení situace. Z informačního hlediska jde o získání relevantních informací, které umožní vytvořit pro velitele zrcadlo reálné situace v prostoru působnosti podřízených jednotek (na bojišti nebo v prostoru odpovědnosti). Tím je minimalizována míra entropie, zjednodušuje se rozhodovací proces a zvyšuje se pravděpodobnost správného odhadu vývoje situace v nejbližší budoucnosti a tím i pravděpodobnost úspěchu celé vojenské operace.

OBRANNÉ INFORMAČNÍ OPERACE

Obrana proti informačním útokům má, podle Davida Albertse z americké Národní univerzity obrany, řadu charakteristik společných s bojem proti společenským neduhům, jako např. civilizační nemoci, užívání narkotik nebo kriminální činnost a organizovaný zločin. [2] Mezi nejdůležitější patří smutný fakt, že stejně jako nelze vymýtit různé společenské neduhy je rovněž nereálné zcela potlačit informační útoky. Reálně lze pouze

dosáhnout, zdůrazňuje Alberts, minimalizaci hrozby informačních útoků na únosnou míru. Vlastní obranu tvoří, pokračuje Alberts, tři hlavní opatření:

- Ochrana sil a prostředků proti útokům, tj. preventivní opatření přijatá ještě před tím, než protivník zahájil útok. Z vojenského hlediska se jedná např. o vybudování protivzdušné obrany kolem velitelských stanovišť, oddělení zbraňových systémů od veřejných sítí, umístění utajených počítačových terminálů do certifikovaných zabezpečených objektů nebo používání pouze prověřených aplikací.
- Omezení účinku útoku, tj. přijetím opatření v době, kdy již byl zahájen informační útok a nepodařilo se mu předejít. Jde o to, aby jeho následky byly co nejvíce minimalizovány a nebyly paralyzovány zbraňové systémy a systémy velení a řízení. Mezi tato opatření patří např. přechod na záložní systém velení, protože hlavní byl již útokem zasažen, přesun míst velení do záložních stanovišť, posílení prostředků protivzdušné obrany a nahrazení zničených, detekce a odstraňování škodlivých programů z odpojených terminálů, aby se nešířily dále do sítí, atd.
- Odstraňování následků informačních útoků. Pokud dojde k této situaci, musí dojít k nejrychlejšímu možnému odstranění následků útoku. Jde mj. i o to, aby nevznikala panika mezi civilním obyvatelstvem, čehož by mohl protivník dále využít. Lze totiž předpokládat, že útok nebude omezen pouze na vojenská zařízení, ale i na civilní objekty. Z vojenského hlediska je nutné přesunout do prostoru nové síly a prostředky, z hlediska informačního obnovit schopnost předávat informace a obnovit poškozené databáze. Civilnímu obyvatelstvu je nutné zdůraznit, jaký je skutečný rozsah útoku a jak dlouho bude obnova infrastruktury trvat. V případě, že je do konfliktu zahrnut i civilní sektor je psychologické působení na obyvatelstvo nezbytné. Jedná se o kontra opatření proti protivníkově psychologické válce.

Burnett z americké armádní válečné školy doplňuje Albertse a přidává ještě čtvrté opatření, jímž je protiútok. [20] Ten bude veden na protivníkova slabá místa, která musí být správně vyhodnocena. Ke správnému výběru slabých míst protivníka a nasazení patřičných sila prostředků přispěje i analýza protivníkova útoku. Tím nepřímo poodhalí bojové kapacity svých jednotek. Protiútok bude samozřejmě nejúčinnější v případě, že bude následovat hned po odražení nepřátelského útoku, tj. protivníkovi se nepodaří překonat ochranu našich vojsk. Neúspěšný nepřátelský útok naznačuje, že protivník nesprávně vyhodnotil naše

kapacity a přecenil vlastní možnosti. Z informačního hlediska nedisponoval relevantními informacemi a jeho velení podcenilo míru neuspořádanosti systému při rozhodování.

Problémy obranných informačních operací

Vedení obranných informačních operací, pokud se neuvažuje pouze o obranných operacích přímo na bojišti, je ze širšího pohledu podobné boji bezpečnostních orgánů s nelegálním obchodem s narkotiky, kriminálními skupinami nebo boj lékařů s civilizačními chorobami. Podílet se totiž na nich musí státní i soukromý sektor. [2] V prostoru bojiště se samozřejmě jedná ryze o „vojenskou záležitost“, v době míru, nebo v zázemí, tedy v situaci kdy jsou vojenské prostředky provázané a závislé na státní infrastruktuře jsou již „ryze vojenská opatření“, včetně nasazení prostředků protivzdušné obrany, nedostačující. Nepřátelský informační útok může ochromit dodávky elektrické energie, vody, plynu, atd. Vojenské jednotky jsou na těchto zdrojích krátkodobě nezávislé pouze na bojišti (disponují elektrocentrálami, omezenými zásobami potravin a vody).

Problém vedení obranných informačních operací vyplývá právě z nutnosti kooperace a koordinace širšího spektra součástí, než jsou pouze vojenské jednotky. Pouhá příprava na možný informační útok, tj. budování ochrany systémů a infrastruktury však vyžaduje značné finanční náklady. Vzhledem k tomu, že tato činnost vyžaduje spolupráci různých organizací, které spolu v konkurenčním prostředí soutěží, je obtížné je přesvědčit, zdůrazňuje Alberts, aby se na financování podílely a téměř nereálné docílit, aby výše poskytnutých finančních prostředků odpovídala skutečným potřebám. [2]

Obranné informační operace nejsou, podobně jako boj proti překupníkům s narkotiky a organizovanému zločinu, statický problém. Pachatelé informačních útoků se stejně jako kriminální podsvětí ze svých chyb učí a jejich útoky se stávají sofistikovanějšími a lépe koordinovanými. Z tohoto důvodu musí být dynamická i obranná opatření, nesmí zaostávat za technologickým pokrokem, aktualizace databází škodlivého software a vývoj antivirových programů musí být nepřetržitý. V této souvislosti je obtížné přesvědčit všechny organizace, aby se na přípravě a vývoji opatření podílely, zejména v období relativního klidu. Veřejnost se k tomuto problému staví netečně a je obtížné získat její podporu. [2]

V období kdy dojde k informačním útokům dochází, podle Albertse, často naopak k horečnatým, nepromyšleným snahám vyřešit problém. [2] V těchto případech je nutné, kromě přijetí obranných opatření rovněž psychologicky působit na veřejnost, protože zmatku a nekoordinovaných opatření využívá protivník. Takové situace využívají zejména teroristické skupiny, kterým jde o upoutání pozornosti veřejnosti a šíření strachu. [113] Reálné škody mohou být ve skutečnosti méně závažné, ale chaos, zmatek a ztráta důvěry ve vládní orgány působí jako mocnitel.

Opatření proti informačním útokům

Proti některým typům informačních operací vznikly v průběhu vývoje vojenské vědy a válečného umění účinné formy boje, nazývané jako tzv. protiopatření nebo kontraopatření. Mezi nejdůležitější patří:

Kontrarozvědná činnost – *„counterintelligence"; „soubor činností, které se týkají identifikace a působení proti ohrožení bezpečnosti zpravodajskými službami, organizacemi nebo jednotlivci protivníka, které se zabývají špionáží, sabotážemi, podvracením nebo terorismem"*. [134] Cílem je zjistit, identifikovat, zhodnotit, provést protiopatření, neutralizovat nebo naopak využít ve svůj prospěch protivníkovo úsilí zaměřené na získávání informací. [61] V nejširším pojetí je tedy tato činnost z informačního hlediska určena k odepření získávání informací o vlastních silách a prostředcích, obranném průmyslu, citlivých, zneužitelných údajích o představitelích státní správy, atd. Kontrarozvědnou činnost vyvíjí i komerční instituce k ochraně svých výrobních tajemství, finančních operací nebo vývoje, pokud jim zákon nenařizuje tyto skutečnosti zveřejnit.

Opatření proti průzkumu protivníka – *„countersurveillance";* zahrnují *„veškerá opatření, aktivní nebo pasivní, prováděná s cílem zabránit sledování protivníkem"*. [134] Jedná se pravděpodobně o jednu z nejstarších způsobů ochrany informací o vlastních jednotkách. Lze provádět fyzickou likvidací nepřátelského průzkumu, různými způsoby klamání, včetně dezinformací a předstírání. V současné době jde o rozsáhlý soubor opatření, protože průzkum doznal od dob Napoleonských válek značného pokroku. Informace získávají kromě tradičních průzkumných jednotek a letounů i bezobslužné platformy, včetně družic, bezpilotních průzkumných prostředků a v poslední době probíhá

i vývoj bezobslužných podhladinových prostředků. Takto získané informace jsou dále předávány v téměř reálném čase do analytických středisek a od nich přímo k bojovým jednotkám.

Opatření proti klamání – *„counterdeception“;* veškeré úsilí, které je zaměřeno na potlačení, neutralizaci, minimalizaci účinnosti nepřátelského klamání, nebo naopak využití protivníkových opatření ku prospěchu vlastní bojové činnosti. Cílem je včas uvědomit vlastní velení o protivníkových aktivitách, aby byly zahrnuty do rozhodovacího procesu při úkolování a nasazení jednotek v prostoru odpovědnosti. [61] Důležitým momentem je, aby protivník neodhalil, že jeho úsilí podávat klamné informace bylo prozrazeno a že své skutečné plány a činnost není schopen dále utajovat.

Opatření proti propagandě – *„counterpropaganda“;* protiopatřením jak čelit různým formám propagandy je tzv. kontrapropaganda. V obecném pojetí ji tvoří soubor opatření a operací, jejichž úkolem je eliminovat nebo alespoň minimalizovat účinky protivníkovy propagandy. Jejím cílem je potlačit (omezit) negativní vliv nepřátelských psychologických operací zaměřených na zejména na spojenecké jednotky a spřátelené obyvatelstvo. [59] Samozřejmě o jedno z možných opatření, v době ozbrojeného konfliktu by bylo odvetné opatření razantnější, včetně fyzické eliminace zdroje nepřátelské propagandy.

Elektronická ochranná opatření – *„electronic protective measures“*, defenzivní součást elektronického boje; jsou chápána především jako součást velení a jsou uplatňována, podle Velíška, následovně [131]:

- *„Řízením vysílání a řízením bezpečnosti, tj. selektivní řízení EM vyzařování, ovlivňující možnosti protivníka toto vyzařování zachytit a využít“*. Cílem je minimalizovat protivníkovy možnosti detekce vyzařování a využití takto získaných informací a dále snížit vzájemné neúmyslné rušení. Řízením bezpečnosti se rozumí strategie pro utajení a zamaskování vysílání vlastních vojsk (provádí se tzv. elektronickým maskováním), kódování a šifrování obsahu vysílání. Cílem je znemožnit nebo alespoň ztížit identifikaci obsahu a možnosti napadení vysílání v případech, kdy ho protivník může zachytit.

- *„Stanovením pasivních a aktivních opatření pro elektronické systémy a stanovením způsobů jejich použití v souladu s bezpečnostními opatřeními a s pravidly činnosti“*. První jmenovaná jsou „nezjistitelná“ opatření, jako např. operační postupy a technické charakteristiky řízení. Zahrnují činnosti jako např. zkrácení doby vyzařování, výběr takových prostředků, které sníží riziko zjištění a ztíží zaměření nebo použití méně citlivých prostředků vůči nepřátelskému rušení a klamání. Aktivní opatření jsou „zjistitelná“ opatření, která zahrnují mj. změny přenosových parametrů vysílačů, použití rozprostřeného spektra, kmitočtové skákání, změnu modulací a další technologická opatření.
- *„Pomocí organizačních, provozních a technických opatření“*, tj. využití výpočtů, zkušeností k objektivně podloženému rozvinutí a použití elektronických systémů s cílem vyloučit nebo alespoň předvídat možná ohrožení funkce elektronických prostředků a tím minimalizovat účinky nepřátelského EB. Provozními opatřeními se rozumí využívání metodik pro obsluhy, aby byla zajištěna odolnost elektronických opatření. Technická opatření zahrnují možnosti, kterými disponuje nasazená technika. Jejich součástí jsou požadované a realizované parametry prostředků EB, které jsou zaváděny do výzbroje ozbrojených sil.
- *„Prakticky z hlediska působení proti činnostem protivníka“*, provádění elektronických ochranných opatření je zaměřeno proti technickému průzkumu protivníka, velmi přesné munici (elektronicky naváděna), elektronickému rušení, elektronickému klamání a rovněž k zajištění současného elektromagnetického působení vlastních elektronických prostředků.

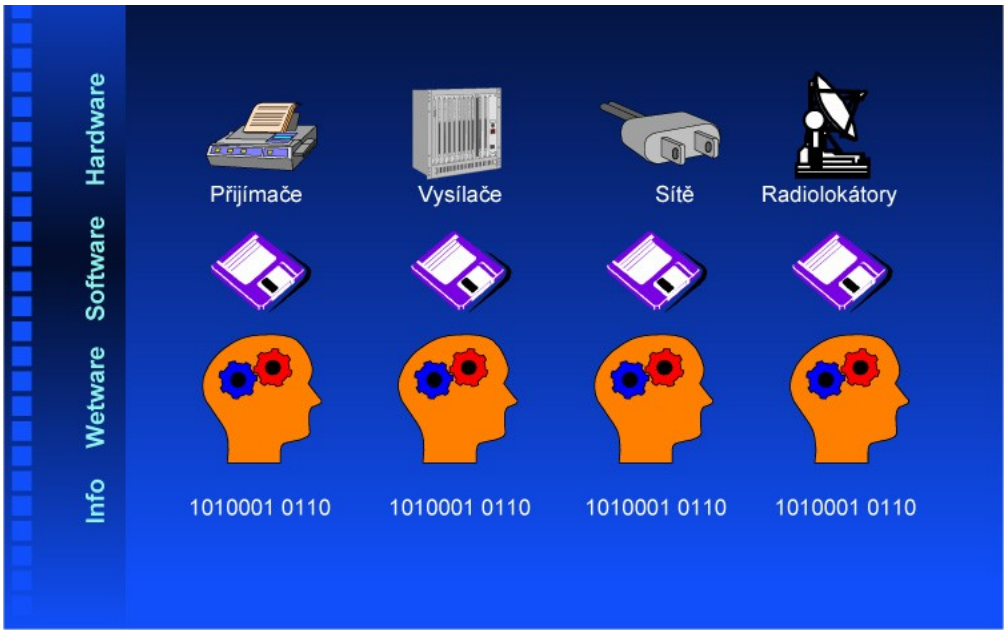
Informační jistota – *„information assurance“;* je soubor bezpečnostních opatření vedených s cílem zajistit ochranu vlastních informací a informačních systémů. Zahrnuje veškeré typy informačních operací, které ochraňují informace a informační systémy a současně zabezpečují jejich dostupnost, integritu, spolehlivost, utajení a nepřetržitý provoz. [57] Jedná se o termín pro široký soubor obranných opatření, který se nepoužívá v rámci Severoatlantické aliance, ale u námořní pěchoty Spojených států. Pod tímto pojmem lze chápat přijetí kteréhokoli uvedeného opatření nebo jejich kombinaci.

ZÁVĚR

Obrana proti informačním operacím je neoddělitelnou součástí vojenských operací. K jejímu zabezpečení je nutné vyčlenit síly a prostředky v případě, že se jedná o „klasický“ ozbrojený střet proti sobě stojících ozbrojených sil. Obranu proti informačním útokům pak tvoří veškerá opatření, která mají ochránit velitelská stanoviště, zajistit nepřetržitý tok informací a zabránit proniknutí a poškození informačních systémů. Jde o nasazení vojenských prostředků, včetně protivzdušné obrany s cílem fyzického a elektronického zabezpečení zbraňových systémů, sítí, programů, dat a všech elektronických prostředků. Při vedení bezpečnostních opatření v krizových oblastech, kde dochází ke střetům s povstaleckými skupinami a boj má charakter asymetrické války, je nutné zajistit mohutnou kontrapropagandu a nepřetržitě vysvětlovat místnímu obyvatelstvu účel mise. Opatření proti nepřátelské propagandě je nezbytné zajistit i v průběhu mírových misí. V obou těchto případech má kontrapropaganda charakter opatření proti psychologickým operacím protivníka (povstalcům nebo radikálním etnickým skupinám). Zvláštní charakter mají obranné informační operace proti teroristickým skupinám a vzhledem k jejich rozsahu je boji s teroristickými skupinami věnována samostatná kapitola.

Během vedení ozbrojených střetů se vyvinula řada způsobů a technik boje proti informačním útokům, které se nazývají protiopatření. K dosažení vítězství však jejich uplatnění nestačí. Jsou určeny pouze k odvrácení, případně minimalizaci nepřátelských útoků. Po jejich aplikaci musí následovat protiútok, jak zdůrazňuje americká *Doktrína informačních operací*. [59] Ten se považuje za součást obranných informačních operací. Nepřátelské informační útoky mohou směřovat prakticky proti všem vojenským součástem v prostoru nasazení, tj. proti zařízení a technice, programovému vybavení, živé síle a proti souborům dat (viz. obr. 26).

Obrázek 26. Cíle informačních útoků



Zdroj: Upraveno a převzato z *Joint Information Operations Planning Handbook.*

Jako velký problém se jeví vedení obranných informačních operací v zázemí a v období míru. Informační systémy vojenských jednotek jsou v prostoru zázemí (mimo bojiště a zpravidla na území vlastního státu) a rovněž v době míru (jsou rozmístěny na základnách) napojeny na infrastrukturu a jsou tedy propojeny s civilním sektorem. Jsou závislé zejména funkčnosti energetických sítí, dodávkách vody a potravin a mnohdy využívají různé služby zajišťované civilním sektorem. V této situaci již nestačí chránit pouze vojenské objekty, obrana musí být komplexní a vyžaduje součinnost nejenom ostatních bezpečnostních složek, ale i civilních státních a soukromých institucí. Problém spočívá v nepochopení trvalé hrozby především kybernetických útoků, za kterými mohou stát jak domácí tak zahraniční pachatelé (radikální skupiny obyvatelstva, skupiny organizovaného zločinu, teroristické skupiny, zpravodajské služby cizích států, cizí ozbrojené síly, etnické skupiny podporované cizími státy, apod.). [135] Soukromé organizace mají totiž tendenci, zdůrazňuje Schroeder z novozélandské Univerzity Massey, zajišťovat informační bezpečnost ad hoc v okamžiku kdy jsou vystaveny informačnímu útoku a navíc všeobecně spoléhají pouze na fyzickou bezpečnost. [113] V období relativního klidu a v době, kdy je útok dosud nerozpoznán odmítají vyčlenit finanční prostředky na opatření a přípravu proti nepřátelským informačním operacím.

. BUDOUCNOST INFORMAČNÍCH OPERACÍ

ÚVOD

V současné době hrají informační operace významnou úlohu ve všech bezpečnostních operacích a jsou jejich neoddělitelnou součástí. Lze předpokládat, že jejich role bude nezastupitelná i v budoucnu, nijak neztratí na své významu, ten naopak téměř jistě ještě vzroste. Hlavním důvodem je, jak uvádí příslušník amerického vojenského námořnictva Moorman, „*exponenciální růst kapacit informačních a komunikačních technologií*“. [1] Rychlost výpočetní techniky se přímo dramaticky zvyšuje a současně se velikost počítačů zmenšuje. Nanotechnologický tým NASA ve své studii z konce devadesátých let uvádí, že lze v brzké budoucnosti vyrobit počítače, které budou milionkrát výkonnější než současné. [46] Rovněž odhaduje, že první molekulární počítače bude možné zkonstruovat již v období 2010 až 2015. Miniaturními počítači by měly být vybaveni tzv. „vojáci budoucnosti“[32] – příslušníci ozbrojených sil. Vyspělé státy tak budou sice technologicky dominovat na bojišti, ale paradoxně právě jejich závislost na složitých technologiích bude zranitelným místem. Lze proto souhlasit s tvrzením Dunlevyho, jenž uvádí, že „*závislost na vyspělých technologiích lze považovat za potenciální Achillovu patu*“. [36]

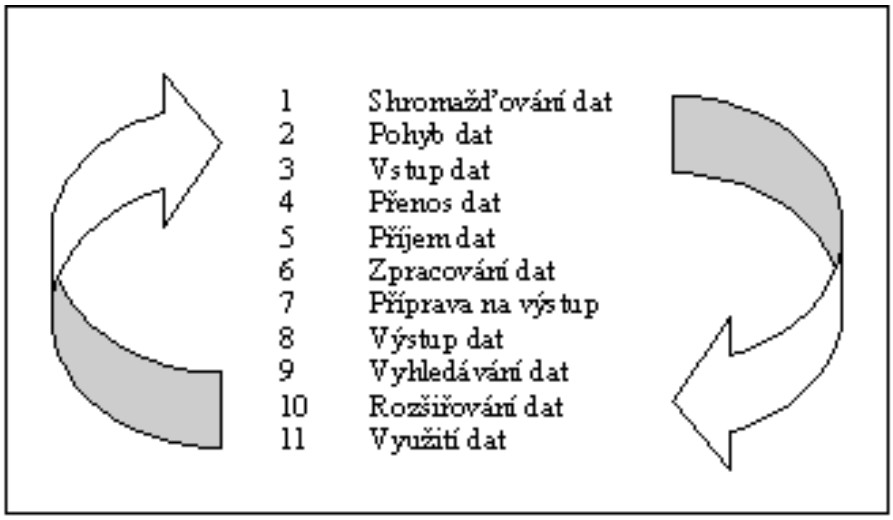
INFORMAČNÍ OPERACE V BRZKÉ BUDOUCNOSTI

Ať již bude na bojišti válčit kdokoli, ať bude obraz bojiště jakýkoli (podmořské hlubiny, kosmický prostor, městské oblasti, horský terén, virtuální prostor počítačových sítí, apod.), budoucí konflikty se budou stejně jako ty současné řídit obecnými zásadami vedení války. Z nich je nejdůležitější ta, že nelze spoléhat pouze na obranu, protože „obranná válka“, jak zdůrazňuje Welch, nemůže vést k vítězství. [140] K tomu vede jedině ofenzivní akce, jejíž součástí jsou i různé typy informačních operací, přesněji řečeno získání informační převahy, která povede k získání informační nadvlády nad protivníkem. Tu definuje americký předpis JP 1-02 jako „*operační výhodu, získanou pomocí schopnosti nepřetržitě*

[32] „Voják budoucnosti“ je jedním z nejžhavějších témat diskusí, ale i rozvíjených projektů MO Spojených států, západoevropských zemí, Ruska a Číny. Názvy projektů se mohou lišit, např. *Future Warrior, Soldier of the Future*, atd. Vychází však ze stejné myšlenky – vyslat na bojiště vojáka, který bude mít dokonalou výstroj a výzbroj a bude vybaven mj. mikropočítačem a spojovacími miniaturními prostředky, které mu umožní získávat, sdílet a šířit informace v reálném čase (z informačního hlediska). Z vojenského hlediska bude samozřejmě na prvním místě vojáka řídit, předávat mu rozkazy a instrukce ke splnění aktuálních úkolů.

shromažďovat, zpracovávat a šířit informace za současného působení na protivníkovi kapacity, aby nebyl schopen provádět totéž“. [32] Jak se budou informační operace vyvíjet a jaké typy informačních operací k tomu budou využívány je spíše záležitostí představivosti a úvahy. Je však jisté, že budou zaměřeny, jak uvádí Yurcik, na všech jedenáct součástí protivníkova informačního cyklu [144] (viz. obr. 27) a samozřejmě na ochranu cyklu vlastního.

Obrázek 27. Jedenáct součástí informačního cyklu



Zdroj: Upraveno a převzato z YURCIK William. *Information Warfare Survivability: Is the Best Defense a Good Offense?*

Nové formy kybernetické války

Vstupní náklady na vedení kybernetické války jsou mimořádně skromné a použití kybernetických strategií může být významným multiplikátorem sil. Menší země, které by ve smyslu konvenčního vojenství nikdy nemohly konkurovat svým větším sousedům, si mohou vytvořit takovou kapacitu, která jim poskytne strategickou výhodu, pokud bude vhodným způsobem použita. Lze proto usuzovat, že počítačové informační systémy členských států NATO budou pravděpodobně neustálým terčem útoků ze strany netradičního nepřítele. V této souvislosti lze uvažovat, uvádí Dunlevy, omezenou a neomezenou formu kybernetické války. [36]

V případě omezené kybernetické války, pokračuje Dunlevy, je informační struktura médiem, cílem i zbraní použitou k útoku. Tento útok je doprovázen jen málo, či vůbec

žádnými akcemi v reálném světě. Jako médium představuje informační struktura nosič, jehož prostřednictvím je útok naveden na cíl – často na základě spojení mezi nepřítelem a jeho spojenci s využitím spojů pro sdílení zdrojů či dat, nebo prostřednictvím plošného síťového propojení. Další možností je, že agent působící ve strukturách nepřítele umístí škodlivý software přímo na jeho sítě. Jakožto cíl útoku představuje infrastruktura prostředek, jehož pomocí je omezována efektivita nepřítele. Znehodnocení kapacit jeho sítí zpomalí, nebo překazí operace, které jsou na ní závislé. Snížení úrovně sítí by mohlo vést protivníka, aby se uchýlil k použití náhradních prostředků, což by mohlo vést k odhalení dalších zranitelných míst. Jako útočná zbraň by mohla infrastruktura být zneužita, aby napadla sama sebe (např. implementací škodlivého software). Cílem omezené kybernetické války by mohlo být zpomalení příprav protivníka na vojenský zásah, nebo by se tato forma mohla stát součástí ekonomické války. [36]

Závažnější a pravděpodobnější je však, jak dále uvádí Dunlevy, neomezená kybernetická válka. Ta by byla komplexní co do rozsahu a nečinila by rozdíly mezi vojenskými a civilními cíli, či mezi zázemím (týlem) a frontou. Rovněž by znamenala fyzické následky a oběti. Některé z nich by byly důsledkem úmyslných útoků, jejichž cílem by bylo způsobit co největší fyzické škody a masakr; další by byly způsobeny kolapsem řídících kapacit jako je kontrola letového provozu, řízení pohotovostních služeb, správa vodních zdrojů a produkce elektrické energie. Kromě ztrát na životech by tato forma kybernetické války mohla mít i značný ekonomický a sociální dopad. [36] Neomezená kybernetická válka by byla zcela jistě zaměřena na infrastrukturu, pravděpodobně by překračovala hranice mezi státním a soukromým sektorem, vleklé ochromení produkce a distribuce elektrické energie by mělo výrazný dopad mj. i na zdravotnické a finanční služby. Vojenské sítě, zejména ty, které používají komerční komunikační kanály by byly rovněž paralyzovány, čímž by bylo přerušeno velení a řízení, logistika a příprava na jakoukoli operaci. Dunlevyho odhady z období 2001 až 2002 se již začínají pomalu naplňovat a zdá se, že opravdová kybernetická válka se může stát realitou ve velmi krátké době. Kromě útoků na estonské servery, které byly ze všech kybernetických útoků v roce 2007 pravděpodobně nejvíce medializovány, zaznamenala podobné útoky proti své informační infrastruktuře také Velká Británie. Ian Brown z Oxfordské univerzity dokonce uvedl, že *„útoky proti britským serverům provedlo nejméně 120 různých zemí, včetně Číny*“. [13] Ta je v současné době, pokračuje Brown, nejaktivnější zemí ve špionáži prostřednictvím internetu a ve vývoji koncepce kybernetické války. Rovněž bezpečnostní orgány Spojených států zabránily

v roce 2007 přibližně 37 tisíc pokusů o proniknutí nebo narušení informačních systémů soukromých společností. Rusko zaznamenalo ve stejném roce, podle prohlášení ředitele Federální bezpečnostní služby (FSB) Nikolaje Patruševa, dokonce 1,4 mil. kybernetických útoků různého rozsahu proti počítačovým systémům státních úřadů. [31] Útoky proti počítačovým systémům Velké Británie, Spojených států a Ruska potvrzují skutečný nástup kybernetické války jako jednoho z typů informačních operací.

Nové formy elektronického boje

Moderní prostředky elektronického boje lze použít jako nekinetickou zbraň, která je schopna vyslat elektromagnetickou energii. Krátké impulsy namířené na informační systémy protivníka trvale poškodí, nebo úplně zlikvidují počítačové obvody. Zatím jsou tyto zbraně ve stádiu zkoušek, jejich použití na bojišti je však otázkou velmi krátké doby. Jejich využití se předpokládá na nejen pozemních platformách, ale i na bojových letounech. Z letounu vyslaný elektromagnetický impuls patřičné síly bude kromě informačních systémů schopen zlikvidovat i protivníkovy radiolokátory, podobně jako leteckou pumou. Tím bude paralyzována protivzdušná obrana, protivník nebude mít potřebné informace o vzdušném prostoru a nebude schopen vytvořit celkový obraz bojiště. Paprsek (impuls) vyslaný z pozemních stanovišť bude využitelný jako součást protiraketové obrany. Zničí obvody blížící se nepřátelské rakety nebo bude působit jako falešný telemetrický signál, který způsobí chybu naváděcích systémů rakety a ta změní trajektorii letu. V obou případech raketa nezasáhne cíl. Další možností využití elektromagnetických nekinetických zbraní je v rámci psychologických operací. Americké vojenské letectvo již údajně vyvinulo nekinetickou zbraň, kterou je možno instalovat na vozidla a používat jako neletální zbraň při potlačování pouličních nepokojů. Využitelná bude v krizových oblastech jako součást psychologických operací - demonstrace síly koaličních jednotek při ovlivňování místního obyvatelstva. [143]

V brzké budoucnosti se předpokládá rovněž využití mikrovlnného impulsu. Jedná se o elektromagnetickou energii s vlnovou délkou pouze několik milimetrů, maximálně centimetrů. Tu lze usměrnit pomocí speciální antény nebo vyzařovače s velkým výkonem na požadovaný cíl, podobně jako laserový paprsek. Její účinnost proti elektronickým zařízením je dokonce vyšší než u elektromagnetického impulsu. V současné době jsou tyto

zbraně ve stádiu zkoušek, při zahájení vojenské operace v Iráku však Spojené státy zvažovaly jejich použití. Vzhledem k vysoké účinnosti proti informačním a komunikačním systémům měly posloužit k paralyzování irácých velitelských stanovišť v podzemních bunkrech. Ty byly sice konstruovány s cílem dosáhnout odolnosti proti pumovým útokům, mikrovlnné záření by však bylo schopné proniknout přes počítačové a energetické sítě, kterými byly bunkry propojeny až do počítačů umístěných uvnitř a způsobit jejich totální zničení. Velení by tak bylo odříznuto od veškerých informačních toků a zcela paralyzováno. Vývoj událostí však probíhal rychleji a úspěšněji, než se před zahájením operace předpokládalo, proto k nasazení těchto zbraní nedošlo. Zkoušky prokázaly, že mikrovlnný paprsek se může odrazit od zemského povrchu a ovlivnit i letouny, pokud dojde k jejich zasažení. V současné době je zvýšená pozornost věnována použití mikrovlnných vyzařovačů velkého výkonu umístěných na bezpilotních prostředcích k úderu proti protivníkovým informačním a komunikačním systémům. Zařazení těchto zbraní do výzbroje plánují, podle Wilsona, Spojené státy v roce 2010. [142]

Kosmická válka

Pod tímto pojmem nelze spatřovat scénáře podobné filmům typu Star Wars, nebo výklady z doby studené války. Na oběžných drahách kolem země však operuje množství družic, včetně vojenských, meteorologických a spojovacích (komunikačních). Všechny jsou zdrojem důležitých informací; zejména obrazových - pořizování snímků družicemi Ikonos nebo Landsat a polohových – z amerického systému GPS[33] nebo ruského GLONASS[34]. Využívání aktuálních snímků z amerických družic je mj. nezbytnou součástí plánování a vedení bezpečnostních operací v Afghánistánu a Iráku. [115] Kromě toho slouží např. k monitorování (a následného vyhodnocování změn) íránského nebo severokorejského jaderného vojenského programu. Globální navigační systémy využívají při přesunech, k rozmístění palebných prostředků a zaměření cílů všechny druhy vojsk. Kromě toho jsou používány i jako jeden z prostředků navigace vojenských letounů a plavidel. Eliminace těchto družic by znamenala přerušení velmi důležitého informačního toku a následně ochromení části řídících systémů míst velení, zejména na strategickém stupni, paralyzování

[33] GPS - Global Positioning System, je Globální družicový navigační systém, který se skládá z pozemního řídícího segmentu, družicového a uživatelského (GPS přijímače pro komerční a vojenské účely).
[34] Glonass – Globalnaja navigacionaja sputnikovaja sistema, je obdobou amerického GPS, ale dosud nemá „globální“ pokrytí.

zbraňových systémů na operačním a taktickém stupni a komplikace přesunu a nasazení bojových jednotek. Zbraněmi, které jsou schopné zlikvidovat družici na oběžné dráze disponovaly dosud pouze Spojené státy a Rusko; jejich zkoušky provedly v 80. letech minulého století. [136] V lednu tohoto roku se však podařilo sestřelit vlastní starší meteorologickou družici pomocí rakety využívající kinetickou energii nárazu i Číně. [73] Zkouška vzbudila značné překvapení a obavy především u Spojených států, protože Čína může nyní teoreticky zasáhnout i cizí družice na oběžné dráze. [27] Pokud by se Čína rozhodla a příslušné technologie prodala i dalším zemím, jako např. Íránu, nebo Pákistánu, byl by i tento typ informačních operací s přibývajícím počtem aktérů v brzké budoucnosti reálný.

Internetová válka

Válka v internetové síti „*netwarfare*“, jak se zdá, by se mohla stát jednou z možných nových forem informační války, jako součást boje proti terorismu. Zahrnovala by v sobě techniky psychologického působení, kybernetické, hackerské války a případně i elektronického boje a působení proti místům velení. Jedná se tedy o součinnost více známých forem informační války. Zvláštnost je však v tom, že se odehrává ve veřejné síti a jejím záměrem není tuto síť zničit, ani pokud možno částečně paralyzovat, protože zároveň může sloužit jako nástroj bezpečnostních složek pro psychologické působení na veřejnost, ale vyhledat roztroušené a skrytě působící teroristické buňky. Toto bojiště lze s trochou představivosti přirovnat k lidskému krevnímu řečišti, kde bílé krvinky bojují s viry. Jeho zničení by tedy neznamenalo vítězství, protože jako je na něm závislý jednotlivec, je na světové síti téměř stejně závislá společnost informačního věku. Její likvidace by samozřejmě neměla takové fatální následky, ale měla by hluboký sociální, kulturní a hospodářský dopad. Jak uvádí Arquilla, teroristé jsou si dobře vědomi významu informační a komunikační techniky pro správné fungování demokratických institucí [7], proto se do budoucna nemusí omezovat pouze na využití internetu ke znásobení účinku fyzických útoků [74], ale mohou se zaměřit na přímé útoky na infrastrukturu. V této souvislosti, pokračuje Arquilla, čeká bezpečnostní složky nebezpečný a velmi obtížný druh boje. Preventivní či odstrašující opatření jsou totiž, uvádí Dunlevy, v kybernetickém světě obtížné, ne-li nemožné. [36]

Ovládnutí cizích informačních a komunikačních systémů

Nepozorované ovládnutí cizích informačních a komunikačních systémů se může na první pohled jevit jako představy z oblasti sci-fi. Ve skutečnosti se však může i tento typ informačních operací stát realitou. V současné době totiž vojenské letectvo Spojených států vyvíjí tzv. systém Suter. Ten je založen na technologii, která údajně umožňuje proniknout do protivníkových informačních a komunikačních systémů bez toho, že by protivník něco takového zaznamenal. Systém nejprve detekuje s vysokou přesností polohu protivníkova vysílače a potom usměrní tok klamných dat přímo do nich. Piloti letounů vybavených systémem Suter mohou údajně monitorovat obraz bojiště, který přináší protivníkovy systémy protivzdušné obrany (zjistí tedy přesně to, co vidí svými prostředky protivník). Systém Suter dokáže kromě „ukradení protivníkova obrazu bojiště“ rovněž klamnými daty ovlivnit pozorovací schopnosti nepřátelské protivníkovy protivzdušné obrany a simulovat klamné (neexistující) cíle, nebo naopak prázdnou oblohu bez letounů. [76] Jedná se o informační operaci podobnou kybernetické válce, s tím, že v případě „klasické“ kybernetické války se předpokládá využití počítačových sítí typu internet, ne však působení na radiolokátory. Systém Suter byl instalován na bojové letouny F-16, létající střediska velení a řízení EC-130 Compass Call a na průzkumné pozorovací letouny RC-135 Rivet Joint. [45] Spojené státy systém, podle dostupných údajů, zkoušely v operacích v Iráku a Afghánistánu. Kromě toho se také spekuluje o pravděpodobném využití této technologie v „ostré akci“ izraelskými bojovými letouny F-15 a F-16 při úderu na syrské vojenské zařízení 6. září 2007. Syrské prostředky protivzdušné obrany, přestože se jedná o moderní systémy ruské výroby, totiž vůbec nereagovaly na průnik izraelských letounů do syrského vzdušného prostoru. Jedna z možností proč se tak stalo je právě nasazení systému Suter a paralyzování syrských zbraňových systémů. [76] Z hlediska informačního je systém Suter dezinformačním zařízením, které je schopno oklamat, tj. doslova vnutit nepravdivé informace nejenom nepřátelským informačním systémům (tedy jiným strojům), ale i jejich obsluhám (lidem).

ZÁVĚR

Význam a důležitost informace se ve vojenství v obecném slova smyslu v brzké budoucnosti nezmění, jak uvádí americká studie *Joint vision 2010*. Zvýší se však přístupnost informací, rychlost jejich přenosu a předávání a rovněž jejich přesnost (přesnost dat získaných z pokročilých senzorů). [67] V současné době se při porovnávání kapacit ozbrojených sil a při odhadování pravděpodobného výsledku jejich konfrontace bere v úvahu zejména faktor fyzické síly a rychlosti (manévrovatelnosti). V budoucnu ho nahradí, podle Moormana, pravděpodobně informovanost - ve smyslu situační připravenosti, tj. schopnosti rychlého nasazení sil a prostředků k obraně vlastních jednotek či k úderu na protivníka. [86] Ani nasazení pokročilých informačních technologií však neodstraní „*válečnou frikci či tření a válečnou mlhu*“ jak o nich hovoří Clausewitz. [24] Cílem bude vždy, aby třenice a komplikace byly na straně nepřítele, aby mlha zhoustla na jeho straně a pro vlastní síly se naopak rozptýlila. V praxi bude proto klíčem k vítězství nad protivníkem dosažení informační převahy a následně informační nadvlády. K té však lze dospět, podle *Joint vision 2010*, pouze účinným vedením informačních operací útočného i obranného charakteru. [67] Předpokládá se, že budou použity tradiční i netradiční formy informačních operací, včetně elektronického boje nebo působení proti místům velení s cílem zmást a oklamat velitele. Výhled do roku 2020 v dokumentu *Joint Vision 2020* dokonce předpokládá výcvik vojenských specialistů určených k vedení informačních operací. [68] Tím dávají Spojené státy, jako vůdčí země v oblasti vojenských technologií, jasně najevo, že sílu informačních operací v žádném případě nepodceňují, naopak vše nasvědčuje tomu, že její význam poroste současně se zvyšující se závislostí společnosti na informačních a komunikačních technologiích.

Podobně uvažují i ruští vojenští odborníci. První zástupce náčelníka ruského generálního štábu generál Alexej Burutin dokonce na fóru o informační bezpečnosti prohlásil, že „*v dohledné budoucnosti nebudou cíle válek a ozbrojených konfliktů dosaženy fyzickým zničením jednotek protivníka, ale paralyzováním vlády a nejvyššího velení, informačních a komunikačních systémů a ovlivněním i dalších informačních institucí, na jejichž funkčnosti je vláda a státní infrastruktura závislá*“. Rusko proto musí být připraveno, pokračoval Burutin, na vedení globální informační války, aby bylo schopné dosáhnout technologické a zejména informační nadvlády nad případným protivníkem. [111]

Jak bude pokračovat technologický rozvoj, budou se rozvíjet i dnes známé typy informačních operací, jako např. kybernetická válka nebo elektronický boj. Nelze ovšem

vyloučit, že vzniknou i zcela nové typy informačních operací, spojené např. s využitím nanotechnologií nebo nových biologických materiálů ve vojenství.

ZÁVĚR

Pokrok v informačních a komunikačních technologiích, v přenosech a sdílení dat zásadním způsobem ovlivnil ozbrojené síly, a to nejenom z hlediska rozvoje informačních systémů,

systémů řízení a vedení palby, ale i z hlediska vedení války. Pravda je, že informační válka je stejně stará jako válka sama a některé typy informačních operací používali schopní válečníci již v dávné minulosti. Stále také platí výrok slavného čínského stratéga Sun Tzu, že „*všechny války jsou založené na klamání*“. [118] Platí i základní zásada vedení války, že cestou k dosažení k vítězství je jedině útok, ne obrana. Technologický pokrok tyto principy nevyvrátil, ani nezměnil. Způsobil však takové organizační a doktrinální změny, že se zásadním způsobem změnil i způsob vedení války. Nekonečné frontové linie, hluboké zázemí, množství kolové a pásové techniky, linkové spojovací prostředky a masivní útoky palebných prostředků, které měnily krajinu k nepoznání, to vše je minulostí. Vystřídalo je bojiště v městských zástavbách, frontu a zázemí dnes již nelze téměř rozlišit, pozemní techniku stále více nahrazují letouny a bezpilotní prostředky, miniaturními bezdrátovými spojovacími prostředky disponuje téměř každý voják v poli a přesně naváděná munice likviduje spolehlivě i nepřátele ukryté mezi civilisty. Nic z toho by však nefungovalo, kdyby mezi všemi jednotkami, zbraňovými systémy a velitelstvími neproudilo množství informací. Právě informace hraje v současném vojenství stále důležitější roli, a jedině ta armáda, která má k dispozici dostatek nejnovějších informací a dokáže je využít může získat informační nadvládu nad protivníkem a dosáhnout vítězství.

Závislost na informačním zabezpečení a vyspělých informačních technologiích má ale i svoji slabou stránku. Bez možnosti informace přijímat, sdílet a šířit je totiž moderní technika prakticky nepoužitelná. Právě zde je místo informačních operací, jejichž zbraněmi i cílem útoku jsou informace a informační technika. Pokud jsou správně vedeny, mohou přerušit tok informací, vyřadit z činnosti zbraňové a informační systémy, spojovací prostředky a dokonce i ovlivnit rozhodovací proces velitelů, morálku jednotek a náladu obyvatelstva. V minulosti používali velitelé při bojových operacích s větším či menším úspěchem některé typy informačních operací, zejména působení proti velení a řízení a psychologickou válku. Ty ještě kombinovali s různými technikami klamání. Mohutný rozmach zaznamenaly informační operace během druhé světové války a některé z nich byly tak úspěšné, že jsou ještě dnes pokládány za nepřekonané. První skutečnou informační válkou se současným využitím různých typů informačních operací najednou však byla první válka v Perském zálivu. Tam se v praxi ukázalo, co znamená dosažení informační nadvlády a dokonalé paralyzování protivníkových jednotek. V současné době vedou koaliční jednotky informační operace v Iráku i Afghánistánu. Kromě toho se osvědčily i v nebojových operacích na podporu míru, jako např. v Bosně a Hercegovině.

V operacích tohoto druhu mají dokonce rozhodující úlohu, protože bojové akce ke stabilitě nepřispějí a vzbudí odpor obyvatelstva. Naopak cíleně vedené informační působení může obyvatelstvo pacifikovat a nenásilně přimět ke spolupráci.

Význam a sílu informačních operací však rozpoznali a některé její formy zvládli příslušníci afghánského hnutí Talibán a zejména globální islámské teroristické organizace. Jejich zbraněmi jsou dnes kromě výbušnin a samopalů i mobilní telefony, počítače a přístupy k internetu. Jeho pomocí znásobují účinky svých fyzických útoků, plánují akce, provádějí finanční transakce, získávají nové členy a psychologicky působí na veřejnost. Všude dostupný internet jim dokonce umožnil změnit hierarchickou organizační strukturu na horizontální a rozptýlenou do malých samostatných buněk. Ty působí skrytě a jsou jen obtížně polapitelné. Jejich informační operace vedené na internetu jsou účinné a bezpečnostní složky na ně zatím nenašly účinnou protizbraň. Vedou sice informační válku proti teroristům a psychologickými operacemi působí na muslimskou komunitu, používají však přitom většinou tradiční sdělovací prostředky. Ty jsou ale ve srovnání s internetem méně účinné. Dosavadní zkušenosti ukazují, že teroristické skupiny typu al-Káida nelze eliminovat bojovými operacemi na taktické úrovni. K jejich potlačení bude nutná kooperace a koordinace vojenských a civilních aktivit a zahájení ofenzivní strategie, včetně naplánování a vedení informačních operací.

Spolu s očekávaným rozvojem informačních a komunikačních technologií se bude zvyšovat význam informačních operací i v brzké budoucnosti. Dojde s velkou pravděpodobností k rozmachu některých typů, jako např. elektronického boje, kybernetické a hackerské války. Použití nanotechnologií, biomateriálů, intenzivnější využívání kosmického prostoru a pokroky v genetice by mohly vést v budoucnu dokonce ke vzniku zcela nových a dosud neznámých typů informačních operací. Pravděpodobně není příliš vzdálená doba, kdy se budou ozbrojené síly porovnávat ne podle množství techniky a manévrovatelnosti, ale podle informačních schopností. Informační operace by proto mohly ve 21. století způsobit tak převratné události, jako ve 20. století způsobil „blitzkrieg“.

Záměrem této práce nebylo dopodrobna analyzovat informační válku a jednotlivé typy informačních operací, ale vytvořit ucelenou přehledovou studii, která by umožnila pochopit pojetí, způsoby vedení a význam informačních operací, tj. využitelnost informací

a informačních systémů ve vojenských operacích. Každá jednotlivý typ informačních operací, historie informačních operací a jejich využití v současných bezpečnostních kampaních jsou natolik rozsáhlá témata, že by si zasloužila samostatné zpracování. Informační operace nejsou samozřejmě omezeny na vojenský sektor, lze je plně uplatnit i při soupeření v komerčním prostředí. Rovněž tato oblast se může stát možným tématem dalších studií.

SEZNAM OBRÁZKŮ

SEZNAM POUŽITÉ LITERATURY

1. AHVENAINEN Sakari. *About Information Warfare*. [online]. January 2000. [cit. 2007-07-14]. 36 s. Dostupný z WWW: <http://www.plutoona.mpoli.fi/dokumentit/iwnet.pdf>
2. ALBERTS David. *Defensive Information Warfare*. Washington : National Defense University, 1996. 80 p. ISBN 07-881-4695-5
3. ALFORD Lionel. Cyber warfare: Protecting Military Systems. *Acquisition Review Quarterly*. Fort Belvoir : Defense Acquisition University, Spring 2000. Dostupný také z WWW: <http://www.dau.mil/pubs/arq/2000arq/alford.pdf>
4. *Al Qaida Dominates Internet*. [online]. Middle East Newsline, a defense news service. December 2007. [cit. 2008-02-15]. Dostupný z WWW: <http://www.menewsline.com/index.html>. Placený komerční zdroj.
5. *Al Qaida Propaganda Plays Key Role In Recruitment*. [online]. Middle East Newsline, a defense news service. August 2007. [cit. 2007-08-09]. Dostupný z WWW: <http://www.menewsline.com/index.html>. Placený komerční zdroj.
6. ANAND Vinod. Chinese Concepts and Capabilities of Information Warfare. *Strategic Analysis*. New Delhi : Institute for Defense Studies and Analyses. Oct-Dec 2006, Vol. 30, No. 4, pp. 781-797. ISSN 0970-0161. Dostupný také z WWW: <http://www.idsa.in/publications/strategic-analysis/2006/oct-dec06/Vinod%20Anand.pdf>
7. ARQUILLA John and others. Networks, Netwar, and Information-age Terrorism. In KHALIZAD Zalmay. *Strategic Appraisal: The Changing Role of Information in Warfare*. Santa Monica : RAND, 2004. 475 p. ISBN 0-8330-2663-1

8. BAMFORD James. The Man Who Sold the War. *Rolling Stone*. New York : Wenner Publishing, November 2005. Dostupný také z WWW: <http://www.rollingstone.com/politics/story/8798997/the_man_who_sold_the_war>

9. BELLAMY Christopher. What is Information Warfare? In MATTHEWS Ron and TREDDENICK John. *Managing the Revolution in Military Affairs*. Basingstoke : Palgrave, 2001. pp. 234-252. ISBN 0-333-78189-9

10. BERKOWITZ Bruce. Warfare in the Information Age. In ARQUILLA John and RONFELDT David. *Preparing for Conflict in the Information Age*. Santa Monica : RAND, 1997. pp. 175-189. ISBN 0-8330-2514-7

11. BITTMAN Ladislav. *Mezinárodní dezinformace, černá propaganda, aktivní opatření a tajné akce*. Praha : Mladá fronta, 2000, 358 s. ISBN 80-204-0843-6

12. BITTMAN Ladislav. *Špionážní oprátky.* Praha : Mladá fronta, 1992, 212 s. ISBN 80-204-0266-7

13. BLAKELY Rhys and RICHARDS Jonathan. UK's Computers Targeted By 120 Countries. [online]. *The Times.* 29 November 2007. [cit. 2008-02-11]. Dostupný z WWW: <http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article2963677.ece>

14. BLOOM Bradley. Information Operation in Support of Special Operations. *Military Review*. Fort Leavenworth : U.S. Army Combined Arms Center in Kansas, January/February 2004. pp. 46-49, ISSN 0026-4148. Dostupný také z WWW: <http://www.iwar.org.uk/iwar/resources/milrev/bloom.pdf>

15. BRIGHT Arthur. Estonia Accuses Russia of „Cyberattack".[online]. *The Christian Science Monitor*. Boston : The First Church of Christ, Scientist, May 2007. [cit. 2008-01-25] Dostupný z WWW: <http://www.csmonitor.com/2007/0517/p99s01-duts.html>

16. BRITZ Johannes. *A critical analysis of information poverty from a social justice perspective*. [online]. Thesis for the degree D Phil, University of Pretoria, October 2006. 247 p. [cit. 2007-08-07]. Dostupný z WWW: <http://upetd.up.ac.za/thesis/available/etd-07212007-122555/unrestricted/00front.pdf>

17. BRZEZINSKI Zbigniew. *Volba: globální nadvláda nebo globální vedení*. Praha : Mladá fronta, 2004. 290 s. ISBN 80-204-1179-8

18. BRZYBOHATÝ Marian. Současný terorismus. *Vojenské rozhledy*. Praha : MO ČR-AVIS, 2002, roč. 11, č. 2, s. 65-79. ISSN 1210-3292

19. BUCHAROVÁ Lenka. *Informační zdroje v oblasti bezpečnosti státu*. Praha, 2006, 102 s. Diplomová práce na Filozofické fakultě Univerzity Karlovy na Ústavu informačních studií a knihovnictví . Vedoucí diplomové práce Richard Papík.

20. BURNETT Peter. *Information Operations*. [online]. USAWC Strategy Research Project, U.S. Army War College, Carlisle, Pennsylvania, April 2002. 24 p. [cit. 2008-02-22]. Dostupný z WWW: <http://www.iwar.org.uk/iwar/resources/carlisle/Burnett_P_L_02.pdf>

21. CEJPEK Jiří. *Informace, komunikace a myšlení : úvod do informační vědy*. Praha : Nakladatelství Karolinum, 2005. 233 s. ISBN 80-246-1037-X

22. CHURCH William. *Kosovo and the future of Information Operations*. [online]. Leeds : University of Leeds, The Institute of Communications Studies. [cit. 2007-08-04]. Dostupný z WWW: <http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&folder=4&paper=1079>

23. CLARKE Ronald and NEWMAN Graemer. *Outsmarting the Terrorists*. Westport : Praeger Security International, 2006. 303 p. ISBN 0-275-99230-6

24. CLAUSEWITZ von Karl. *Vom Kriege.* Translated and edited by HOWARD Michael and PARET Peter. Princeton : Princeton University Press, 1989. 732 p. ISBN 0-691-01854-5

25. COLLINS Steven. Mind Games. *NATO Review*. Brussels : Director of Information and Press NATO, summer 2003, Vol. 51, pp. 13-16

26. COMRAS Victor. Al Qaeda Finances and Funding to Affiliated Groups. [online]. *Strategic Insights*. Monterey : Naval Postgraduate School, Center for Contemporary Conflict, California, January 2005, Volume IV, Issue 1. 19 p. [cit. 2008-01-18] Dostupný z WWW: <http://www.apgml.org/frameworks/docs/7/Al%20Qaeda%20Financing_%20V%20Comras_Jan05.pdf>

27. Concern over China's missile test. [online]. *BBC News*, 19 January 2007. [cit. 2007-08-11]. Dostupný z WWW: <http://news.bbc.co.uk/2/hi/asia-pacific/6276543.stm>

28. *Cornerstones of Information Warfare*. IWS – The Information Warfare Site [online]. [cit. 2007-14-07]. Dostupný z WWW: <http://www.iwar.org.uk/iwar/resources/usaf/iw/corner.html>

29. COX Joseph. *Information Operations in Operations Enduring Freedom and Iraqi Freedom – What Went Wrong?* [online]. A Monograph, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 2006. 127 p. [cit. 2007-08-05]. Dostupný z WWW: <http://www.fas.org/irp/eprint/cox.pdf>

30. DAVIS Jessica. From Kosovo to Afghanistan: Canada and Information Operations. *Canadian Military Journal*. Kingston : Canadian Defence Academy, Autumn 2005. pp. 33-42, ISSN 1492-0786. Dostupný také z WWW: <http://www.journal.forces.gc.ca/engraph/Vol6/no3/home_e.asp>

31. Director of Russian FSB sums up security results of 2007. [online]. *ITAR-TASS*. 21 December 2007. [cit. 2007-12-22]. Dostupný z WWW: <http://www.itar-tass.com/eng/>. Placený komerční zdroj.

32. *Department of Defense Dictionary of Military and Associated Terms.* Washington : Chiefs of Staff, April 2001. 764 p. Joint Publication 1-02. Dostupný také z WWW: <http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf>

33. *Doctrine for Intelligence Support to Joint Operations.* Washington : Chiefs of Staff, March 2000. 84 p. Joint Publication 2-0. Dostupný také z WWW: <http://www.bits.de/NRANEU/others/jp-doctrine/jp2_0.pdf>

34. *Doctrine for Joint Psychological Operations.* Washington : Chiefs of Staff, September 2003. 125 p. Joint Publication 3-53. Dostupný také z WWW: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/02_psyop-jp-3-53.pdf>

35. DRENNAN Shane and BLACK Andrew. *Jihad online – The changing role of the internet*. [online]. Jane's Intelligence Review. July 2007. [cit. 2007-08-09]. Dostupný z WWW: <http://www.janes.com/>. Placený komerční zdroj.

36. DUNLEVY Casey, SHIMEALL Timothy, WILLIAMS Phil. Countering Cyber war. *NATO Review*. Brussels : Director of Information and Press NATO, winter 2001/2002, Vol. 49, pp. 16-19

37. EICHLER Jan. Terorismus a války v dnešním světě. *Mezinárodní politika*. Praha : Ústav mezinárodních vztahů, 2006, č. 10. s. 25-28. ISSN 0543-7962

38. EMERY Norman. Information Operations in Iraq. *Military Review*. Fort Leavenworth : U.S. Army Combined Arms Center in Kansas, May/June 2004. pp. 11-14, ISSN 0026-4148. Dostupný také z WWW: <http://www.iwar.org.uk/iwar/resources/io-in-iraq/emery.pdf>

39. *Encyklopedie špionáže*. Praha : Libri, 1993. 432 s. ISBN 80-901579-1-2

40. Estonia Hit by „Moscow Cyber War". [online]. *BBC News*. 17 May 2007. [cit. 2008-01-25] Dostupný z WWW: <http://news.bbc.co.uk/2/hi/europe/6665145.stm>

41. *Exercise Beef Wellington 5*. Shrivenham : Royal Military College of Science, Cranfield University, 2003. 96 p. Normandy 1944 Study Guide.

42. FARRADANE J. The nature of information. [online]. *Journal of Information Science*, 1979, Vol. 1, No. 13, pp. 13-17. ISSN 1741-6485. [cit. 2007-11-12]. Dostupný z WWW: <http://jis.sagepub.com>. Placený komerční zdroj.

43. FARRIS Kate. *Chinese Views on Information Warfare*. [online]. Final Report, Naval War College, Newport, Rhode Island, April 2000. 51 p. [cit. 2008-01-11]. Dostupný z WWW: <http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA382118&Location=U2&doc=GetTRDoc.pdf>

44. FINNER Jonathan and STRUCK Doug. Bloggers, Money Now Weapons in Information War. *The Washington Post*. Wahington : The Washington Post Company. December 2005. Dostupný také z WWW: <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/25/AR2005122500659.html>

45. FULGHUM David, DORNHEIM Michael and SCOTT William. Pictures Give Insights Into Stealth Projects. [online]. *Aviation Week*. Washington DC : The McGraw-Hill Companies, Inc., 12 February 2005. [cit. 2008-02-11]. Dostupný z WWW: <http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/02145p04.xml>

46. GLOBUS Al, BAILEY David, HAN Jie, JAFFE Richard, LEVIT Creon, MERKLE Ralph, and SRIVASTAVA Deepak. NASA applications of molecular nanotechnology. *The Journal of the British Interplanetary Society*, 1998, Vol. 51, pp. 145-152. Dostupný také z WWW: <http://www.nas.nasa.gov/News/Techreports/1997/PDF/nas-97-029.pdf>

47. GERWEHR Scott and GLENN Russel. *The Art of Darkness: Deception and Urban Operations*. Santa Monica : RAND, 2000. 81 p. ISBN 0-8330-2787-5

48. GREEN Joshua. The Myth of Cyberterrorism. *Washington Monthly*. Wahington : The Washington Post Company, November 2002. Dostupný také z WWW: <http://www.washingtonmonthly.com/features/2001/0211.green.html>

49. HAINES Steven. Genocide, Humanitarian Intervention and International Law. *Working Paper for inclusion in Hudson Papers Vol. II*. Oxford : Oxford University Hudson Trust/Naval Staff, 2004. 32 p.

50. HAWKINS Charles. Coming to Grips With Information Warfare. [online]. *Beijing Special Lecture*. Beijing : China Defense Science & Technology Information Center, March 1997. [cit. 2008-01-29] Dostupný z WWW: <http://www.herolibrary.org/iwa4web.htm>

51. HLUBOČEK Vladimír. Novodobá informační válka na digitálním bojišti. *Computerworld.* Praha : IDG Czech a.s., 2000, roč. 11, č. 10, s. 20-25. ISSN 1210-9924

52. HODICKÝ Jan. Informační věk ve vojenství. In *Informační věk, informační společnost a vojenství.* Praha : MO ČR-AVIS, 2007. Kapitola 4, s. 76-102. ISBN 978-80-7278-379-3

53. HOFFMAN Bruce. *The Use of the Internet By Islamic Extremists*. [online]. Testimony presented to the House Permanent Select Committee on Intelligence. Santa Monica : RAND, May 2006. 20 p. [cit. 2007-08-09]. Dostupný z WWW: <http://www.rand.org/pubs/testimonies/2006/RAND_CT262-1.pdf>

54. HORÁČEK Přemysl. *Informační operace v Afghánistánu*. Praha, MO ČR, červenec 2007. Osobní rozhovor s bývalým příslušníkem mise ISAF.

55. HOŘEJŠÍ Tomáš. V éře e-džihádu. *Euro, ekonomický týdeník*. Praha : Euronews a.s., 26. března 2007, č. 13. s. 50-51. ISSN 1212-3129

56. HUTCHINSON Harold. Iraqi Tribes Turn on al Qaeda. *Strategy Page*. [online]. [cit. 2007-08-06]. Dostupný z WWW: <http://www.strategypage.com/dls/articles2006/200610122619.asp>

57. *Information Management*. Washington : Headquarters, Department Of The Navy, April 2000. 38 p. MCWP 3-40.2. Dostupný také z WWW: <https://www.mfp.usmc.mil/TeamApp/s3/Topics/20070928005709/MCWP%203-40-2%20230707.pdf>

58. *Information Operations.* Washington : Headquarters, Department Of The Army, August 1996. 162 p. FM 100-6. Dostupný také z WWW: <http://www.iwar.org.uk/iwar/resources/usarmyio/fm100-6.pdf>

59. *Information Operatinos*. Washington : Chiefs of Staff, February 2006. 119 p. Joint Publication 3-13. Dostupný také z WWW: <http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf>

60. *Information Operations: Doctrine, Tactics, Techniques, and Procedures*. Washington : Headquarters, Department Of The Army, November 2003. 313 p. FM 3-13. Dostupný také z WWW: <http://www.iwar.org.uk/iwar/resources/doctrine/fm-3-13.pdf>

61. *Information Operatinos Primer*. Carlisle : U.S. Army War College, Philadelphia, November 2006. 168 p. Dostupný také z WWW: <http://www.au.af.mil/au/awc/awcgate/army-usawc/info_ops_primer.pdf>

62. INGWERSEN Peter. *Information Retrieval Interaction.* London : Taylor Graham Publishing, 1992. 256 p. ISBN 0-94756854-9. Dostupný také z WWW: <http://vip.db.dk/pi/iri/files/Ingwersen_IRI.pdf>

63. *Intelligence.* Washington : Headquarters, Department Of The Army, May 2004. 211 p. FM 2-0.

64. *Internet Banking, Hawala and Terrorism*. [online]. London : Medea Group, Analysis, May 2007. 16 p. [cit. 2008-02-15]. Dostupný z WWW: <http://medeagrp.com/index.php?option=com_docman&task=doc_view&gid=6&Itemid=34>

65. JENSEN Owen. Information Warfare: Principles of Third – Wave War. *Aerospace Power Journal*. Alabama : Maxwell AFB, Winter 1994. ISSN 1535-4245

66. *Joint Information Operations Planning Handbook*. Norfolk : Joint Forces Staff College National Defense University Norfolk, Virginia, July 2002. 208 p. Dostupný také z WWW: <http://www.iwar.org.uk/iwar/resources/jiopc/io-handbook.pdf>

67. *Joint Vision 2010*. Washington : Chiefs of Staff. 39 p. Conceptual template of America's Armed Forces. Dostupný také z WWW: <http://www.dtic.mil/jv2010/jv2010.pdf>

68. *Joint Vision 2020*. Washington : Chiefs of Staff. 40 p. Conceptual template of America's Armed Forces. Dostupný také z WWW: <http://www.dtic.mil/jointvision/jvpub2.htm>

69. KARLSSON Roger and HÄGG Magnus. *Counter-terrorism Information Operations*. [online]. Crisis and Risk Network, ETH Zurich. [cit. 2007-08-09]. Dostupný z WWW: <http://www.crn.ethz.ch/_docs/HaeggKarlsson_Counterterrorism%20IO.pdf>

70. KIMMAGE Daniel and RIDOLFO Kathleen. *Iraqi Insurgent Media: The War of Ideas and Images*. Washington : RFE/RL, Inc., An RFE/RL Special Report, June 2007. 74 p. ISBN 978-0-929849-15-7. Dostupný také z WWW: <http://realaudio.rferl.org/online/OLPDFfiles/insurgent.pdf>

71. KIRK Jeremy. Estonia Recovers from Massive DDoS Attack. [online]. *Computerworld*. International Data Inc., May 2007. [cit. 2008-01-25] Dostupný z WWW: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9019725>

72. KLAPÁLEK Karel. *Ozvěny bojů*. Praha : Naše vojsko, 1987. 236 s.

73. KOTRBA Štěpán. Sestřelení družice potvrzeno americkým monitorovacím centrem. [online]. *Britské listy*. 20. ledna 2007, ISSN 1213-1792. [cit. 2007-08-11]. Dostupný z WWW: <http://www.blisty.cz/2007/1/22/art32392.html>

74. LACHOW Irving and RICHARDSON Courtney. Terrorist Use of the Internet: The Real Story. *Joint Force Quarterly*. Washington : National Defense University Press, 2nd quarter 2007, issue 45, pp. 100-103. Dostupný také z WWW: <http://www.ndu.edu/inss/Press/jfq_pages/editions/i45/24.pdf>

75. Letiště s hangáry ve skále. *A-report*. Praha : MO ČR-AVIS, 2007, č. 13, s. 16-17. ISSN 1211-801X

76. LEYDEN John. Israel suspected of hacking Syrian air defence. *The Register*. [online]. 4 October 2007. [cit. 2008-02-11]. Dostupný z WWW: <http://www.theregister.co.uk/2007/10/04/radar_hack_raid/>

77. LIA Brynjar. *Al-Qaeda online: understanding jihadist internet infrastructure*. [online]. Jane's Intelligence Review. January 2006. [cit. 2007-08-09]. Dostupný z WWW: <http://www.janes.com/>. Placený komerční zdroj.

78. LIBICKI Martin. *What Is Information Warfare?* Washington : Institute for National Strategic Studies, 1995. 105 p.

79. LIN C. Abe. Comparison of the Information Warfare Capabilities of the ROC and PRC. [online]. *Internet Security Review*. August 7, 2001, Vol. 2, No. 32. [cit. 2008-01-11] Dostupný z WWW: <http://cryptome.org/cn2-infowar.htm>

80. LÍSKOVÁ Radka. Psychologické operace – stabilní součást moderních vojenských operací. *Vojenské rozhledy*. Praha : MO ČR-AVIS, 2003, roč. 12, č. 2, s. 127-134. ISSN 1210-3292

81. MASARYK Jan. *Volá Londýn*. Praha : Práce, 1948. 323 s.

82. McWILLIAMS Brian. Iraq's Crash Course in Cybewar. [online]. *Information Security News*. May 2003. [cit. 2007-08-05]. Dostupný z WWW: <http://www.wired.com/politics/law/news/2003/05/58901>

83. *Military Deception*. Washington : Chiefs of Staff, July 2006. 79 p. Joint Publication 3-13.4. Dostupný také z WWW: <http://www.fas.org/irp/doddir/dod/jp3_13_4.pdf>

84. MOCKAITIS Thomas. *The „New" Terrorism: Myths and Reality*. Westport : Praeger Security International, 2007. 158 p. ISBN 0-275-98963-1

85. *Monty's Double*. [online]. RAPC Regimental Association. [cit. 2007-07-22]. Dostupný z WWW: <http://www.rapc.co.uk/articles/monty/monty.htm>

86. MOORMAN John. *The Future Role of Information Operations in Operational Art*. [online]. Master's Thesis, Naval War College, Newport, Rhode Island, May 2002. 19 p. [cit. 2007-08-11]. Dostupný z WWW: <http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA405639&Location=U2&doc=GetTRDoc.pdf>

87. MULVENON James. The PLA And Information Age. In MULVENON James and YANG Richard. *The People's Liberation Army in the Information Age*. Santa Monica : RAND Corporation, 1998. 297 p. ISBN 0-8330-2716-6. Dostupný také z WWW: <http://www.rand.org/pubs/conf_proceedings/CF145/>

88. NASTOUPIL Josef. Gerila a internet. *Vojenské rozhledy*. Praha : MO ČR-AVIS, 2006, roč. 15, č. 2, s. 98-104. ISSN 1210-3292

89. NASTOUPIL Josef. Informační válka: způsoby a průběh jejího vedení. *Vojenské rozhledy*. Praha : MO ČR-AVIS, 1999, roč. 9, č. 1, s. 77-84. ISSN 1210-3292

90. NASTOUPIL Josef. Operační klamání. *Vojenské rozhledy*. Praha : MO ČR-AVIS, 2003, roč. 12, č. 2, s. 46-54. ISSN 1210-3292

91. *NATO Glossary of Terms and Definitions*. Brussels : North Atlantic Treaty Organization, NATO Standardization Agenc, 2006. 344 p. AAP-6. Dostupný také z WWW: <http://www.fas.org/irp/doddir/other/nato2006.pdf>

92. NEJEDLÝ Zdeněk. *Hovoří Moskva*. Praha : Odeon, 1977. 150 s.

93. NORDESTE Bruno. *A Framework for Understanding Terrorist Use of the Internet*. [online]. Ottawa : Canadian Centre for Intelligence and Security Studies, 2006. [cit. 2007-08-09]. Dostupný z WWW: <http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp>

94. NOVOTNÝ Karel. K místu a úloze vojenské vědy. *Obrana a strategie*. Brno : Ústav strategických studií Univerzity obrany, 2005, roč. 5, č. 1, s. 123-136. ISSN 1214-6463

95. O'BRIEN Kevin and LEV Izhar. *Information operations and counterterrorism*. [online]. Jane's Intelligence Review. September 2002. [cit. 2007-08-09]. Dostupný z WWW: <http://www.janes.com/>. Placený komerční zdroj.

96. OPPENHEIM Charles, STENSON Joan and WILSON Richard. Studies on Information as an Asset I: Definitions. [online]. *Journal of Information Science*, 2003, Vol. 29, No. 3, pp. 159-166. ISSN 1741-6485. [cit. 2007-11-12]. Dostupný z WWW: <http://jis.sagepub.com>. Placený komerční zdroj.

97. Ó TUATHAIL Gearóid. Post Modern Geopolitics? The Modern Geopolitical Imagination And Beyond. In Ó TUATHAIL and DALBY *Rethinking Geopolitics*. Oxford : Routledge, 1998. pp. 16-38. ISBN 0415172519

98. PACNER Karel. Špinavé triky čili dezinformace jsou věčné. *MF Dnes*. Praha : Marfa a.s., červen 2002. Dostupný z WWW: <http://zpravy.idnes.cz/vedatech.asp?r=vedatech&c=A020603_145443_vedatech_jan&r2=vedatech>

99. PACNER Karel. Zavinil Beneš maršálovu smrt? *MF Dnes*. Praha : Marfa a.s. 2002. Dostupný z WWW: <http://zpravy.idnes.cz/vedatech.asp?r=vedatech&c=A020129_105324_vedatech_jan>

100. PFAU Michael and others. Embedded Reporting During the Invasion and Occupation of Iraq: How the Embedding of Journalists Affects Television News Reports. *Journal of Broadcasting & Electronic Media*. Tempe : Arizona State University, December 2005, Vol. 49, No. 4, pp. 468-487. Dostupný z také WWW: <http://www.leaonline.com/doi/pdfplus/10.1207/s15506878jobem4904_7?cookieSet=1>

101. POTŮČEK Jan. Berka: dezinformace je legitimní součástí konkurenčního boje. [online]. *RadioTV*. Praha : Limemedia, 2004. 4 s. ISSN 1214-0279. [cit. 2008-01-18] Dostupný z WWW: <http://www.radiotv.cz/radio-clanky/2894/xxx.html>

102. POŽÁR Josef. Některé trendy informační války, počítačové kriminality a kyberterorismu. *Kriminalistika*, 2005, roč. 38, č. 4, s. 265-275. ISSN 1210-9150

103. PROCHÁZKA Josef. Psychologické a informační operace. *Vojenské rozhledy*. Praha : MO ČR-AVIS, 2001, roč. 4, č. 1, s. 124-136. ISSN 1210-3292

104. *Psychological Operations*. Washington : Headquarters, Department Of The Army, August 1979. 257 p. FM 33-1. Dostupný také z WWW: <http://www.fas.org/irp/doddir/army/fm33-1/index.html>

105. RENNSTICH Joachim Karl. *War In The Digital Age: Informational Power, Geopolitics, And The Fifth Dimension*. [online]. Philadelphia : Temple University, March 2003. 22 p. [cit. 2007-07-07]. Dostupný z WWW: <http://www.fordham.edu/politicalsci/profs/rennstich/pdfs/JKR03-War_Digital_Age.pdf >.

106. RESSLER Miroslav. *Informační věda a knihovnictví : výkladový slovník české terminologie z oblasti informační vědy a knihovnictví*. Praha : Vysoká škola Chemicko- technologická v Praze, 2006. 161 s. ISBN 80-7080-599-4

107. ROGAN Hanna. *Jihadism Online - A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes*. [online]. FFI/Rapport-2006/00915. Kjeller : Forsvarets Forskningsinstitutt, Norwegian Defence Research Establishment, 2006. 36 p. [cit. 2007-08-09]. Dostupný z WWW: <http://rapporter.ffi.no/rapporter/2006/00915.pdf>

108. ROMANYCH Marc. Tactical Information Operations in Kosovo. *Military Review*. Fort Leavenworth : U.S. Army Combined Arms Center in Kansas, September/October 2004. pp. 56-61, ISSN 0026-4148. Dostupný také z WWW: <http://www.au.af.mil/au/awc/awcgate/milreview/romanych.pdf>

109. ROTHENBERG Gunther. *The Art of Warfare in the Age of Napoleon*. Indiana : Indiana University Press, 1978. 272 p. ISBN 0253310768

110. RULF Eduard. *Volá Káhira 1939-1945. Vzpomínky na čs. Vojenské rozhlasové vysílání z Káhiry*. Olomouc : Votobia, 2000. 573 s. ISBN 80-7198-403-5

111. Russia should be ready for global information war – general. *ITAR-TASS*. [online]. 31 January 2008. [cit. 2008-02-12]. Dostupný z WWW: <http://www.itar-tass.com/eng/>. Placený komerční zdroj.

112. SCHMITT Michael. *Counter-Terrorism and the Use of Force in International Law*. Garmisch-Partenkirchen : The Marshall Center Papers, 2002, 107 p. ISBN 1-930831-08-0

113. SCHROEDER Sebastian and Wilton David. *Potential Impact of Information Operations and Possible Countermeasures: Evidence from the Financial Services Sector*. [online]. Massey : Institute of Information and Mathematical Sciences, Massey University Auckland, New Zealand, December 2006. 5 p. Postgraduate Infosec Research Project presented to the 23rd Chaos Communication Congress, Köln. [cit. 2008-02-23]. Dostupný z WWW: <http://events.ccc.de/congress/2006/Fahrplan/attachments/1177-IOPaper.pdf>

114. SCHWARTAU Winn. *Information Warfare: chaos on the electronic superhighway*. New York : Thunder's Mouth Press, 1994. 432 p. ISBN 1-56025-080-1

115. SEPPÄLÄ Tiina. *"New wars" and old strategies: From traditional propaganda to information warfare and psychological operations.* [online]. Lapland : University of Lapland, July 2002. 18 p. Paper presented to the 23 Conference and General Assembly AMCR/AIECS/AIERI International Association for Media and Communication Research, Barcelona. [cit. 2007-07-24]. Dostupný z WWW: <http://www.portalcomunicacion.com/bcn2002/n_eng/programme/prog_ind/papers/s/pdf/s001_sepal.pdf>

116. SHY John. Jomini. In PARET Peter. *Makers of Modern Strategy. From Machiavelli to the Nuclear Age.* Oxford : Clarendon Press, 1986. pp. 143-185. ISBN 0-19-820097-8

117. STOLL Clifford. The cuckoo's egg : tracking a spy through the maze of computer espionage. New York : Pocket Books, 1990. 356 p. ISBN 0671726889

118. SUN TZU. *The Art of War*. Translated by GRIFFITH Samuel. Oxford : Oxford University Press, 1971. 197 p. ISBN 0-19-501476-6

119. SVOBODA Oldřich a kolektiv. *Stručný slovník vojenství*. Praha : Naše vojsko, 1984. 374 s.

120. SZAFRANSKI Richard. A Theory of Information Warfare: Preparing for 2020. *Airpower Journal*. Alabama : Maxwell AFB, College of Doctrine Aerospace Research and Education, 1995. ISSN 0897-0823

121. ŠEDIVÝ Jiří. Boj proti terorismu není válkou. *Hospodářské noviny*. Praha : Economia a.s., 2001. s. 12. ISSN 1213-7693.

122. *Terminologický slovník zpravodajství*. [online]. Praha : Vojenské zpravodajství, 2005. [cit. 2007-07-28]. Dostupný z WWW: <http://www.vzcr.cz/?id=pojmy&styl=graphic>

123. *The Oxford Companion to Military History*. Edited by HOLMES Richard. Oxford : Oxford University Press, 2003. 1048 p. ISBN 0-19-860696-6

124. *The Secrets of Bletchley Park*. Bletchley Park : The Bletchley Park Trust, 2003. 24 p. Souvenir Guide

125. THOMAS L. Timothy. China's Electronic Strategies. [online] . *Military Review*. Fort Leavenworth : U.S. Army Combined Arms Center in Kansas, May/June 2001. ISSN 0026-4148. [cit. 2008-01-11]. Dostupný z WWW: <http://leav-www.army.mil/fmso/documents/china_electric/china_electric.htm>

126. THOMAS L. Timothy. Russian Views On Information-Based Warfare. *Airpower Journal*. Alabama : Maxwell Airforce Base, July 1996, Special Edition. pp. 25-35. ISSN 0897-0823

127. TURZA Pavol. *Mým bojištěm nebyly zákopy*. Praha : Naše vojsko, 1985, 224 s.

128. URBANOVSKÝ Svatopluk. Maskování – nezbytná součást vojenského umění. *Vojenské rozhledy*. Praha : MO ČR-AVIS, 1998, roč. 8, č. 1. ISSN 1210-3292

129. *US forces find Al-Qa'idah media production room in Samarra*. London : Quds Press news Agency, 5 Aug, 2007. Open Source Center. Dostupný z WWW: <https://www.opensource.gov>. Veřejnosti nepřístupný zdroj.

130. VALLEY Paul. *From PSYOP to MindWar: The Psychology of Victory*. [online]. San Francisco : Report, Headquarters, 7th Psychological Operations Group, United States Army Reserve, Presidio of San Francisco, California. 1980. 10 p. [cit. 2008-02-05]. Dostupný z WWW: <http://www.xeper.org/maquino/nm/MindWar.pdf>

131. VELÍŠEK Jaroslav. Elektronický boj. *Vojenské rozhledy*. Praha : MO ČR-AVIS, 2000, roč. 10, č. 2, ISSN 1210-3292. Dostupný také z WWW: <http://www.vrtulnik.cz/mil/reb-eb.htm>

132. VICKERY Brian. *Information science – part 1*. [online]. [cit. 2007-08-07]. Dostupný z WWW: <http://www.lucis.me.uk/infosci1.htm#start>

133. VICKERY Brian C., VICKERY Alina. *Information Science in Theory and Practice*. München : K. G. Saur Verlag GmbH, 2004. 393 p. ISBN 3-598-11658-6

134. *Výkladový slovník pojmů a definic NATO*. Praha : MO ČR, Oddělení pro koordinaci standardizace, 1998. 250 s. Pomůcka AAP-6.

135. WALTZ Edward. *Information Warfare, Prinicples and Operations*. Boston : Artech House Publishers, 1998. 397 p. ISBN 0-89006-511-X

136. WATSON Rob. China test sparks space arms fears. [online]. *BBC News*. 19 January 2007. [cit. 2007-08-11]. Dostupný z WWW: <http://news.bbc.co.uk/2/hi/asia-pacific/6278867.stm>

137. WEBBER Sheila. Information Science in 2003: A Critique. [online]. *Journal of Information Science*, 2003, Vol. 29, No. 4, pp. 311-330. ISSN 1741-6485. [cit. 2007-11-12]. Dostupný z WWW: <http://jis.sagepub.com>. Placený komerční zdroj.

138. WEBBER Sheila and JOHNSTON Bill. Conceptions of information literacy: new perspectives and implications. [online]. *Journal of Information Science*, 2000, Vol.

26, No. 6, pp. 381-397. ISSN 1741-6485. [cit. 2007-11-12]. Dostupný z WWW: <http://jis.sagepub.com>. Placený komerční zdroj.

139. WEIMANN Gabriel. How Modern Terrorism Uses the Internet. *The Journal of International Security Affairs*. [online]. Washington : Jewish Institute for National Security Affairs, Spring 2005, No. 8. [cit. 2007-08-09]. Dostupný z WWW: <http://www.securityaffairs.org/issues/2005/08/weimann.php>

140. WELCH Donald, BUCHHEIT Nathan and RUOCCO Anthony. *Strike Back: Offensive Actions in Information Warfare*. [online]. New Security Paradigms Workshop, Caledon Hills, Ontario, Canada, 1999. pp. 47-52. [cit. 2007-08-11]. Dostupný z WWW: <http://delivery.acm.org/10.1145/340000/335192/p47-welch.pdf?key1=335192&key2=9541386811&coll=&dl=&CFID=15151515&CFTOKEN=6184618>

141. WHALEY Barton. Toward a General Theory of Deception. *The Journal of Strategic Studies*. London : Strategic Studies Institute, 1982, vol. 5, No. 1, pp. 178-192

142. WILSON Clay. *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*. [online]. Washington : Congressional Research Service, April 2006. 21 p. CRS Report for Congress. [cit. 2008-02-12] Dostupný z WWW: <http://fas.org/sgp/crs/natsec/RL32544.pdf>

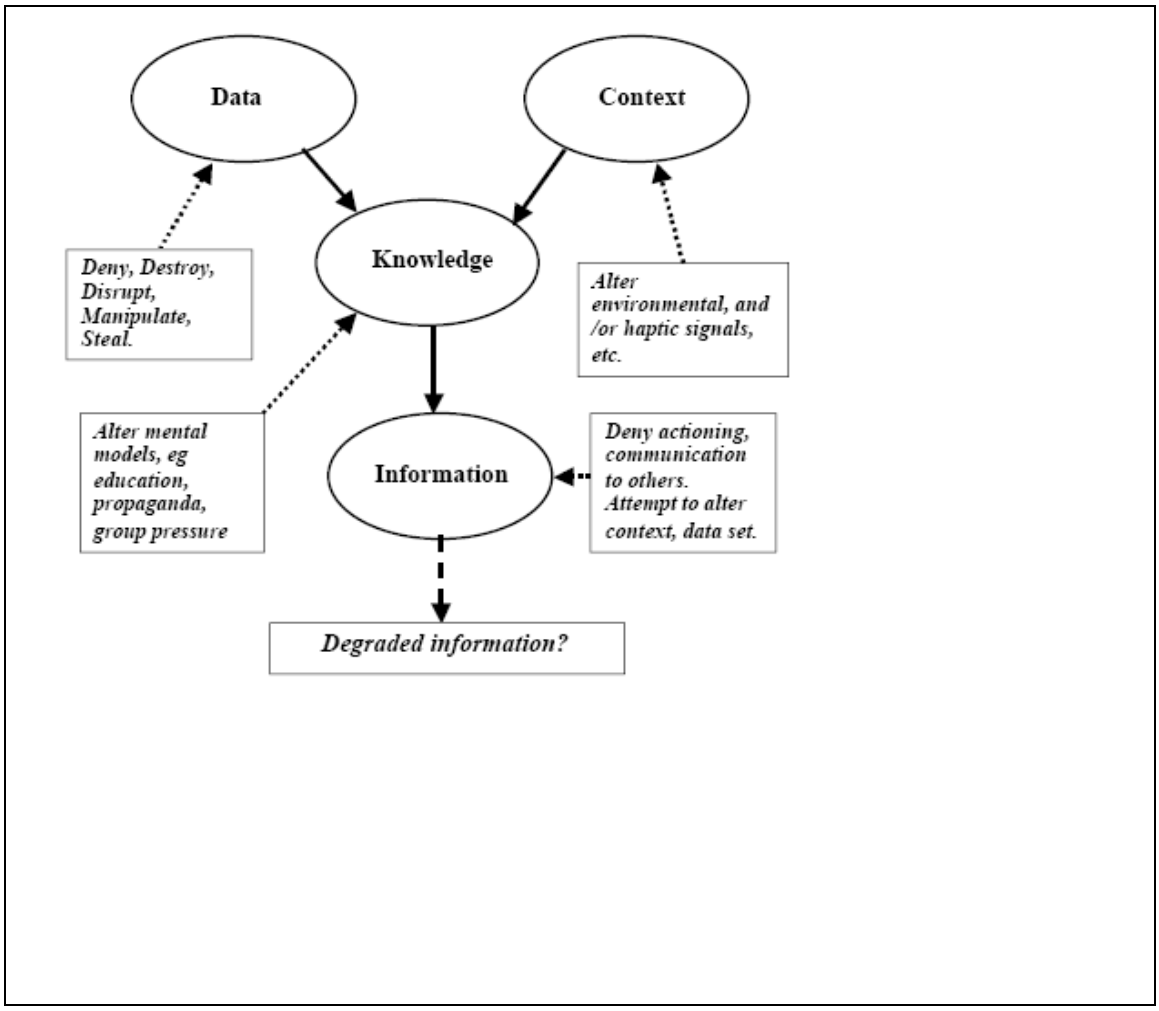
143. WILSON Clay. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues* [online]. Washington : Congressional Research Service, March 2007. 18 p. CRS Report for Congress. [cit. 2007-07-26] Dostupný z WWW: <http://www.fas.org/sgp/crs/natsec/RL31787.pdf>

144. YURCIK William. *Information Warfare Survivability: Is the Best Defense a Good Offense?* [online]. Published in Proceedings of the 5th Annual Ethics and Technology Conference, Loyola University, Chicago, Illinois, 2000. 18 p. [cit. 2007-08-11]. Dostupný z WWW: <http://www.projects.ncassr.org/hackback/ethics00.pdf>

145. ZADRAŽILOVÁ Iva. *Informace a dezinformace*. [online]. Brno, 2007, 5 s. Studentská konference InfoKon, Filozofická fakulta Masarykovy Univerzity. [cit. 2008-01-18]. Dostupný z WWW: <http://www.phil.muni.cz/vik/InfoKon/files/zadrazilova.pdf>

SEZNAM PŘÍLOH

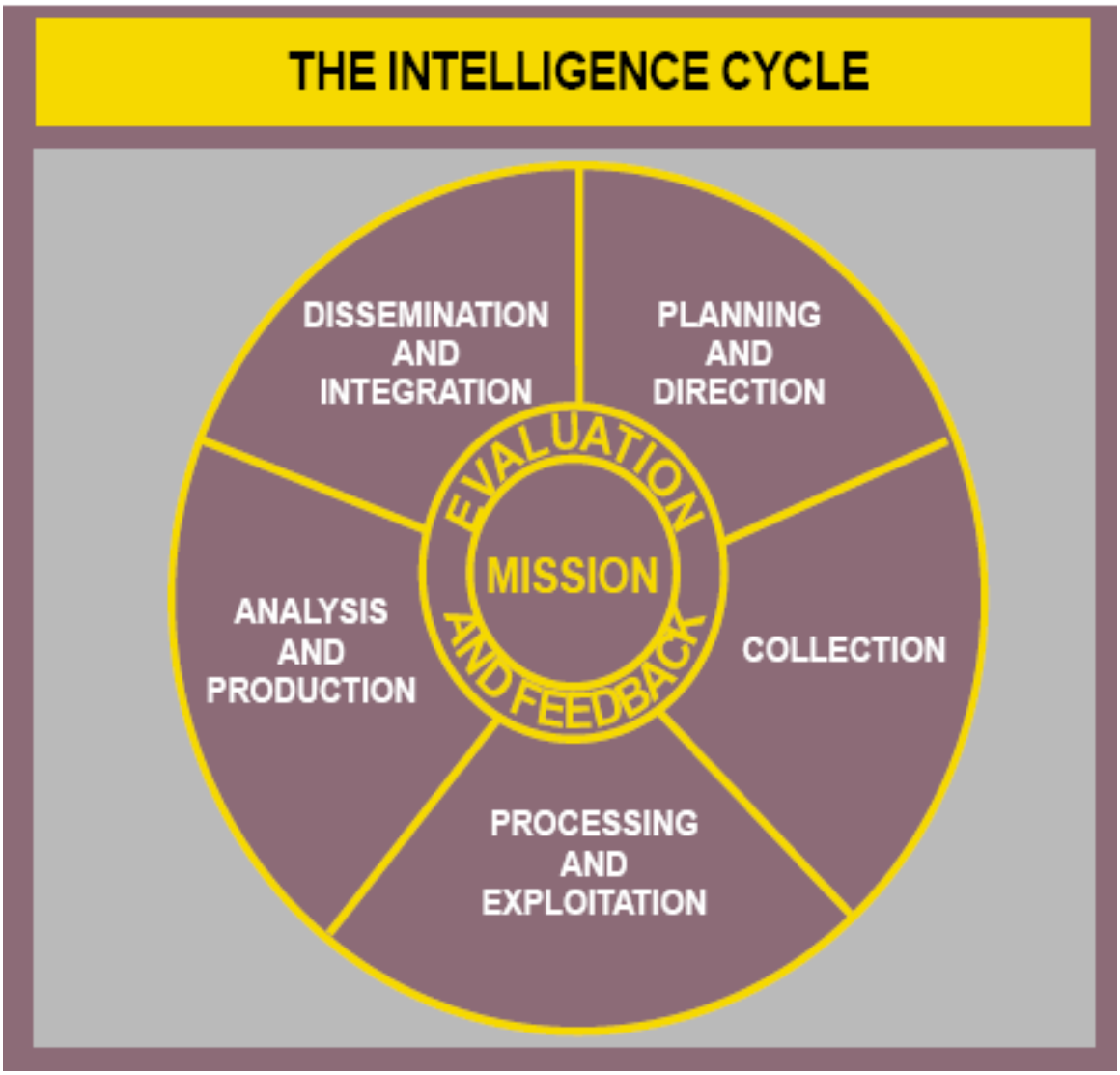
PŘÍLOHA Č. 1 – Informační útoky na součásti komunikačního procesu



Zdroj: HUTCHINSON William and WARREN Matt. Principles of Information Warfare.

PŘÍLOHA Č. 2 – Zpravodajský cyklus

Pět fází zpravodajského cyklu podle americké Doktríny pro zpravodajskou podporu společných operací.



Zdroj: Doctrine for Intelligence Support to Joint Operations

PŘÍLOHA Č. 3 – Leták shazovaný nad územím protektorátu z britských letounů

Obě strany letáku, který shazovali nad územím protektorátu britští a českoslovenští letci k morální podpoře obyvatelstva. Měl připomenout výročí založení samostatného Československa.

Poselství britských a československých letců k 28. říjnu

25

PRAVDA VÍTĚZÍ

LIDU ČESKOSLOVENSKÉMU!

PO řadě dvacátých osmých říjnů, jejichž velký národní význam nikdy nesejde z myslí nás všech, padlo před třemi roky temno na náš den svobody.

Před třemi roky nastoupil náš národ novou křížovou cestu. Německé barbarství, vybičované zvrácenou ideologií nacistickou a sesílené moderní technikou, dolehlo opět na naše země. Po Ferdinandovi—Heydrich, po Koniášovi—Frank. Ošklivá pověst o německých drakonádách sedmnáctého století u nás zanikla a zcela vybledla před bezohledností, krutostí a nenasytností dnešních nacistických dobyvatelů.

Hrůzy a útrapy, které v tomto roce prožíváte, jsou jistě vyvrcholením Vašeho utrpení. Letošní dvacátý osmý říjen je pro Vás zatím dnem smutku. Leč jest jedna útěcha, která Vás a Vaše odhodlání může posilovat: Není před Vámi tři sta let poroby, ani ne tři leta. Snad už ani ne rok!

Nedejte se klamat proradnou a lživou německou propagandou. Není všechno skutečným vítězstvím, co německý rozhlas hlásá do světa a uvádí hlučným vířením bubnů. Snad je to právě ta hlučná hudba, která má zaplašit v duších Němců strach před zúčtováním, které je neodvratné.

Nacisté dobře vědí, na čem jsou. Svojí filosofií o nadřaděnosti své rasy, svojí touhou po zotročení jiných národů a po ovládnutí světa, svojí ukrutností a barbarským ničením kultury vzbudili proti sobě nenávist celého světa. Němců je 85 milionů a z těch daleko ne všichni jsou nacisté. Proti nim stojí přes 500 milionů lidí v britské říši, přes 180 milionů Rusů a více než 130 milionů občanů Spojených Států. A připočtěte všechny ostatní v Evropě — Poláky, Jugoslávce, Řeky, Nory a Francouze a nás i Vás, kteří všichni čekají na znamení, aby povstali a zúčtovali s německým zlem, které bude vždy představovat nejčernější kapitolu v dějinách lidstva.

Vy, právě jako my, bedlivě sledujete poměry v Německu a víte jistě dobře o vnitřním rostoucím rozvratu uvnitř nacistické strany, která dnes Německo ovládá. Vzpomeňte roku 1918, kdy německé noviny až do poslední chvíle přinášely honosné zprávy o německých vítězstvích, až jednoho dne — prostě nevyšly.

Netruchleme dnes nad československou republikou, neboť ona nezemřela. Žije dále v srdcích nás všech a brzy povstane opět nová, svobodná a krásnější než byla. V naší zemi, na mohyle slavkovské, jsou na rudé žule zlatým písmem napsána slova biblického proroka:

„Moji zavraždění povstanou z mrtvých."

I naši mrtví a všichni ti Heydrichem popravení vlastenci českoslovenští, kterých dnes vzpomínáme, povstanou. Povstanou jako mstitelé a aby viděli, že nezemřeli nadarmo. Po hrůze větší, než byla pobělohorská, musí přijít také těžší trest, než byl po dvacátém osmém říjnu 1918. A musí přijít také lepší život, o nějž bojujeme a pro nějž Vy dnes trpíte.

Přinášíme Vám pozdrav presidenta československé republiky Edvarda Beneše. Neseme Vám pozdrav československé vlády. Neseme Vám hold československé armády ve Velké Britanii, na Rusi a na blízkém Východě. Neseme Vám hold a prosbu Mistra Jana Husi: „K poznané pravdě stůjte."

Vytrvejte! Vítězství patří nám a jeho chvíle není daleká!

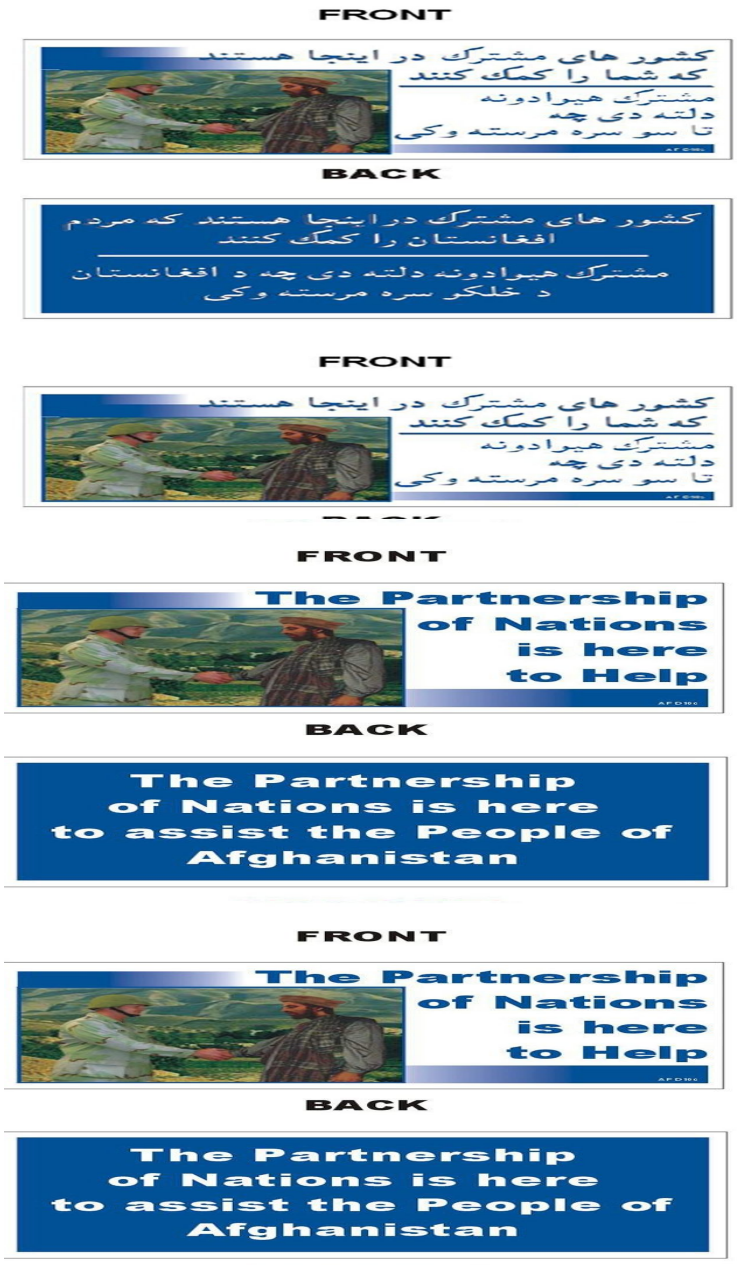
Pozdravy od československých letců k 28. říjnu

456

Zdroj: Vojenský historický archiv v Praze

PŘÍLOHA Č. 4 – Leták shazovaný při zahájení operace Trvalá svoboda v Afghánistánu

Obě strany letáku shazovaného z koaličních letounů v rámci psychologické války během počáteční fáze operace Trvalá svoboda v Afghánistánu.



Zdroj: The Information Warfare Site

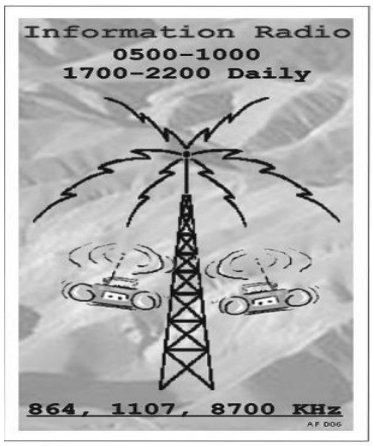
PŘÍLOHA Č. 5 – Leták shazovaný v průběhu operace Trvalá svoboda v Afghánistánu

Obě strany letáku shazovaného z koaličních letounů v rámci psychologické války v průběhu operace Trvalá svoboda Afghánistánu.

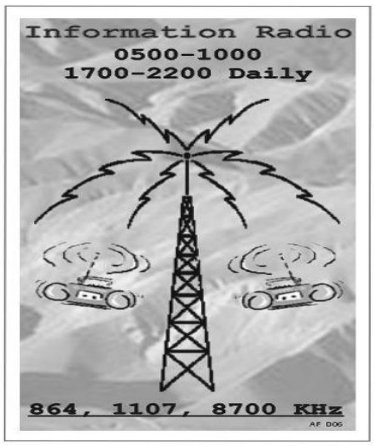
FRONT

BACK

FRONT



BACK



Zdroj: The Information Warfare Site

Evidence výpůjček

Prohlášení:

Dávám svolení k půjčování této rigorózní práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

V Praze dne 5. 3. 2008 Vít Černovský

Jméno	Katedra / Pracoviště	Datum	Podpis