Doktrína informačních operací

(Americká koncepce)

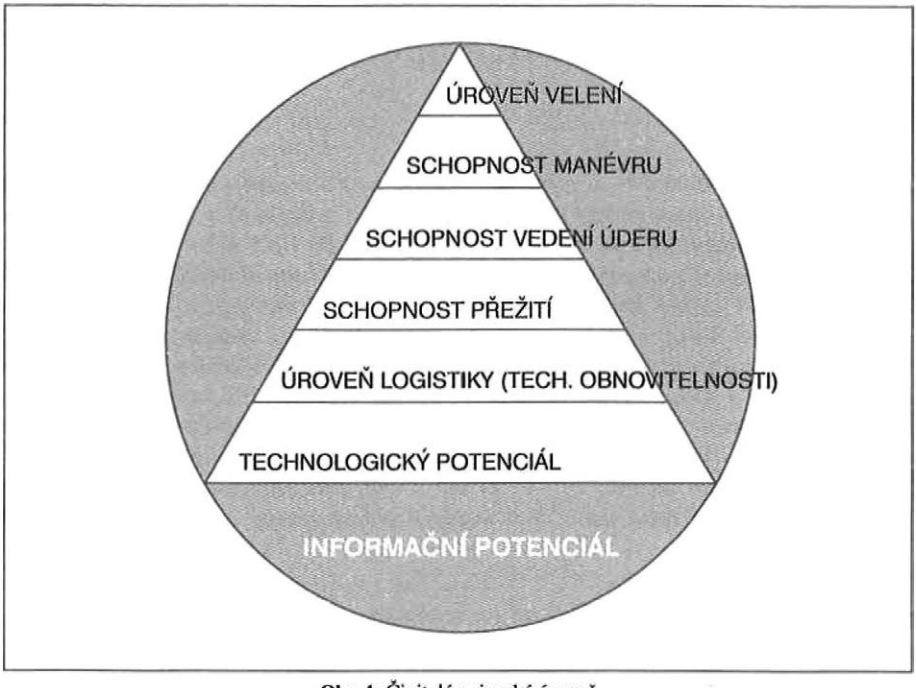
Poslední roky narůstá četnost publikací, v jejichž názvu se vyskytuje termín informační válka nebo termín jemu podobný. Tyto publikace „si pohrávají" s tezemi obsaženými v doktrinálních dokumentech Ministerstva obrany (DoD) USA nebo výboru náčelníků štábů (JCS) a zpravidla opomíjejí uvádět zdroje. Z jejich obsahu máme dojem, jako by celý svět projednával „války řízené počítačovými centry". Tento dojem zesilují oficiální předpovědi nové doktrinální koncepce typu ***Network-Centric Warfare****. Ve skutečnosti takovéto využívání počítačů zahrnuje pouze nepatrnou část informačních operací, zatímco cíle, organizace a postupy s tím spojené jsou rozpracovány v příslušných dokumentech. Cílem tohoto článku je seznámit čtenáře s koncepcí informačních operací v návaznosti na oficiální dokumenty Ministerstva obrany USA. Jsou to prakticky jediné dostupné zdroje z této oblasti. Třeba přiznat, že tyto zdroje určují základní referenční materiál pro vypracování národní nebo koaliční doktríny v oblasti tvorby informačních proporcí obranného potenciálu.*

Činitelé vojenské úrovně

Je třeba zdůraznit, že **vojenská doktrína NATO, a to především Spojených států, je založena na koncepci** ***mnohofaktorové vojenské převahy*** *(multifactor military superiority)* s podporou cílené a rozhodující převahy informací *(information superiority)* a převahy technologické *(technological superiority)*. Stejně tak je znázorněna strategie tvorby obranného potenciálu v doktrinálních dokumentech ze svazků *Joint Publication Hierarchy* Ministerstva obrany USA, a tento princip, více či méně se s ním shodující, dodržují i ministerstva obrany ostatních zemí Aliance. Zjednodušenou strukturu této koncepce ukazuje **obr. 1**. Ten zdůrazňuje podstatu doktríny - totiž že tzv. **operační činitelé vojenské převahy** (úroveň velení, schopnost manévru, schopnost vedení úderů, schopnost přežití, úroveň logistiky) spočívají na **převaze technologické**. Do praxe se mohou úspěšně zavádět na reálném nebo hypotetickém (chybí-li účinné odstrašování) bojišti za podmínek rozhodující převahy informací.

*

Různé formy informačních opatření mají dlouhou historii. Dosud se jednalo o aktivity v oblasti diplomacie, rozvědky, kontrarozvědky a propagandy, ale také v oblasti ochrany vědních poznatků a technologií (politika embarga). Rostoucí závislost všech oblastí fungování společnosti, bojové techniky a systémů velení vojskům (řízení obranného potenciálu) na informační infrastruktuře vytvořila nové možnosti i nová ohrožení. Úroveň informací se stala činitelem podmiňující kvalitu vojenských doktrín, jejichž základem je dynamické vytváření lokálních ohnisek rozhodující převahy bojového potenciálu na konkrétním místě a v konkrétním čase.



Obr. 1: Činitelé vojenské úrovně

Ve shodě s americkými koncepcemi mají tato opatření za cíl paralyzovat či zneschopnit informační potenciál protivníka a rovněž chránit vlastní informační potenciál. Pravděpodobně budou ovlivňovat základní prvky vedení ozbrojeného boje na bojišti, jejichž poměr, pokud jde o následujících pět - manévr, zpravodajství a REB, protivzdušná obrana, palebná podpora, služby bojového zabezpečení *(Maneuver Control, Intelligence/EW, Air Defense, Fire Support, Combat Services Support)* - je dosud určen způsobem dosti nejasným.

Doktrinální dokumenty informačních operací

Směrnice pro vypracování doktrinálních dokumentů byly v tomto rozsahu obsaženy v nařízení Ministerstva obrany USA *Information Operations* a též v instrukcích předsedy výboru náčelníků štábů *(Chairman of the Joint Chiefs of Staff): 3210.1A - Joint Information Operations Policy* a *6510.01B - Defensive Information Operations Implementation* Ty stanovily základ pro zpracování dvou doktrinálních dokumentů: *Joint Doctrine for Information Operations (Joint Pub 3-13)* a *Joint Doctrine for Command & Control Warfare - C2W (Joint Pub 3-13.1).*

První z výše uvedených dokumentů definuje doktrínu informačních operací prováděných v době míru, narůstání válečného nebezpečí a v době války. Informační operace prováděné v době války se nazývají *Information Warfare* (informační boj, informační bojová činnost atp. - dosud nebyl specifikován a ujednocen oficiální polský

termín). *Command & Control Warfare* soustřeďují pozornost na poměr mezi systémy velení válčících stran. Z důvodu toho, že dosud neexistuje adekvátní polský termín, zůstaneme u původního *C2 Warfare.*

Informační potenciál a jeho struktura

Informační potenciál, jako jeden z činitelů vojenské úrovně, se skládá z následujících prvků:

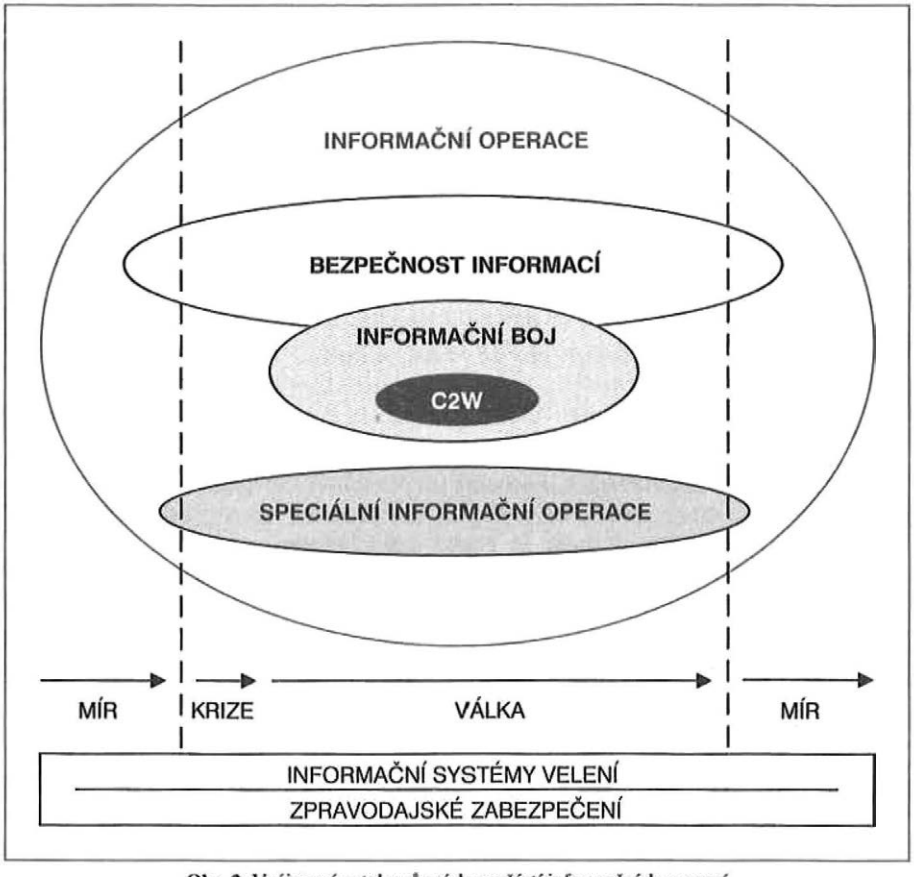
- ***nepřetržité (institucionální) faktografické vědní poznatky***, spojené se všemi činiteli této úrovně (např. současné rozložení a činnost vojsk protivníka, jeho strategické, operační a taktické zámysly, takticko-technická data výzbroje atp.),
- ***nepřetržité (institucionální) obecné vědní poznatky***, tzn. výsledky vědeckých výzkumů spojených s obranou, technologie, metodiky řešení operačně-taktických problémů, včetně metodiky hodnocení situace a přijetí rozhodnutí, plánování operací atp.,
- ***lidé zapojení v informačních procesech*** (např. velitelsko-štábní skupiny, skupiny, které programují rozvoj ozbrojených sil, skupiny, které realizují vědecko-výzkumné programy) spolu se svými individuálními poznatky a vzděláním, i emotivním vztahem a motivacemi,
- ***informační infrastruktura*** zahrnující infrastrukturu senzorovou, telekomunikační a infrastrukturu založenou na bázi informatiky (*Joint Intelligence Support to Military Operations*, Joint Pub 2-01.), jež je spojena s bezpečností státu a která funguje v rámci zpravodajských systémů, velení vojskům a řízení bojových prostředků.

Informační potenciál, jakožto jeden z činitelů potenciálu vojenského, je však tvořen také **nepřímými činiteli**. Jsou to:

- ***úroveň informací nevojenské sféry chodu státu*** (státní správy, oblastní správy, finančních institucí, vědeckého a výzkumně-vývojového zázemí, energetiky, telekomunikací, dopravy atp.),
- ***úroveň informací institucí rezortu obrany***, včetně orgánů odpovědných za programování vývoje a vývoj ozbrojených sil,
- ***úroveň informací ozbrojených sil.***

Důležitou úlohu zde sehrávají **strategické informační soubory**. Jsou tvořeny těmi součástmi vědních poznatků, které jsou důležité pro národní zájmy a které vyžadují důkladnou evidenci, unifikaci a aktualizaci, jakož i zvláštní ochranu. Část strategického informačního potenciálu zahrnuje armádní administrativa nebo spadá organizačně pod informační infrastrukturu ozbrojených sil.

Doktrína zdůrazňuje, že rysem současné „technologií ovlivněné" civilizace je organizace informačního potenciálu na informační systémy s rozvětvenou a vzájemně provázanou strukturou. Faktografické a procedurální lidské poznatky byly totiž přeneseny z knih a sejfů do databází pro zavedené programy počítačů, a to se v závislosti na stálosti a hodnověrnosti oběhu informací stalo kritickým. Tyto systémy jsou citlivé na fyzickou destrukci a informační diverzi, která je založena na zborcení



Obr. 2: Vzájemné vztahy různých součástí informačních operací

informačních souborů hackery nebo na jejich záměně, vedení informačního provozu v rozporu se zákonnými postupy, na provádění nepovolených procedur tvorby dat atp. Jednoznačně se jedná o systémy velkou měrou vystavené (alespoň dosud) počítačové rozvědce, založené na „hackerském" zneužívání vědních poznatků shromážděných v jejich souborech. Z tohoto rysu informačních systémů vyplývá na jedné straně ohrožení bezpečnosti vlastní země, na straně druhé se pak vytváří možnosti analogického vlivu na informační systémy potenciálního protivníka.

Tato situace způsobila nezbytnost „doktrinizace" informačních operací, výsledkem čehož jsou výše uvedené dokumenty rezortu obrany USA.

Je třeba zdůraznit možnou různorodost ovlivňovaného působení na informační potenciál v závislosti na specifikách prvků, ze kterých se skládá.

Například:

- *faktografický i obecný vědní poznatek* může být **blokován** (ochrana vlastních souborů, jejich „maskování"), **ničen** nebo **zaměněn za falešný** (vniknutím do

informační infrastruktury protivníka a fyzickým zničením nebo záměnou informací či postupů jejich tvorby), **manipulován** (rozvíjením klamných velitelských stanovišť), **zpochybňován** (zvětšením míry neurčitosti) atp.,

- *lidské hodnoty v informačních procesech* mohou být **paralyzovány** působením prostředků psychologického boje nebo manipulováním pomocí vytříděných či selektivně zpřístupněných informací (včetně vědeckých), dokumentů a též během speciálně zorganizovaných informačně-společenských sezení.
- *informační infrastruktura* může být **zneschopněna** působením falešného telekomunikačního provozu nebo zborcením programů použitím virů, zanesených do nitra systému operací *C2 Warfare* a zavedeným dodavatelem počítačové soupravy (nebo programu) a jeho aktivací v daném momentě.

Cílem informačních operací je působení na informační systémy a informační potenciál protivníka a zároveň obrana vlastních systémů a potenciálu před informačními operacemi protivníka (*Joint Doctrine for Information Operations*, Joint Pub 3-13.)

Doktrinálním rozkazem jsou do informačních operací zapojeny všechny vládní instituce, instituce veřejné (média) a armádní (v závislosti na stupni operace, postavení výkonných orgánů a okolnostech), jejichž činnost ovlivňuje vlastní informační potenciál, informační potenciál protivníků, potenciálních protivníků, spojenců a potenciálních spojenců.

Doktrína stanovuje zvláštní postavení informačních operací: plánují se a provádějí se jak v době míru, tak v období krize či za války. Vztah různých forem (či spíše funkčních součástí) informačních operací ukazuje **obr. 2.**

Stanovení kompetence

Doktrinální dokumenty stanovují kompetence v oblasti plánování a provádění informačních operací, ale i v oblasti personálního zabezpečení. Nebudeme zasahovat do podrobností, ale je třeba zdůraznit některé zásady.

- Pora dcem ministra národní obrany pro strategii ve věcech informačních operací jako činitele vojenského potenciálu je **předseda výboru náčelníků štábů**. Ten odpovídá mimo jiné za doktrínu, za plánování organizačního a materiálového zabezpečení informačního boje, za koordinaci činnosti ve všech ozbrojených složkách i v mimorezortních oblastech a též za provádění školicích programů a simulátorových modelů v armádních školicích střediskách, za vojenská cvičení, štábní nácviky a válečné hry.
- Oblastní velitelé (*combatant commanders*) **a velitelé spojených sil** odpovídají za rozpracování problematiky informačního boje pro periodické plánování a operační plánování v době krize i za války, vyčlenění sil a prostředků (včetně prostředků počítačové podpory) potřebných pro plánování a plnění úkolů informačního boje (zvláště C2W), nácvik informačního boje během cvičení, štábní nácviky a válečné hry. Mají na starost rovněž organizaci štábních buněk odpovídajících za plánování a koordinaci informačního boje v otázkách válečného velení.

■ Za organizaci výzkumně-vývojových prací a tendencí vývoje v oblasti zpravodajského zabezpečení informačního boje jsou odpovědni **šéfové zpravodajských služeb a velitelství speciálních operací.** Rovněž nesou na svých bedrech odpovědnost za zavedení stanovené problematiky do programů jim podřízených učebních center i školicích a výcvikových základen a společně s **Agenturou obranných informačních systémů (DISA)** za koordinaci vývoje a distribuci souborů dat pro plánování a provádění informačního boje.

■ Za programování vývoje technologie a služeb v oblasti bezpečnosti informačních systémů (INFOSEC) a v oblasti operační činnosti vojsk (OPSEC) odpovídá **Agentura národní bezpečnosti (NSA).** Kromě toho provádí běžné monitorování, analýzy a hodnocení stupně ohrožení vlastních systémů a informačních souborů.

■ Vojenská zpravodajská agentura (DIA) odpovídá mimo jiné za tvorbu souborů dat a informačních systémů umožňujících zevšeobecnění zpravodajských informací a jejich postoupení uživatelům. Velitelům vyšších stupňů poskytuje odbornou pomoc v oblasti plánování a provádění informačního boje. Kromě toho Vojenská zpravodajská agentura ve spolupráci s DISA a dalšími vládními a nevládními agenturami rozpracovává operační úkoly v oblasti varování z hlediska hrozeb informačního útoku.

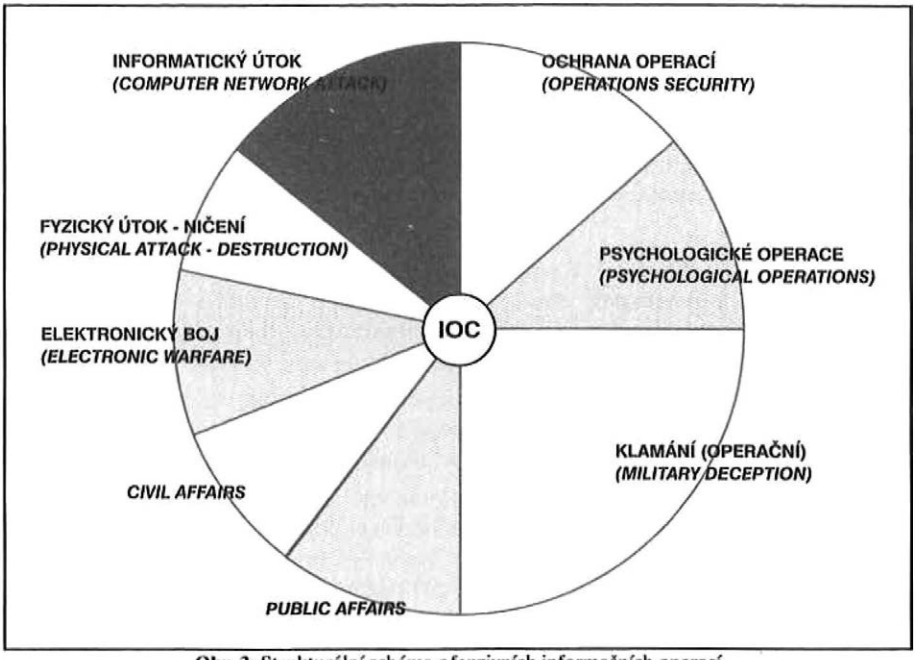
■ Zvláštní úkoly mají přidělena **výzkumná a školicí střediska** (*Joint Command & Control Warfare Center, Joint Warfighting Center*). Tyto úkoly zahrnují zpracování metodik a modelů (včetně simulačních) pro výzkum a výcvik procedur informačního boje.

Ofenzivní a defenzivní opatření a jejich struktura

Doktrína rozlišuje **ofenzivní informační opatření** a **defenzivní informační opatření.** Taktéž zdůrazňuje význam synergického efektu těchto činností pro výsledek jejich synchronizace a koordinace. Zajištění synergismu (spolupůsobení - pozn. překl.) je služební povinností vrcholných orgánů, které odpovídají za bezpečnost státu, a velitelů na všech stupních - operačních a taktických svazků, které jsou začleněny v organizační struktuře. Funkční stavbu ofenzivních a defenzivních operací ukazují **obr. 3** a **4.**

Ofenzivní informační operace

Jednotlivé segmenty reprezentují „realizační kanály" ofenzivní činnosti, které jsou zaneseny do operačního plánu coby mechanismy dosažení doktrinálních cílů informačních operací (ovlivňování rozhodnutí protivníka, zneschopnění nebo zničení jeho systému velení). Velikost segmentů na obrázku není mírou jejich podílu či úlohy v operaci. Ve shodě s operační doktrínou (informační opatření) mohou tyto segmenty být hlavní nebo pomocné. Stejně tak závisí mechanismy činností a jejich účinnost na stupni velení a na charakteru a stupni ohrožení. V domácích publikacích (J. Janczak: *Walka informacyjna na wspólczesnym polu walki* /= Informační boj na současném bojišti/, VII. armádní konference telekomunikace a informatiky, část 1, Zegrze 1998) je možno nalézt méně či více důkladnou charakteristiku fungování těchto segmentů, jinak se tato problematika omezuje pouze na komentáře odpovědných osob s odkazem na zdroje doktrinálních dokumentů.



Obr. 3: Strukturální schéma ofenzivních informačních operací
(Information Operations Cell – IOC)

◆ **Ochrana operací** (*Operations Security* /Joint Doctrine for Operations Security, Joint Pub 3-54/) obsahuje opatření, která mají za cíl zkrytí těch informací před protivníkem, jež vypovídají o stavu a možnostech vlastních vojsk a zámyslech velitele, a která u něj podmiňují přijímání vlastních rozhodnutí. Jde o prodloužení procesu velení u protivníka a znemožnění mu získat věrohodné informace. Základem plánování ochranných opatření je zpravodajská činnost ***kontrarozvědky*** (předpokládané metody a způsoby získávání informací protivníkem) a ***rozvědky*** (zpravodajské možnosti protivníka, postupy a způsoby hodnocení situace, přijetí rozhodnutí atp.). Základ opatření je založen na zablokování informací a pohybu osob.

◆ **Psychologické operace** (*Psychological Operations*) obsahují opatření, která mají za cíl působit na chování určitých subjektů, skupin osob nebo jednotlivců ovlivňováním jejich emocí, motivů činnosti, míry soudnosti a racionality. Použité mechanismy závisí především na stupni operačního kontinua. Například na ***strategickém stupni*** se využívá kanálů diplomatických, obchodních, bankovních, mediálních atd. Na ***operačním stupni*** se lépe kontrolují lokální média a lokální agentury (skupiny). Na ***stupni taktickém*** mohou do hry vstoupit dokonce i běžné propagační prostředky. V informačních operacích mají psychologická opatření vedlejší roli a zpravidla se za důležitější pokládají pomocné klamné operace.

◆ **Klamání, operační klamání, použití lsti apod.** (*Military Deception* /Joint Doctrine for Military Deception, Joint Pub 3-58/) jsou opatření, jejichž cílem je ovlivňovat

rozhodovací proces protivníka poskytováním falešných nebo neurčitých informací pro jeho zpravodajský systém (rozvědku). Operačním cílem klamání je příprava takových zdrojů nepravdivých informací, aby protivník prováděl činnost ve shodě s námi vypracovaným scénářem. Jak potvrzuje doktrína, účinné klamání v operačním měřítku je efektivní vzhledem k nutnosti zasazení vojsk, což je někdy spojeno s velkými lidskými ztrátami. Pokud máme technologickou převahu, můžeme dosáhnout analogického efektu i jemnějšími metodami, založenými na pronikání do informační infrastruktury systému velení.

◆ **Elektronický boj** (*Electronic Warfare* /*Electronic Warfare in Joint Military Operations*, Joint Pub 3-51/) se provádí éterem (záměrně jsme nepoužili termínu „radio-elektronický boj"). Elektronický boj v sobě zahrnuje tři typy opatření: ***elektronický útok***, ***elektronickou ochranu*** a ***podporu elektronického boje***.

● ***Elektronický útok*** si klade za cíl vyloučení nebo omezení možnosti využití elektromagnetického spektra jako informačního média. Účinný elektronický útok může zbavit protivníka znalostí o situaci a prodloužit rozhodovací proces.

● ***Elektronická ochrana*** má za cíl protičinnost vůči účinkům elektronického útoku protivníka a ochranu před protivníkem využívaným elektromagnetickým spektrem jak za účelem zpravodajským, tak za účelem navádění prostředků ničení. Zvláštním úkolem elektronické ochrany je prevence před negativními účinky vlastní elektronické aktivity.

● ***Podpora elektronického boje*** je základním činitelem získávání informace o protivníkovi, a to vyhledáváním, identifikací a sledováním jeho zdrojů elektromagnetického vyzařování. Rovněž zahrnuje monitorování vlastních zdrojů nekontrolované emise.

Shodně s platnou doktrínou o pěti oblastech činností uplatňujících se na bojišti patří elektronický boj do stejné oblasti činností jako zpravodajství *(Intelligence)*.

◆ **Fyzický útok - ničení** (*Physical Attack/Destruction*) představuje tradiční oblast informačních operací a prakticky figuruje pouze v rámci C2W nebo speciálních operací. Je založený na umlčení, zničení, zneschopnění nebo vyloučení důležitých prvků informačního systému protivníka (např. velitelských stanovišť, spojovacích středisek apod.). Takový útok se provádí v rámci působení palebnými prostředky a v rámci speciálních operací (diverzních akcí).

◆ **Informatický útok** (*Computer Network Attack*) spočívá v prolomení informační obrany systémů protivníka, v jejich zneschopnění, zarušení a také v manipulaci s poznatky v těchto systémech obsažených.

◆ **Úřad tiskového mluvčího a vztahů s veřejností** (*Public Affairs* /*Doctrine for Public Affairs in Joint Operations*, Joint Pub 3-61/ a ***Civil Affairs*** /*Doctrine for Joint Civil Affairs*, Joint Pub 3-57/) jsou subjekty odpovědné za prezentaci zpráv související s tematikou obrany v masově-sdělovacích prostředcích a za styky s lokálními civilními institucemi. Určují vlastně integrální prvek štábní struktury. Jejich úloha v informačních operacích je podružná a je podřízená cílům psychologických operací. Stupeň jejich zapojení do informačních operací stanoví velitel v organizačních směrnicích. Za nejúčinnější prostředek působení propagandy se považuje ***internetová síť***, jelikož umožňuje

zpřístupnit informace, jejichž hodnověrnost bývá hodnocena mnohem lépe než u informací pocházejících z veřejných médií, jež se především v období krizového stavu podezřívají z manipulování.

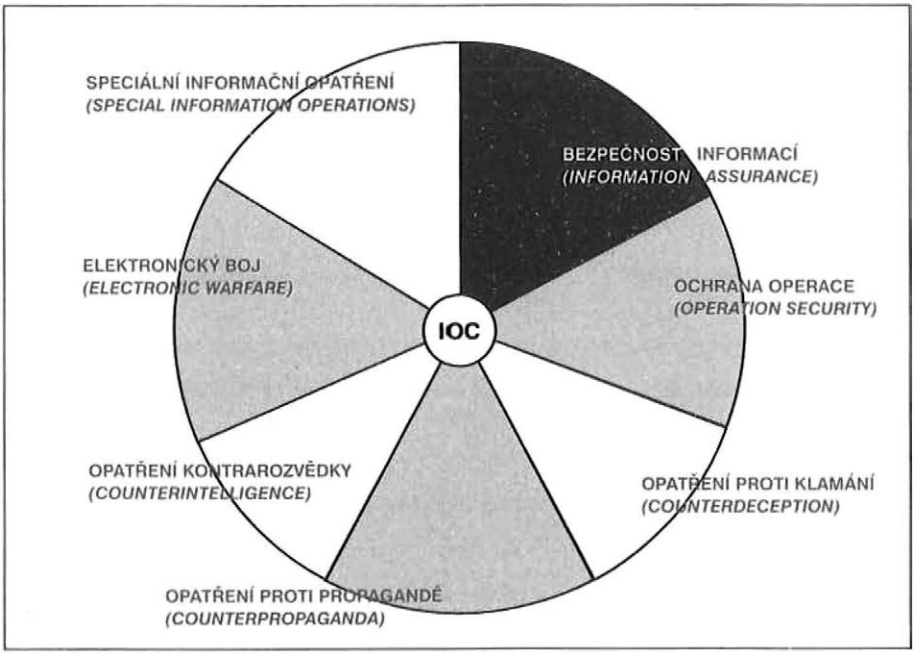
Defenzivní informační operace

Doktrinálním cílem defenzivních informačních operací je ochrana a obrana vlastního informačního potenciálu před činností protivníka. Defenzivní opatření se vyznačují dlouhodobým charakterem. Zahrnují čtyři fáze:

- **ochranu informačního prostředí** *(information environment protection)*,
- **vykrytí útoku** *(attack detection)*,
- **obnovení potenciálu** *(capability restoration)*,
- **protiútok** *(attack response)*.

Defenzivní úkoly se plní pomocí příslušných „realizačních kanálů". Jejich princip je znázorněn na **obr. 4**.

Úlohu *ochrany operací* a *elektronického boje* během defenzivních opatření ovlivňují výše uvedené doktrinální dokumenty. Úkoly plněné v rámci *protičinnosti v oblasti propagandy a klamání* jsou úzce svázané s činnostmi týkající se klamání, psychologie a propagandy. Doktrinální zásady *opatření kontrarozvědky* vytyčuje zvláštní doktrína (*Joint Doctrine and Tactics, Techniques and Procedures for Counterintelligence Support to Operations*, Joint Pub 2-01.2). ***Speciální informační opatření*** jsou zde objasněny dosti nejasně. Ty musí prakticky zahrnovat všechny operace vedené proti ofenzivnímu informačnímu působení protivníka, které vyžadují zvláštní informační ochranu.



Obr. 4: Strukturální schéma defenzivních informačních operací
(Information Operations Cell — IOC)

Podobně jako informatické útoky (*Computer Network Attack*) ve struktuře ofenzivních informačních operací, také **bezpečnost informací** v případě selhání defenzivních operací je zvláštní oblastí působení subjektů vedení informačního boje (IOC). Bezpečnost informací má mnohačetnou strukturu složek, kterou ukazuje **tabulka**.

Posuzovaná doktrína informačních operací *(Joint Doctrine for Information Operations*, Joint Pub 3-13*)* klade zvláštní důraz na systematické provádění analýzy výběru informačních systémů pro ofenzivní působení na různé subjekty (nejen na politického či vojenského protivníka), hodnocení jejich bezpečnosti a též určení a plánování potřeb. V souvislosti s tím mají velitelé a náčelníci uloženo využívat štábních cvičení a nácviků, používat simulátorové modely a ostatní počítačovou techniku zkvalitněnou informačními technologiemi, především dostupnou technologií INFOSEC. Technologie INFOSEC se dělí na dvě části: COMPUSEC a COMSEC. První z nich obsahuje metody, způsoby a postupy zajištění bezpečnosti (viz tabulka) počítačové techniky a zavedených programů. Druhá se týká telekomunikační infrastruktury.

Tabulka

Složky bezpečnosti informací

Složka	Charakteristika
Legalita *(Authentication)*	Možnost potvrzení pravosti zdroje poznatku, autorství dokumentu atp.
Nepopírání *(Nonrepudiation)*	Možnost zdůvodnění účasti (např. autorství, vysílání, příjmu)
Dostupnost *(Availability)*	Zajištění dosažitelnosti poznatku (dokumentu) všem oprávněným odběratelům
Celistvost *(Integrity)*	Zabezpečení ochrany před neautorizovanými zásahy
Důvěrnost *(Confidentiality)*	Zabezpečení nedostupnosti poznatku (dokumentu) pro neoprávněné odběratele

Doktrína informačních operací stanoví rovněž závazky institucí a zainteresovaných skupin v oblasti ***odhalování a identifikace informačního ohrožení*** *(IO Attack Detection)* a v oblasti ***obnovování informačního potenciálu*** *(Capability Restoration)*. Rozhodující statutární roli z hlediska analýz, hodnocení a programování vývoje v této oblasti nesou *Information Warfare Centers* druhů ozbrojených sil a spojených operací (celkem čtyři instituce). Výrobci počítačové techniky a autoři programů musí být připraveni splnit příslušná nařízení ohledně bezpečnosti informací. Rovněž dodavatelé služeb teleinformatiky a správcové administrativních sítí i celkové administrativy musí dodržovat zvláštní postupy, a to jak ve styku s lidmi, tak i v technické infrastruktuře informačních systémů. Dokument činí velitele odpovědnými za zajištění bezpečnosti informací, konkrétně za splnění nařízení týkající se informační infrastruktury systémů velení a plánování potřeb, za provádění systematické verifikace během cvičení, nácviků a válečných her i za vyškolení velitelsko-štábních skupin, včetně provádějících subjektů (jednotek).

* * *

Oblast počítačové problematiky informačního boje je komplikovaná a dostatečně neujasněná jak ve vědomí velitelsko-štábních skupin, tak i navrhovatelů systémů velení. Orientaci v této oblasti mají usnadnit výše jmenované standardy. Množství a tematický okruh standardizačních dokumentů pro oblast bezpečnosti informací systémů stále roste a zvládnutí veškeré v nich obsažené problematiky si vynucuje radikální a rychlá institucionální řešení. Například pro podklady na VII. vědeckou konferenci věnovanou automatizaci velení (P. Zaskórski, A. Grochalski: *Problemy bezpieczeństwa w zautomatyzowanych systemach dowodzenia*, Jelenia Góra, 1999) bylo využito 52 dokumentů NATO, z nichž 38 je prakticky nedostupných. Obecná dostupnost některých dokumentů je však podmínkou formování „kultury bezpečnosti".

Článek, jehož autorem je ***doc. Dr. Andrzej Stokalski*** *z Ústavu automatizace systémů velení WAT, byl otištěn v č.2/2000 časopisu* ***Myśl wojskowa*** *a pro Vojenské rozhledy jej přeložil Ing. Igor Jalůvka.*