Informační válka: způsoby a průběh jejího vedení

V mnoha zemích již po několik let probíhá 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. To znamená, že informace je považována za zbraň. Toho jsou si vědomy ozbrojené síly členských států NATO, které činí praktická technická, organizační i výcviková opatření v rámci příprav k informační válce. Svědčí o tom série článků uveřejněných v čísle 4/98 časopisu REPORT VERLAG. Tyto články byly podkladem i pro následující práci.

* * *

Ve dvacátém století byl pojem „válka" spojován s atributy označujícími použitou zbraň: chemická válka, biologické válka, letecká válka, jaderná válka. Tím nemělo být řečeno, že se o rozhodnutí usilovalo pouze použitím chemické, biologické nebo jaderné zbraně, nebo samotným letectvem. Jisté však je, že žádný stát, který měl např. leteckou převahu, válku neprohrál.

Vedení války proti nepřátelské informační infrastruktuře je označován jako informační válka. V souvislosti s informační válkou se ještě běžně používají pojmy týkající se války všeobecně: útok, obrana, průzkum, operace, převaha ap. Někteří autoři zařazují pod pojem informační válka také psychologickou válku, elektronický boj apod. Zde jsou uvedeny stručně jen pro úplnost.

Informační válka je definována jako souhrn veškerých opatření a) pro ochranu vlastních informací a procesů na nich 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 formou vedení války pomocí informací a informační techniky proti informacím a informační technice. Zabývá se v nejširším smyslu získáváním, zpracováním a využíváním informací, jakož i ovlivňováním lidí a strojů a jejich rozhodování.

Zranitelnost státu

Rozšiřující se používání informační techniky vede v technicky vyspělých zemích k **situaci ohrožení.** Na jedné straně se vytvořila vysoká závislost na informacích a na používání informačních systémů, na druhé straně existují nové útočné prostředky, které mohou používat nových způsobů útoku, útočníci mohou zůstat anonymní a zeměpisné hranice ztrácejí svůj význam. Útoky proti státu mohou být vedeny namísto proti ozbrojeným silám také proti civilním cílům jako banky, obchod, doprava nebo řízení

letového provozu. Útoky mohou být, na rozdíl od dřívějška, vedeny v mezinárodních sítích, a proto z velmi vzdálených míst.

K dosažení cílů se v rámci informační války používá tzv. **informační operace**. Cílem informační operace je dosáhnout a udržet **informační převahu**, která je definována jako schopnost ve vlastním informačním systému vytvářet, zpracovávat a udržovat nepřerušený tok informací, zatímco je nepřátelský tok informací odposloucháván, manipulován a přerušován.

Informační převaze je pro rozhodnutí konfliktu připisován minimálně stejný význam jako třeba letecké převaze. Je to pochopitelné, protože za informační války budou cílem operací především systémy velení a spojení. Budou-li narušeny systémy velení a spojení, budou ochromeny všechny jimi řízené dílčí systémy.

V rámci informační války nejde o nic menšího než o udržení **volnosti jednání** systémů velení a spojení.

Vojenský význam činitele informace

Využívání informací ve vojenství vždy hrálo důležitou úlohu. Existuje mnoho historických příkladů toho, že schopnost vědět všechno o nepříteli a zároveň ho ponechat v nejistotě o vlastních záměrech může být ve válce rozhodující. Avšak přes historické důkazy mělo a dodnes má získávání, zpracování, rozdělování a bezpečnost informací jen podpůrnou úlohu pro vlastní zasazení zbraní. Důležitými činiteli, určujícími vojenský potenciál států, jsou stejně jako dříve druh, počet a kvalita personálu a zbraňových systémů.

Naproti tomu se úvahy o informační válce naprosto liší: Za rozhodující veličinu v budoucích konfliktech je považována schopnost pokud možno optimálně zasadit jako určujícího činitele informace. Zásadním cílem je ovlivňovat rozhodujícím způsobem proces nepřátelského rozhodování, tvořený prvky zjišťování a hodnocení situace, přijetí rozhodnutí a jednání. K tomu je především nutná elementární znalost nepřátelských informačních toků a procesů zpracování informace.

Obraz informační války není vázán na určité technologie, nýbrž při všech úvahách je nutno brát zřetel také k **netechnologickým aspektům**, mezi jiným strukturálního a organizačního druhu. Tyto aspekty **mohou mít stejnou, nebo dokonce vyšší řádovou hodnotu než použití nových technologií**.

V rámci doktríny informační války je nutno počítat s velkými změnami. Vedoucí myšlenkou by přitom mohla být decentralizace velení, aby bylo dosaženo pružnějšího jednání a také nižší zranitelnosti.

Potenciální protivníci

Know-how nezbytné pro informační útoky lze získat snadno a levně. Namísto drahých zbraňových systémů lze používat levného přístrojového (hardware) a informačního (software) vybavení. Požadavky na technické znalosti útočníků nejsou vysoké. K provádění útoků je zapotřebí relativně málo personálu. Útoky je možné provést jednoduchými prostředky, a přitom mohou mít velmi silné účinky a způsobit vysoké škody. Proto se mění nejen obraz příštích konfliktů, ale i potenciálního protivníka.

Dříve vycházela ohrožení zpravidla od jiných, většinou sousedních států a konflikty se řešily mezi nimi. Nyní se kromě toho nabízejí relativně jednoduché a levné možnosti útoků

na jiné státy i relativně vzdáleným státům (včetně států třetího světa), teroristům, zločineckým organizacím, revolučním organizacím, náboženským extremistům, jednotlivcům.

Formy informační války

1. Na prvním místě je nutno uvést přímé vedení boje s **použitím zbraní proti místům velení**. Účelem je zničení nebo narušení prostředků velení a neutralizace velení. Účinnost těchto opatření je značně závislá na míře centralizace umlčované struktury velení. Pro účinné použití této metody je nezbytná velmi dobrá znalost nepřátelského systému velení. Účinná ochrana vyžaduje decentralizované struktury, jakož i klasická opatření jako zodolnění a maskování.

2. **Získávání a ochrana informací**. K *ofenzivním opatřením* patří působení všech běžných průzkumných prostředků, včetně zpracování dat. Účelem je mít trvale obsáhlý obraz o stavu nepřítele a bojiště. K *defenzivním opatřením* patří všechny možnosti, jak uniknout zjištění a pozorování nepřítelem, např. maskováním, klamáním nebo používáním nesnadno zjistitelných stanovišť.

3. **Elektronický boj** (electronic warfare) je důležitou formou budoucí informační války. Zahrnuje všechna ofenzivní i defenzivní opatření pro využívání elektromagnetického spektra. Patří sem maskování, klamání a zvláště rušení v oblastech průzkumu a komunikace. Příkladem je buď umlčování nepřátelských radarů elektronickým rušením nebo ničení protiradarovými raketami. V oblasti komunikace bude ochranou proti rušení nebo manipulaci zpráv digitalizace, jakož i používání moderních šifrovacích metod. Zdroje elektromagnetických impulzů ve formě pum mohou levně a jednoduše vyřadit z používání informační a komunikační systémy. Výroba takových pum je relativně levná.

4. **Kybernetická válka.** Výše uvedená opatření odpovídají běžnému obrazu války spojeného s uplatněním síly. S rozšiřujícím se používáním počítačů ve všech vojenských oblastech zvětšují také možnosti, že se značné části konfliktů budou odehrávat ve virtuálním světě počítačových systémů nebo sítí. Tato forma informační války je označována jako „kybernetická válka".

Především je zde nutno uvést všechna opatření, jejichž cílem je proniknout do nepřátelských informačních systémů, aby byly manipulovány nebo zničeny informace v nich obsažené („válka vedená hackery" neboli „počítačovými kasaři"). Přímou cestou počítačových kasařů (hackerů) je pronikání do datových sítí, jakož i manipulace informačního vybavení (software) a bází dat. Nepřímé, a proto účinnější jsou viry zavedené do počítačů, aktivované za určitých podmínek. Takových programových prvků existuje mnoho variant: např. „červi", „logické bomby", „trojské koně". Útoky nebudou zčásti ihned zpozorovány, nýbrž mohou probíhat po dlouhá období, dříve než se projeví prvé škody.

Není jasné, jak se má v jednotlivém případě postupovat při výskytu prvních škod, aby se rozhodlo, zda probíhá vážný informační útok a jak je nutno mu čelit, nebo zda se jedná o nahodilou událost.

5. Cílem **psychologické války** je ovlivňovat nepřátelskou vůli nepřímo, bez použití zbraní. Rozvoj komunikačních prostředků, zvláště družicových, umožňuje státům působit

téměř přímo na obyvatelstvo a jeho speciální cílové skupiny v jiných zemích s cílem jejich demoralizace. Falšování informací a cílené šíření falešných nebo neúplných informací, které mají vliv na vojenské rozhodovací procesy, mohou vést k nesprávným závěrům.

Manipulace rozhodovacích procesů

Cílovými objekty mohou být: informace, vojenské informační a komunikační systémy, informační technika zbraňových systémů, samotné vojenské rozhodovací procesy, průmyslové podniky, banky, pojišťovny, obchod a další.

Vlastní manipulace rozhodovacích procesů se uskutečňuje ve smyčce tvořené těmito členy: pozorování (tj. získávání dat), orientace (zpracování informace), rozhodování (využití informace) a jednání.

„Pozorování" může být ovlivňováno falešnými informacemi, cílenou volbou informací, přetížení daty, skrýváním informací, klíčováním dat aj.

Všechny prvky smyčky mohou být manipulovány rušením napájení energií, změnami zpracovávaných dat, manipulací informačních systémů aj. Je možné například manipulovat obrazy pomocí informační techniky, takže rozhodovací činitelé nebudou vědět, co je skutečnost a co fikce.

Informační útoky mají za účel ovlivňovat jednání protivníka, tj. vyvolat, manipulovat je, nebo mu zabránit.

Na **obr. 1** jsou znázorněny různé možnosti útoku na systém pro zpracování informací, který je pod naší kontrolou. Některé jeho objekty, které jsou důležitým základem pro vlastní procesy, jsou kontrolovatelné jen zčásti nebo vůbec ne.

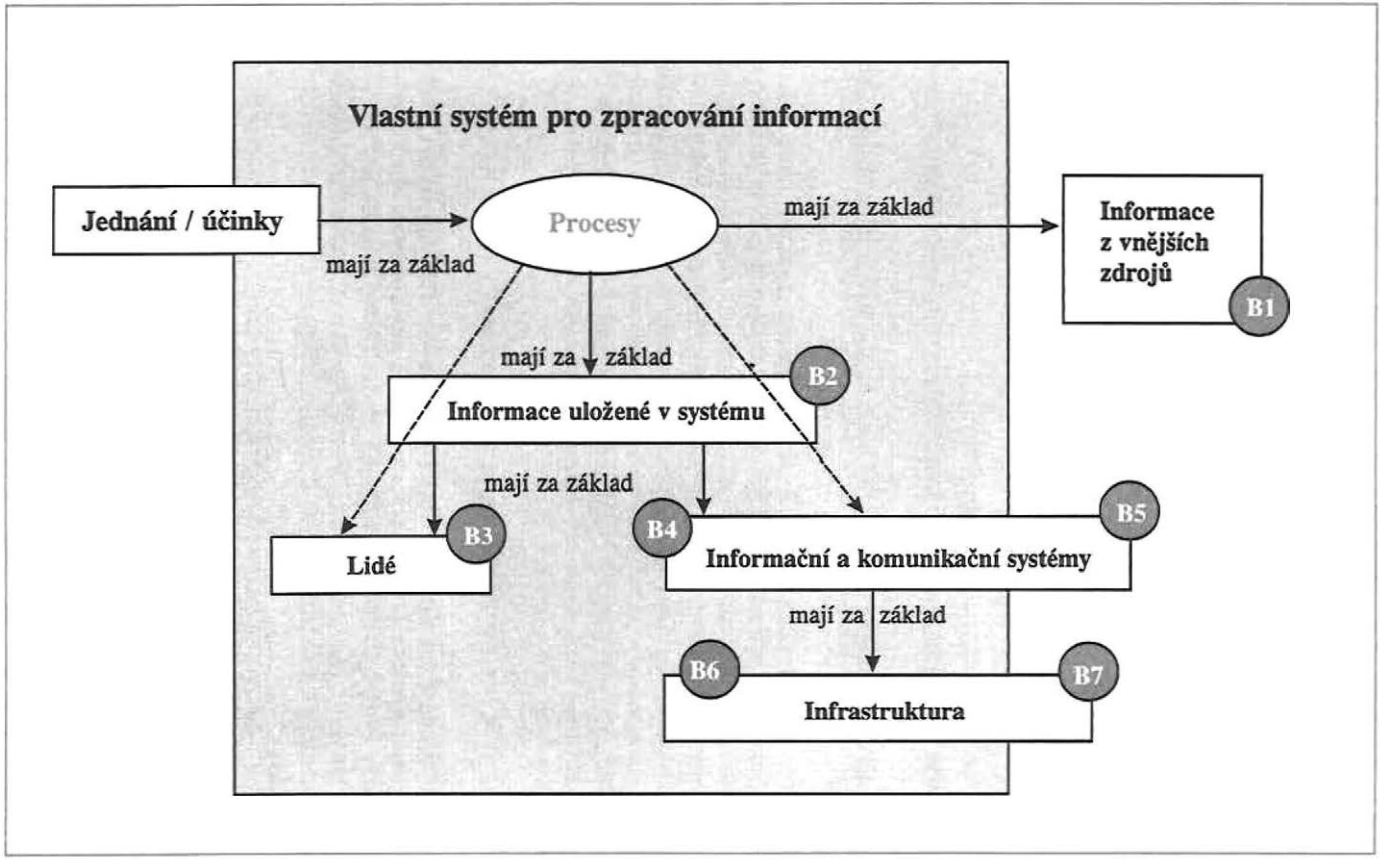
V tomto systému pro zpracování informací existuje mnoho bodů, na něž je možno vést útok podle volby útočníka.

Bod útoku B1. Útočník může manipulovat rozhodovací proces zvenčí přiváděnými informacemi, zavádět přídavné informace nebo přerušit tok informací zvenčí. Ohrožením může být přehlcení systému informacemi, přivádění platných informací v nežádoucím okamžiku, klamání, přivádění neplatných informací a ovlivňování lidí sdělovacími prostředky. Takovými akcemi mohou být diskreditovány orgány národní bezpečnosti, nebo může být ztíženo plnění jejich úkolů.

Bod útoku B2. Útočník se může pokusit získat, změnit, vymazat nebo jinak manipulovat informace obsažené v informačním systému nepřítele. Typickým ohrožením může být vyhodnocení zbývajících informací, zavedení nesprávného zdroje informací a změna vztahů informací.

Bod útoku B3. Útočníci působící uvnitř informačního systému se mohou snažit ovlivňovat osoby, například povolením neoprávněného zásahu, nebo neoprávněným předáním informací a nositelů informací.

Bod útoku B4. Útočník se může snažit zbavit nepřátelské procesy jejich funkční základny, rušit je nebo ovlivňovat tím, že přímo napadne technické složky nepřátelských informačních a komunikačních systémů. Typickými ohroženími jsou neoprávněné vniknutí do informačních systémů, zneužití privilegií oprávněných uživatelů, nebo zavedení červů, virů nebo trojských koní. Fyzického zničení lze dosáhnout pomocí pumy vytvářející elektromagnetický impuls. Elektronickými metodami je možno přerušit struktury velení na bojišti nebo se zázemím.


Vlastní systém pro zpracování informací
Jednání / účinky
Procesy
mají za základ
mají za základ
Informace z vnějších zdrojů
B1
mají za základ
B2
Informace uložené v systému
mají za základ
B3
Lidé
B4
B5
Informační a komunikační systémy
mají za základ
B6
B7
Infrastruktura

Obr. 1

Bod útoku B5. Útočníci se mohou pokusit manipulovat nepřátelské informační systémy již ve fázi jejich vývoje, např. zavedením dodatečných informací nebo funkcí.

Bod útoku B6. Útočníci se mohou snažit rušit vnitřní systémovou infrastrukturu nepřátelských informačních systémů logickými nebo fyzickými útoky.

Bod útoku B7. Útočník se může pokusit rušit vnější infrastrukturu, která je základem nepřátelských informačních systémů. Cílovými objekty jsou přitom spolupracující vojenské a civilní infrastruktury jako civilní komunikační systémy používané také ozbrojenými silami.

Informační operace

Informační operace vedené za informační války jsou:

a) **ofenzivní** (informační operace zahrnují všechna opatření pro rušení, manipulování a vyřazení nepřátelské informační infrastruktury),

b) **defenzivní** (informační operace se snaží zabránit nebo zmařit ofenzivní informační operace),

c) **explorativní** (informační operace tvoří průzkumnou složku ofenzivních a defenzivních informačních operací).

Explorativní operace jsou účinné již před zahájením možného konfliktu. Slouží soustavnému pozorování sítí a informací v nich přenášených, a to s cílem včasného získání informací, které by mohly naznačovat nadcházející agresi. Úkolem oblasti explorativní informační operace je vedle přímého rozpoznání útoku také včasné varování.

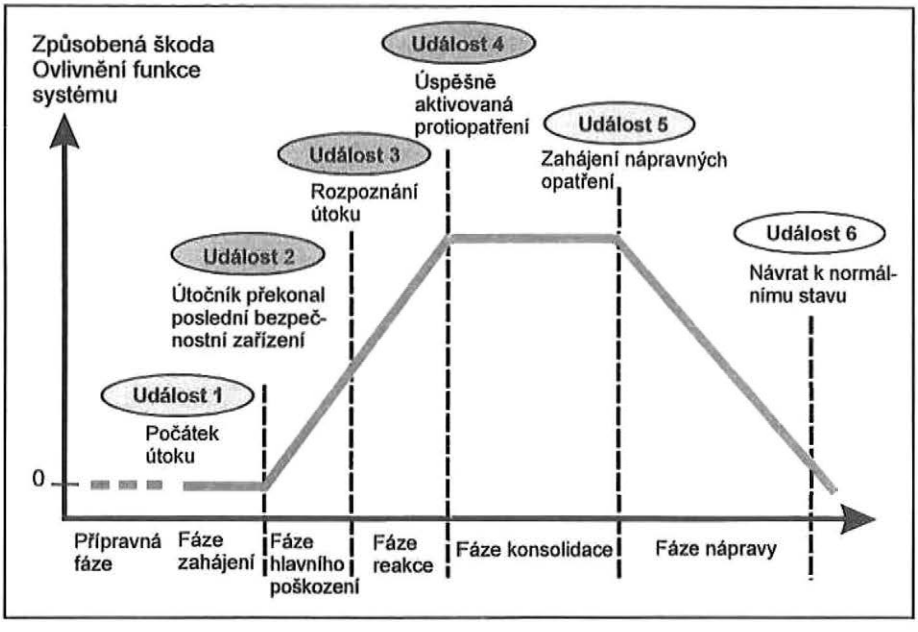
Informační válka klade velký důraz na **metodický postup** útočníků. Také koordinovaný postup informační války s jinými způsoby útoku (např. noční přepad) pro manipulaci systému a pozdější využití vzniklého slabého místa dokazují rozšíření dimenze informační války. Přitom jsou možné rozmanité způsoby kombinace ohrožení zevnitř (špionáž, sabotáž) a klasických informačních operací v sítích.

Průběh informační války

Způsoby útoku a obrany v rámci informační války mají mnohé analogie s konvenční válkou. Význam včasného průzkumu a rozpoznání nepřátelských záměrů je v obou případech velmi vysoký. Zcela odlišná je však *časová dynamika* útoku, jehož hlavní fáze mohou proběhnout ve zlomcích sekundy. Potenciální škoda, kterou lze způsobit v této krátké době, může být nezměrná. Na **obr. 2** jsou vysvětleny typické průběhy útoku v rámci informační války.

Přípravná fáze předchází útoku a může trvat několik minut až několik měsíců nebo roků. Během této fáze se útočník krátce trvajícími akcemi snaží získat pokud možno nejvíce informací o systému, který má být napaden. Přitom může používat různých zdrojů od špionáže až po hackery. Akce jsou prováděny skrytě, aby nebyly prozrazeny skutečné záměry. Útočník na základě získaných informací zpracuje plán a taktiku útoku se zřetelem k očekávaným překážkám.

Fáze zahájení útoku na informační systém. Tato fáze trvá až do okamžiku, v němž útočník překonal poslední bezpečnostní překážku informačního systému. Je tím kratší, čím



Obr.2

více toho útočník ví o systému. Neočekávanými překážkami se může fáze zahájení značně prodloužit.

Fáze hlavního poškození. Poté, co útočník překonal poslední zabezpečovací zařízení, je schopen způsobit v systému největší možnou škodu. Čím déle může útok nerušeně probíhat, tím větší je očekávaná škoda. Fáze hlavního poškození končí okamžikem, v němž cílový systém zjistí útok.

Fáze reakce. Po zjištění probíhajícího útoku je možno provést jeho analýzu, zvolit a provést vhodná protiopatření. Tuto fázi musí cílový systém pokud možno zkrátit, protože během ní může ničivé působení útočníka pokračovat. Závěr fáze reakce je definován úspěšně aktivovaným protiopatřením, jež útočníkovi zabrání způsobit další škody.

Fáze konsolidace. Po úspěšném „odražení" útočníka je zahájena fáze konsolidace. Během ní se zjistí a analyzuje zjištěná škoda a zvolí se vhodná nápravná opatření.

Fáze nápravy. Uskuteční se nápravná opatření zvolená ve fázi konsolidace a tím je dosaženo návratu do normálního stavu.

Vysvětlené fáze útoku se v konkrétním případě mohou vzájemně překrývat a mohou se opakovat. Útočník může např. provádět proti-protiakce (opatření proti protiopatřením), přitom může změnit útočnou taktiku, místa útoku, metody útoku. Fáze zahájení, fáze hlavního poškození a fáze reakce mohou probíhat několikrát po sobě se vždy jinými výsledky.

Při posuzování po sobě následujících fází je jasné, na čem při úspěšné obraně záleží: **Z hlediska obránce je nutno fázi zahájení pokud možno nejvíce prodlužovat, zatímco průběh následujících fází pokud možno nejvíce zkracovat.** Cílem úspěšné defenzivní informační operace musí být posunout „událost 4" (úspěšně aktivované protiopatření) před „událost 2" (útočník překonal poslední bezpečnostní zařízení), a tím zcela zabránit poškození chráněné informační infrastruktury.

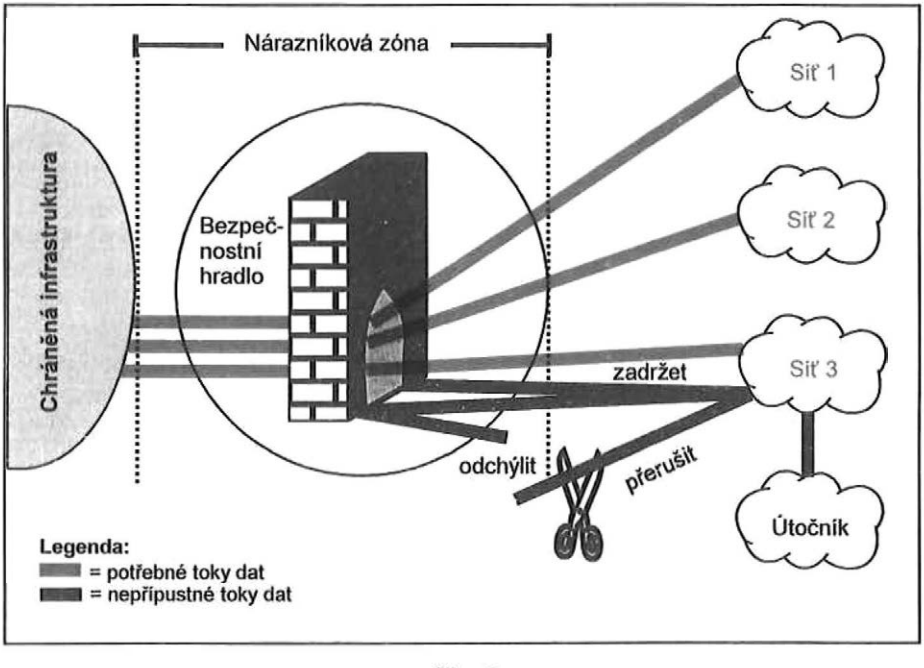
Ochranná opatření

Popsané průběhy a fáze útoku dokazují, že největší význam má zdržování útoku, a tím prodlužování fáze zahájení. Toho lze dosáhnout tak, že útočník bude jemu neznámými překážkami a bezpečnostními opatřeními v nárazníkové zóně (oddělené od chráněné informační infrastruktury) zdržován tak dlouho, aby mohly být uskutečněny rozpoznání a analýza útoku a aktivována úspěšná protiopatření.

Spolkové ozbrojené síly (Bundeswehr) používají koncepci tzv. bezpečnostního hradla (Security Gate). Tato koncepce (**obr. 3**) realizuje princip „selektivní otevřenosti", která musí být udržena i během útoku. V konkrétním případě ochrany vojenského systému velení bude jeho komunikační schopnost nejdůležitější, když nepřítel v rámci svého koordinovaného postupu zahájí informační útok. Úkolem bezpečnostního hradla je zachovat toky dat nezbytné pro velení, a zároveň odrazit útočné informační operace nepřítele.

Bezpečnostní hradlo ke splnění své funkce používá tyto složky:

* „Požární zdi" realizují princip selektivní otevřenosti používáním rozsáhlých filtračních pravidel a selektivní oprávněnosti přístupu.



Obr. 3

* Prodloužení kritické fáze zahájení útoku lze dosáhnout neočekávanými překážkami, jako je kontrola protokolu.

* Systémy pro zjištění vniknutí zjistí útok, analyzují použitou metodu a napomáhají při zjištění útočníka.

* Hotovostní zabezpečovací systémy umožňují udržet funkceschopnost přepnutím na redundanční systémy při vyřazení důležitých složek.

* „Aktivní reakce" zahrnuje všechny druhy aktivní obrany používané nejen k tomu, aby byl přerušen probíhající útok, ale také k tomu, aby bylo útočníkovi znemožněno pokračovat v dalších útočných plánech.

Závěr

Úvahy o informační válce se nevztahují na konflikt s nepřítelem používajícím nevyspělou technologii. Schopnost vedení „obyčejného" boje bude proto i pro moderní armády v budoucnosti důležitá. Z tohoto důvodu **obraz informační války neodstraňuje dosavadní obraz války a krize**, nýbrž je jeho nezbytným doplňkem.

Nejdůležitější důsledky existují ve vztahu mezi civilní a vojenskou oblastí. Ozbrojené síly ale nemohou ochránit hospodářství před informačními útoky - není to ani jejich úkol. Požaduje se - především z cenových důvodů - **účelná kooperace a koordinace vojenských a civilních aktivit** pro ochranu před útoky informační války.

Některé formy informační války mají ryze 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 každém případě bude dosud platný výklad války jako ozbrojeného střetnutí mezi státy vyžadovat novou definici, resp. rozšíření.

Se zřetelem k aspektům informační války je nezbytné zaujmout i nový přístup ke státní bezpečnosti. Nyní existující resp. budoucí technologie a na nich založené technické inovace totiž mění povahu budoucích válečných konfliktů natolik, že se mohou vyvinout zcela nové vojenské struktury, strategie a doktríny.

Ing. Josef Nastoupil