

Nová tvář války: strategická informační válka

Článek byl pod názvem „Strategic Information Warfare: A New Face of War“ zveřejněn v americkém časopise *Parameters*, podzim 1996. Jeho autory jsou výzkumní pracovníci firmy RAND Corporation R. C. Molander, A. S. Riddle a P. A. Wilson, který pracuje pro Institut obranných analýz (CIA). Tento příspěvek, který je redakčně zkrácen a upraven, shrnuje výsledky jejich společného pětiměsíčního výzkumu.

Přes rozdíly v dimenzích a dosažené úrovni, existují a budou existovat v České republice podobné problémy.

* * *

Informační válka (*information warfare*) představuje novou, rychle se rozvíjející, avšak dosud jen nepřesně definovanou oblast rostoucího zájmu rezortu obrany a politických činitelů. Pramenem jak zájmu, tak nejasností v této oblasti je tak zvaná informační revoluce, podmíněná rychlým vývojem v oblasti počítačových modelů trojrozměrného prostředí (kybernetického prostoru, *cyberspace*) minicomputerů a s nimi souvisejících dalších informačních technologií. Americká armáda stejně jako celá americká společnost se snaží co nejrychleji využít výhod a možností, které tento vývoj přináší. Tuto rychle se rozvíjející globální informační strukturu se pro vojenské účely pochopitelně nesnaží využívat jen Amerika a její spojenci, ale také současní respektive budoucí protivníci.

Konečný výsledek, respektive důsledky těchto probíhajících změn pro mezinárodní či jiné formy konfliktu jsou velmi nejisté. Podaří se USA a jeho spojencům překonat potenciálně zranitelná místa počítačového modelování, získají a udrží si taktické i strategické výhody, které tato oblast nabízí? Nebo snad nastupující změny vyvolané informační revolucí budou tak rychlé a hluboké, že ohrozí jak tradiční způsob vedení ozbrojených operací, tedy od základu změni charakter budoucí války?

Proto americký ministr obrany již v lednu 1995 vytvořil „pracovní skupinu pro informační válku“, jíž bylo uloženo formulovat „národní cíle informační války a jejich dosažení“. Skupina měla zpracovat analytický rámec pro zjištění základních problémů informační války, vyšetření jejich důsledků a objasnění východisek pro zpracování příslušné politiky, umožňující dosáhnout konsenzu o její celkové strategii.

Co je to „informační válka“?

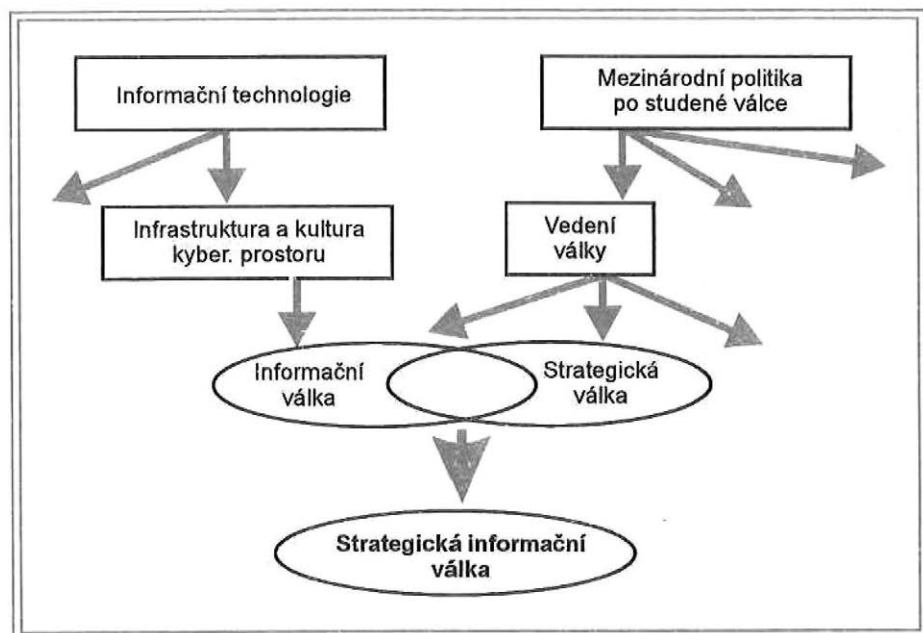
Ještě před pouhými deseti lety byly za informační válku považovány pouze boj proti velitelským stanovištím protivníka na bojišti a válčisti (*command and control warfare*, C²W), rušení a jiné metody radioelektronického boje (*electronic warfare*, EW).

Nyní vztahujeme pojem informační války na stále širší soubor koncepcí vedení války informačního věku. Tyto koncepce přímo souvisejí s představou, že současný rychlý vývoj v oblasti počítačového modelování (globální informační infrastruktury) může přinést další možnosti boje, ale také odkrýt nová zranitelná místa. Tato revoluce by mohla ohrozit

současné prostředky obrany i mimo tradiční bojiště a válčiště způsobem, který ovlivní jak národní vojenskou strategii, tak i širší národní bezpečnostní strategii.

Informační válka je ovšem stále v raném stadiu svého vývoje. Tento pojem nelze zatím přesně vymezit. Nicméně existuje jedna složka informační války, která je při běžném používání tohoto termínu všemi stejně chápána a užívána. Jako „strategickou informační válku“ se označuje konflikt, při kterém:

- je k ovlivnění strategických vojenských operací používáno počítačové modelování (kybernetický prostor, *cyberspace*),
- jsou poškozovány národní informační infrastruktury potenciálních účastníků konfliktu.



Obr. 1: Strategická informační válka

Infrastruktura a kultura trojrozměrného počítačového modelování (kybernetického prostoru) znázorněná na obr. 1, vztahující se k vedení války (navzdory podílu ministerstva obrany při vzniku počítačové sítě Internet) se v minulých letech rozvíjela téměř výlučně mimo vojenské prostředí.

Paralelně s tímto rozvojem probíhá vývoj na mezinárodně politické scéně. V tomto kontextu se také vyvíjí i Clausewitzova slavná definice „války jako nástroje politiky“. Vynořují nové strategické zájmy, které přinášejí nové strategické problémy. Vytvářejí se nové strategické cíle, proti nimž lze používat všech nástrojů, včetně hrozby použití nových (i starých) druhů strategické síly. Vznikají nová strategická ohrožení a nová strategická zranitelná místa. Je nesporné, že vývoj strategického vedení války bude zahrnovat dimenzi

ohrožení a zranitelných míst prostřednictvím počítačového modelování (kybernetického prostoru), takže označení „strategická informační válka“ je plně oprávněno.

Strategická informační válka

Současné státy mají rozsáhlé prostředky na využití informatiky, včetně složitých řídicích systémů i infrastruktur zahrnujících řízení elektrické energie, toku peněz, letecké dopravy, dopravy ropy a plynu. Proto jsou stále závislejší na informačních infrastrukturách. Pokud se potenciální protivníci pokusí tyto systémy poškodit s využitím metod informační války, informační válka získá strategický rozměr.

Základním aspektem strategické informační války je, že neexistuje žádná „frontová linie“. Strategické cíle ve Spojených státech mohou být útokem stejně zranitelné jako prostředky velení, řízení, spojení a průzkumu (*command, control, communications and intelligence, C³I*) na válčišti. Pozornost účastníků konfliktu se proto rozšiřuje mimo jediné tradiční regionální operační válčiště na čtyři samostatná operační válčiště:

- bojiště jako takové,
- vnitřní pásma zúčastněných států,
- mezinárodní pásmo sloužící ke spojení a přesunům,
- domácí území státu vedoucího operace v zahraničí.

Při reagování na útoky informační války tohoto druhu se vojenská strategie již nemůže soustředit jen na vedení a zabezpečení operací výhradně v určitém regionu. Je nezbytné zevrubné posouzení důsledků informační války pro infrastruktury vlastního státu i spojenců, které jsou závislé na nerušeném zpracování informací.

Základní rysy strategické informační války

Autoři uvádějí sedm charakteristických rysů strategické informační války:

* *Nízké vstupní náklady.* Na rozdíl od tradičních zbrojních technologií vývoj metod založených na informatice nevyžaduje rozsáhlé finanční prostředky. Jedinými předpoklady jsou odborná znalost informačních systémů a přístup k důležitým sítím.

* *Neostré tradiční hranice.* Tradiční rozlišování např. veřejných zájmů oproti soukromým, bojového jednání proti zločinnému, či historicky definovaných zeměpisných hranic, je komplikováno rozšiřující se interakcí v rámci informační infrastruktury.

* *Zvýšená možnost ovládnutí veřejného mínění.* Nové informační metody mohou značně zvětšit schopnost klamání a vůbec činností spojených s manipulací obrazu nepřítele, což zkomplikuje úsilí jakékoli vlády získávání politické podpory iniciativ týkajících se bezpečnosti.

* *Nové úkoly strategického zpravodajství.* Nedostatečná obrana proti prostředkům informační války obnažuje zranitelná místa a strategické cíle. Je snížena účinnost klasických metod získávání a analýzy zpravodajských dat. Proto bude nutno vypracovat nové metody analýzy zaměřené na strategickou informační válku.

* *Závažné problémy taktické výstrahy a hodnocení útoku.* S současné době totiž neexistuje žádný adekvátní taktický výstražný systém umožňující rozlišovat mezi

strategickými útoky informační války a jinými druhy aktivit v kybernetickém prostoru, včetně špionáže anebo nezaviněných poruch.

* *Obtíže při vytváření a udržování koalic.* Spoléhání se na aliance pravděpodobně rozšíří zranitelnost bezpečnostního postavení všech členů aliance v rámci strategické informační války, což protivníkům poskytne neúměrně velkou strategickou výhodu.

* *Zranitelnost zázemí státu vedoucího expediční válku.* Informační technologie způsobují, že geografické vzdálenosti jsou irelevantní. Cíle ve vzdáleném zázemí jsou stejně zranitelné jako cíle na válčišti. Ekonomika i společnost spočívající na vysoce výkonné a propojené informační infrastruktuře vytváří pro potenciální protivníky, připravené k vedení informační války, soustavu přitažlivých strategických cílů.

Existuje „stupňovitý“ efekt těchto rysů: každý z nich vytváří vhodné podmínky pro následující stupeň.

Vstupní náklady

Vzájemně propojené sítě mohou být vystaveny útoku a narušení nejen agresivními státy, nýbrž také nestátními činiteli, včetně rozptýlených skupin či dokonce jednotlivců. Potenciální protivníci mohou mít také rozsáhlé spektrum možností. Ohrožení státu může být značně rozšířeno a bude se neustále měnit s rozvojem složitějších systémů a rozšiřováním potřebných odborných znalostí.

Cena útoku v rámci informační války může být zvýšena zamezením snadného přístupu k sítím a řídicím systémům, využitím nových metod kódování informačního vybavení (softwaru). Tím snad mohou být zmírněna určitá ohrožení, avšak neodstraní se ohrožení propojeného systému zevnitř, např. podplaceným pracovníkem (systémovým operátorem) anebo snad i přímým fyzickým útokem. Zároveň se zvyšují obtíže při zpracování zpravodajských údajů týkajících se útočníků ve strategické informační válce na všech třech zájmových úrovních: strategické, operační a taktické.

Tradiční hranice mizí

Při daném velkém množství možných protivníků, zbraní a strategií je stále obtížnější rozlišovat mezi cizími a domácími zdroji ohrožení a možných útoků vedených prostředky informační války. Nelze vědět, kdo byl napaden kým, nebo kdo je v pozadí útoku. Důsledkem toho jsou:

- značné komplikace při rozlišování tradiční úlohy mezi orgány vnitřní bezpečnosti na jedné straně a národními bezpečnostními a zpravodajskými orgány na straně druhé,
- nemožnost jasného rozlišování mezi různými úrovněmi protistátní činnosti, jejíž spektrum sahá od prostého zločinu, až po vedení války.

Nepřátelské státy mohou upustit od tradičních vojenských nebo teroristických akcí a za využití jednotlivců nebo nadnárodních zločineckých organizací vést „strategické zločinecké operace“.

Ovládání veřejného mínění

Informační válka zvyšuje možnost manipulace s informacemi, které jsou klíčem k formování veřejnému mínění:

- různé politické, teroristické skupiny či nevládní organizace mohou využívat k získávání politické podpory např. Internet,

- vzniká možnost, že „fakta“ týkající se nějaké události mohou být zmanipulována a rozšiřována metodami sdělovacích prostředků,
- a naopak může dojít k poklesu schopnosti dosáhnout či udržet podporu kontroverzních politických akcí u veřejnosti.

Vlády mohou používat Internet třeba jako součást jakékoli veřejné informační (volební) kampaně, proto veřejnost obvykle odmítá podporovat jakákoli mimořádná opatření vlád k „převzetí kontroly“ sdělovacích prostředků (včetně Internetu) jako reakce na možný útok v rámci informační války. Budoucí vlády mohou tedy stát před nesnadným úkolem utvářet a udržovat domácí podporu pro akce v oblasti informační války.

Potřeba strategického zpravodajství

Při řešení zpravodajských problémů informační války budou mít tradiční metody shromažďování a analýzy zpravodajských dat jen omezenou použitelnost. Cíle jsou nesnadno rozpoznatelné, vyčleňování zpravodajských prostředků je obtížné vzhledem k rychle se měnící povaze ohrožení. Zranitelná místa a soubory cílů nejsou dosud správně chápány. Stručně řečeno, stát může jen nesnadno rozpoznat potenciální protivníky, jejich záměry a jejich možnosti. Důsledkem toho je, že je třeba vybudovat nové organizační vztahy v rámci zpravodajských institucí, mezi těmito institucemi a jinými orgány. Také může být nezbytná restrukturalizace rolí a úkolů.

V tomto směru existuje potřeba vybudování mezioborové struktury, která by umožnila koordinované shromažďování a analýzu „cizích“ a „domácích“ zdrojů.

Taktická výstraha a hodnocení útoku

Tento rys vedení války představuje od základu nové problémy v podmínkách kybernetického prostoru. Základním problémem je rozlišování mezi útoky a jinými událostmi, jakými jsou nehody, poruchy nebo proniknutí do systému. Hlavním důsledkem tohoto rysu je, že oficiální orgány nemusí vůbec vědět, kdy došlo k útoku, kdo je útočník, nebo jak byl útok proveden!

Vytváření a udržování koalic

Mnozí spojenci budou zranitelní útoky informační války vedenými na jejich hlavní informační infrastruktury. Například závislost na mobilních telefonech v průmyslových zemích způsobí, že telefonní spojení těchto států bude velmi ohroženo. I další odvětví (energie a finance atd.) mohou rovněž být zranitelnými místy, na která může protivník vést útok, aby zmařil účast v koalici. Takové útoky mohou narušovat realizaci koaličních plánů. Koaliční partneři, kteří naléhavě potřebují vojenskou pomoc, mohou požadovat ujištění, že plán zasazení spojeneckých sil v jejich regionu není zranitelný akcemi informační války.

Zranitelnost zázemí

V informační válce neexistuje žádná frontová linie. Potenciální bojiště jsou všude, kde síťové systémy připouštějí přístup. Ekonomika bude stále více spoléhat na složité, do sítí propojené řídicí systémy v životně důležitých oblastech jakými jsou ropovody, plynovody a elektrické sítě. Ne všichni si uvědomují zranitelnost těchto systémů. Jaké budou prostředky odstrašování a odvety není jisté; mohou spočívat na tradičních vojenských

nástrojích doplňujících hrozbu informační války. Zázemí tedy není chráněno proti útoku zvenčí.

Žádná rázná opatření, např. zastavení provozu infrastruktury, nebudou jako obranná opatření účinná. Je nutno posoudit koncepci „minimální nezbytné informační infrastruktury“ založené na metodách zjištění útoků informační války a metodách obnovy, které budou minimalizovat účinky jakéhokoli narušení sítě.

Analytické a politické zásady pro řešení problémů strategické informační války

Během prováděného výzkumu byla velká pozornost věnována **stanovení možné spodní meze závažnosti ohrožení strategickou informační válkou** vedenou v kybernetickém prostoru. Mnohé existující informační systémy jsou zjevně zranitelné jistou úrovní narušení nebo zneužití. Zároveň je rozvoj v kybernetickém prostoru tak dynamický, že existující „zranitelnost“ může být zmírněna v rámci přirozeného vytváření imunity vůči ohrožením provázejícím každou tak rychle se rozvíjející soustavu. Závislost na počítačovém modelování (na kybernetickém prostoru) v informačních systémech všeobecně rovněž rychle roste a klade zneklidňující otázky, zda může být proces „imunizace systému“ zachován, a tak zabránit, aby nevnikla nebezpečná zranitelná strategická místa, kterých by mohl protivník využít.

Dosud nebyl mezi odborníky nalezen statistický konsenzus v tom, kde se nyní nacházíme na stupnici spektra ohrožení a kam směřujeme. Problém strategické informační války téměř stále postupuje dolů po stupnici (viz obr. 2). Čím více času bylo věnováno tomuto tématu, tím vyvstávalo více a více vážných problémů, které neměly konkrétní řešení a u nichž (v některých případech) ani neexistovala představa, kde začít.

Pravděpodobně důsledky strategické informační války vedou k základnímu závěru: Klíčové předpoklady národní vojenské strategie jsou zastaralé a neadekvátní pro hrozby vytvářené strategickou informační válkou. Autoři komentované studie proto vypracovali pět základních doporučení, týkající se řízení na národní (vládní) úrovni, hodnocení rizik, úlohy vlády, národní bezpečnostní strategie a národní vojenské strategie.

1. Kdo na má být pověřen vedením?

Okamžitým a nutným prvním krokem je zřízení ústředního řídicího orgánu v rámci federální vlády pro zabezpečení koordinované akce proti možnému ohrožení strategickou informační válkou. Tento ústřední orgán by měl být zařazen do „executivního úřadu prezidenta“, protože pouze z této úrovně je možno účinně uskutečňovat nezbytnou mezioborovou koordinaci velkého počtu vládních organizací i spolupráci s americkým Kongresem. Tento orgán musí mít také odpovědnost za úzkou koordinaci s průmyslem. Jakmile bude zřízen, musí okamžitě převzít odpovědnost za zpracování a řešení souborného přehledu problémů strategické informační války na národní úrovni.

2. Hodnocení rizika

Výše uvedený vládní orgán musí jako první krok provést hodnocení rizik a zjištění o možném rozsahu zranitelnosti klíčových prvků systému současné národní bezpečnosti a národní vojenské strategie strategickou informační válkou. Součástí tohoto přehledu budou soubory strategických cílů, účinky informační války a hodnocení zranitelnosti a

Situace:		Závěry:
"USA jsou jedinou a zbývající supervelmocí."		Žádné problémy: ani nyní, ani v budoucnu.
"Protivníci se neodvážejí něco podniknout."		USA mají převahu ve všech směrech.
"Protivníci jsou příliš hloupí."		USA mají technologickou převahu.
"Utřípíme jen menší ztráty."		USA mohou použít vojenskou sílu.
"Informační struktury se automaticky zahojí."		Není nutné provádět nějakou vojenskou akci.
"Informační struktura může být snadno napravena."		Je nutné, aby USA provedly určitou akci.
"Vzrůstá závislost na zranitelných informačních systémech."		Situace se zhoršuje.
"USA mohou být sraženy na kolena velmi rychle malou skupinkou osob, které ovládají vyspělé technologie."		Situace nemůže být horší.

Obr. 2: Spektrum perspektiv

ohrožení. Bez takového hodnocení rizik neexistuje rozumný základ pro rozhodování o otázkách strategické informační války.

Použití síly bude možné odložit, jestliže díky počítačovému modelování vznikne neprostupná, odolná obrana, což je v podstatě velmi reálné. Posílení imunního systému, který je vystaven neustálým útokům, což kybernetický prostor je a nesporně bude, vytvoří pevnou národní informační infrastrukturu. Avšak tak daleko se vývoj ještě nedostal.

3. Úloha vlády

Úloha vlády spočívající v řešení potřeb obrany proti ohrožení strategickou informační válkou se bude vyvíjet. Vláda plní určité základní přípravné funkce, jako je budování vojenských sil. Kromě toho může hrát účinnou úlohu při podpoře (zabezpečování) některých informačních systémů a infrastruktury. Může uplatňovat určitou politiku pro snížení zranitelnosti a usnadnění obnovy.

Důležitým činitelem je změna úlohy vlády spočívající v přechodu od národní obrany veřejné bezpečnosti k obraně veřejného dobra. Vláda v této oblasti bude musit nalézt rovnováhu mezi tím, jak veřejnost pochopí ztrátu občanských svobod, a komerční sektor vládní omezení jeho metod a trhů.

4. Národní bezpečnostní strategie

Po ukončení počátečního vyhodnocení rizika musí národní bezpečnostní strategie řešit připravenost pro zjištěné ohrožení. Připravenost bude překračovat některá tradiční rozhraní mezi vojenským a občanským, mezi zahraničním a domácím a mezi celostátním a místním.

Velmi slibnou může být koncepce „*minimálně důležité informační infrastruktury*“ jako možná strategie obrany proti informační válce. Minimálně důležitá informační infrastruktura je chápána jako minimální kombinace informačních systémů, procesů a zákonů nezbytných pro zajištění plynulého fungování společnosti i za útoku v rámci strategické informační války.

Jedním z rysů této informační infrastruktury může být soubor pravidel a předpisů vydaných vládou pro motivaci vlastníků a provozovatelů různých národních infrastruktur (včetně např. daňového zvýhodňování) k přijetí opatření pro snížení zranitelnosti jejich infrastruktury a pro zajištění rychlé obnovy po útocích v rámci informační války. (Analogickým konceptem je strategická nouzová komunikační síť budovaná pro případ jaderného útoku.)

5. Národní vojenská strategie

Současná americká národní vojenská strategie zdůrazňuje udržení schopnosti přemísťovat vojenské síly na válčiště do klíčových regionů Evropy a Asie (tzv. *power projection*). Vzhledem k již zmiňovaným vznikajícím čtyřem samostatným operačním válčičtím v kybernetickém prostoru (vlastní bojiště, území zúčastněných států, mezinárodní prostředí sloužící ke spojení a přesunům, území státu vedoucího operace v zahraničí) se značně zmenšuje význam vzdálenosti vzhledem k prostoru rozvinutí a zasazení zbraní. Proto může být „zranitelnost“ velení, řízení, spojení a průzkumu (C³I) na bojišti méně významná než zranitelnost národní infrastruktury. Musíme opakovat, plánovací východiska současné národní vojenské strategie jsou zastaralá. Je třeba, aby do národní vojenské strategie byly začleněny také úvahy o rysech informační války.

* * *

Existuje stále riziko, že se Spojené státy mohou v blízké budoucnosti ocitnout v krizi, kdy budou stát přímo před možností informační války, nebo budou existovat alespoň příznaky takového útoku. Jestliže se prezident otáže, zda jsou Spojené státy vystaveny útoku v rámci informační války, a jestliže ano, útoku koho, zda jsou ohroženy americké vojenské plány a strategie, nebude možné odpovědět „nevíme“.

Strategická informační válka je zcela novým pojmem přinášejícím s sebou celou řadu nových problémů. Tyto problémy mohou být vyřešeny, nikoli však bez inteligentního a informovaného vynaložení energie, řídící práce, peněz a jiných zdrojů, uzavírají autoři svůj svůj článek. Plný text provedeného výzkumu je možné nalézt ve zprávě *Strategic Information Warfare*, vydané v Santa Monice, Calif., RAND 1996, nebo na adrese <http://www.rand.org/publications/MR/MR661.pdf>.

-NAS-