Informačné vojny a eDžihád

Tomáš Gál

V ostatných rokoch sa dostáva do popredia termín *infoware* – informačné vojny. Ich koncept je založený na neoddiskutovateľnom fakte, že informácie a informačné technológie nadobúdajú kľúčovú dôležitosť pre národnú bezpečnosť všeobecne a pre jej vojenskú zložku obzvlášť. Žiaden div, keď odhady hovoria o tom, že budúce konflikty sa budú vo vyššej miere dotýkať bojov v informačných systémov. Všetky typy boja s cieľom kontrolovať a disponovať informáciami je potom možné považovať za varianty jedného typu boja a techniky vedenia *infoware* sa tak stávajú aspektmi jedinej disciplíny. Ten, kto zvládne techniky *infoware*, získa výhodu nad tými, ktorým sa to nepodarí. Na informačné vojny možno nazerať z viacerých uhľov pohľadu:

- Informačné vojny, ako samostatné techniky vedenia vojny neexistujú. Čo existuje, je množstvo aspektov informačných vojen, každý náležiaci istému väčšiemu konceptu. Z tohto pohľadu je možné rozlíšiť sedem ucelených foriem *infoware*:
  - *Command-and-control warfare* (C2),
  - *Inteligence wargare,*
  - *Electronic warfare,*
  - *Psychological warfare,*
  - *Hacker warfare,*
  - *Economic Information warfare,*
  - *Cyber warfare.*

Každá z týchto siedmich foriem je len pomerne úzko spojená s ostatnými.

Napriek tomu, že sa informačné systémy stávajú dôležitými, neznamená to, že útoky na ne sa *apriori* stávajú dôležitejšími. Naopak, distribuovanie informačných systémov do veľkej miery zmenšuje nebezpečenstvo vyplývajúce z aplikácii techník *infoware* proti nim.

Informáciu stále nie je možné považovať za nositeľa vojenskej operácie (okrem úzkeho okruhu aspektov). Informačná nadradenosť síce má svoj zmysel, avšak absolútna informačná zvrchovanosť, ktorá môže zabrániť vstupu protivníka do boja, nijako neprevyšuje význam logistickej zvrchovanosti (z čisto taktického hľadiska).

Command and Control Warfare (C2W)

Je to integrované využitie bezpečnostných operácií, klamlivých vojenských útokov, psychologických operácií, rádioelektronického boja, fyzickej deštrukcie, vzájomnej podpory rozviedky na zadržiavanie informácii, vplývania, degradovania alebo ničenia protivníkových schopností velenia a riadenia (Command and control), pri ochrane vlastných schopností velenia a riadenia. Command and control warfare je aplikáciou informačných operácií v rámci vojenských operácií, skrátene C2W. C2W existuje v ofenzívnej aj v defenzívnej forme. Útočná forma bráni efektívne rozvinúť protivníkovi jeho nástroje velenia a riadenia. Defenzívna verzia je zameraná na udržanie operačnej schopnosti vlastné nástroje velenia a riadenia.

Information based warfare (IBW)

O IBW hovoríme, ak sú nástroje zvláštnych služieb prítomné priamo na vojenských operáciách, nie v prípade, kedy ich informačne podporujú. IBW je v rámci *infoware* primárne zamerané na získavanie dát, až sekundárne na ich likvidáciu. Napriek rozdielom v kognitívnych metódach a cieľom, systémy, ktoré zbierajú a podávajú ďalej informácie získané z neživých systémov, môžu byť napadnuté, zmätené, prípadne inak zámerne znehodnocované metódami, ktoré sú efektívne pri systémoch C2W. Obdobne ako pri C2W možno rozlíšiť ofenzívne a defenzívne metódy vedenia IBW.

Electronic warfare (EW)

Techniky EW sú najmä technikmi rádioelektronického boja a kryptografickými technikami. Možno ich považovať za nástroje vedenia komunikačnej vojny. Metódy EW sú zamerané na likvidáciu fyzických možností prenosu informácii (rádioelektronický boj) a na narúšanie dešifrovanie) správ (kryptografický boj). Oba tieto aspekty EW historicky predchádzajú vznik *infoware*. Ich začlenenie do neho je spôsobené orientáciou na informačné technológie na strategickej úrovni. Medzi najvýznamnejšie nástroje EW patria protiradarové nástroje, nástroje zamedzenia komunikácie a šifrovacie nástroje.

Psychologic warfare

Psychologická vojna v rámci *infoware* počíta s využívaním informácií proti ľudskému mysleniu. Vo všeobecnosti zahŕňa štyri kategórie:

- Operácie proti národnému postoju (*national will*),
- operácie proti protivníkovým veliteľom,
- operácie proti nepriateľským jednotkám,
- vedenie kultúrnych konfliktov.

O psychologickej vojne možno tiež povedať, že historicky predchádza *infoware*. *Infoware* jej však dodáva nový rozmer a možnosti koordinácie s inými sofistikovanými nástrojmi a metódami vedenia vojenských operácií.

Hacker warfare

Útoky hackerov sú paradigmou *infoware*. Vojna v kybernetickom priestore, na rozdiel od fyzických konfliktov, je špecifická zameraním sa na časti jednotlivých systémov. Jedná sa o útoky cez bezpečnostné diery v systéme. Dôležitým aspektom hackerských útokov je, že nie sú závislé na fyzickom pôsobení útočníka a môžu prísť z ľubovoľného miesta. Najčastejšie používanými nástrojmi hackerských útokov sú vírusy, logické bomby, trójske kone, červy. *Hacker warfare* narába s pojmom hackerský útok v rámci jeho civilného (nevojenského) nasadenia, keďže čisto vojenský hackerský útok je záležitosťou C2W. Aj keď technika napadnutia systému môže byť vo všeobecnosti rovnaká, útok na vojenský cieľ vyžaduje rádovo vyššiu odbornosť (a pravdepodobne aj nástroje), keďže vojenské informačné systémy sú viac zabezpečované a neexistuje do nich verejný prístup.

Z hľadiska operačného nasadenia môžu byť nevojenské systémy napadnuté fyzicky, syntakticky alebo sémanticky. Hlavnou doménou hackerských útokov sú syntaktické útoky. Otázka fyzického napadnutia môže byť marginalizovaná. Sémantické napadnutia sú doménou *cyber warfare*. Ako všetky predchádzajúce aspekty *infoware*, aj *hacker warfare* môže byť delená na ofenzívnu a defenzívnu.

Economic Information warfare (EIW)

EIW možno považovať za syntézu informačnej vojny a ekonomickej vojny, ktorá môže nadobúdať dve formy:

- Informačnú blokádu,
- informačný imperializmus.

Význam informačnej blokády stúpa s tým, že v súčasnom stave informatizácie znamená informačná blokáda vždy materiálnu blokádu. Zablokovanie prístupu k informáciám (napríklad o prístupe na cudzie trhy) má za následok poškodenie ekonomiky inkriminovaného štátu.

Rovnakým okom treba nahliadať na informačný imperializmus. Zadržiavanie informácií má svoj ekonomický rozmer.

Cyber warfare

Kybernetický boj zahŕňa informačný terorizmus, sémantické útoky, simulovaný boj a Gibsonov útok. Je najmenej postihnuteľný a postrehnuteľný, pretože sa dotýka čisto informačných systémov a má minimálnu fyzickú rovinu. Na druhej strane, kybernetický boj nedosiahol hranicu významu svojej nebezpečnosti, pretože technológie, ktoré by boli potrebné na jeho

plné uplatnenie, ako aj charakteristika jeho optimálnych cieľov, ešte nedosiahli fázu realizácie.

Z hľadiska analýzy využiteľnosti nástrojov *infoware* a ich praktickej aplikácie v moderných konfliktov sa najefektívnejší javí nástroj psychologickej vojny nazývaný *defacement.*

Defacement

Defacement – doslovne znetvorenie, zohyzdenie, ale aj zaškrtanie a prerazítkovanie, etymologicky z angličtiny znamená v kontexte heraldiky a vexiológie pridanie symbolu k pozadiu. V tomto význame možno v angličtine povedať, že „*the national flag of Slovak republic may be described as white-blue-red tricolour defaced by Slovak national emblem.*" (Zástavu Slovenskej republiky možno popísať, ako bielo-modro-červenú trikolóru „orazítkovanú" Slovenským znakom.) V tomto kontexte nie je *defacement* považovaný za zneváženie pozadia, na ktorom je umiestnený, pretože inkriminovaný symbol je zvyčajne využívaný na vyznačenie rozdielov svojho nositeľa od vlastníkov iných symbolov.[1] V terminológií informačných technológií sa rozumie pod *defacement*om webovej stránky jej nahradenie záškodníkom. Existujú viaceré motívy (prejavujúce sa následne aj na formách) *defacement*u, najčastejšie sa však jedná o *defacement* ako druh umeleckého prejavu – grafiti a *defacement* používaný teroristickými skupinami pre rozširovanie ich politického názoru, oznamovanie útokov alebo zosmiešňovanie protivníka.[2]

Táto práca sa bude zaoberať využívaním *defacement*u, ako pomocného prostriedku terorizmu. V tomto poňatí patrí *defacement* svojou povahou do kategórie maligného softvéru, a tak sa stal obľúbenou súčasťou informatického vojnového arzenálu. Už z povahy plánovania útoku a jeho dosahu je zrejmá atraktivita takéhoto typu softvéru pre malé zoskupenia alebo militantné, teroristické skupiny. Je nutné si uvedomiť, že informačná vojna je asymetrická, teritoriálne neobmedzená a náklady na realizáciu útoku vzhľadom k potenciálnym škodám, ktoré môžu byť protivníkovi spôsobené, sú minimálne. (V tomto ohľade informačný útok presahuje všetky možnosti fyzického, vrátane leteckých, ICBM a podobne.)

Možnosti teroristických útokov v *cyberspace* je pestrá paleta. Jedná sa najmä o vírové útoky, DoS útoky, poškodzovanie dát v systéme a podobne. V prípade vyššie menovaných môže byť pomerne komplikované identifikovať zdroj a zámer útočníka. a preto je pomerne komplikované priradiť konkrétny útok k politickému dianiu.

Práve *defacement* je tak jedným z typov informačného útoku, kde je možné identifikovať zámery útočníka, keďže často slúži primárne na jeho zviditeľnenie, prípadne rozšírenie konkrétnych informácií, najlepšie za pomoci infiltrovaných serverov protivníka.

Odborníci sledujúci problematiku sa zhodujú na fakte najímania (skupín) odborníkov na počítačovú bezpečnosť (*hackerov*) pre potreby teroristických útokov. Otázka zneužívania *infowaru* týmito skupinami je sporná. Skupiny *black-hats*[3] sa vo všeobecnosti hlásia ku etickému kódexu, ktorý hovorí, že ich aktivity nemajú poškodzovať používateľské dáta,[4] iné skupiny preferujú zviditeľnenie svojich výsledkov a netaja sa svojimi referenciami.[5] Medzi ich klientov patria všetky zložky ozbrojených síl USA, nemecké a rakúske letectvo a podobne. Možno konštatovať, že ešte minimálne pár rokov si budú aj bohaté a mocné štáty najímať odborníkov na počítačovú bezpečnosť na testovanie svojich serverov, ale aj na útoky na znepriatelené štáty, nadnárodné korporácie a vplyvné združenia.

Z dlhodobého hľadiska možno predpokladať využívanie týchto expertov štátmi s nižšou úrovňou informatizácie a malým počtom vlastných odborníkov vo svojich bezpečnostných agentúrach. Nemožno prehliadnuť očividnú výhodu z asymetrických útokov proti silnejším protivníkom s minimálnymi ekonomickými nákladmi a outsourcovanou zodpovednosťou. Vzhľadom na štruktúru súčasnej mediálnej spoločnosti je tiež významným faktorom veľký počet nezávis-

lých sympatizantov s nonkomformnými združeniami, často prepojenými s teroristickými organizáciami. Najviditeľnejšími sú rôzne antiglobalistické skupiny, prípadne populárno-moslimské združenia. Títo, aj keď nemusia byť vedení jednoznačnou ideológiou, individuálne sa púšťajú do akcií na základe informácií, ktoré majú k dispozícii (či už cez mainstreamové média, alebo rôzne alternatívne webziny alebo blogy).

Vyššie uvedené aktivity možno priradiť k psychologickému boju, kedy pretvorenie webových stránok (prezentácií) má za cieľ vo vhodnom okamihu podporiť účinky okamžitého politického snaženia.

V prípade konkrétneho útoku hrá veľkú rolu lokalizácia cieľa. V prípade jasne špecifikovaných národnostných/etnických/náboženských konfliktov, ako sú Izraelsko-Palestínsky alebo Indicko-Pákistánsky, je pomerne jednoduché nájsť príslušné servre podľa národnej domény prvej úrovne (Napríklad Izrael – Il). V prípade Izraela bola odsledovaná súvislosť medzi politickým vývojom a počtom útokov na Izraelské servre.[6] Rastúce tendenciu takýchto útokov možno odsledovať od roku 2000. V opačnom garde to bol napríklad nedávny útok na protivládny izraelský server indymedia[7] pravicovou skupinou g00ns.[8] Ďalším vyprofilovaným internetovým združením je Internet Haganah, ktorý sa považujú za oficiálny nástroj boja proti zlým fašistickým a moslimsko-fašistickým webstránkam. Okrem narúšania iných stránok elektronicky sa snaží aj o ich fyzické odpojenie.[9]

Konflikt prerastá cez rýdzo politické ciele ľahko k rasovej nenávisti.[10] Medzi Indiou a Pakistanom možno odsledovať útoky hackerov otvorene propagované ako náboženské. Podľa administrátora portálu Zone-H, počínajúc rokom 2001 narastá aktivita skupiny Pakistanských defacerov, WFD, radikálne a emotívne sa vyjadrujúca proti Hinduistom, propagujúca práva Pakistanu na Kašmír.

Po incidente 9-11 vzniká z Pakistanskej skupiny G-force iniciatíva Al Qaeda Alliance, ktorá má za cieľ jednak zjednotiť všetkých moslimských hackerov, jednak koordinovať útoky na západné servre s cieľom získavať a ničiť dôležité informácie. Al Qaeda Alliance bola tvorená najmä členmi skupín G-force, PHC (Pakistani Hacker Club) a A.I.C. (Anti India Crew).

Al Qaeda Alliance úspešne zasiahla veľké množstvo servrov, na ktoré umiestnila nápis „Osama Bin Laden is a holy fighter" a „We urge all the muslims to go to the nearest mosque to get instructed how to join the Jihad". A. I. C. neskôr opúšťa rady Al Qaeda Alliance a zameriava sa na svoj primárny cieľ – Kašmír, možno aj preto, že Pakistan sa oficiálne pridáva do kampane proti Al Qaede. V nedávnej dobe (ostatných 15 mesiacov) sa presúva ťažisko moslimského *defacementu* z Maroka a Egypta do Turecka.

Údaje o *defacemente* ukazujú, že množstvo útokov narastá. Útoky sa stávajú sofistikovanejšími a lepšie koordinovanými (jednak v rámci hackerských komunít, jednak s politickými a teroristickými akciami). *Defacement* tvorí v psychologickej vojne *infoware* nástroj na šírenie individuálnych alebo skupinových názorov, politických, náboženských a inak ideologických. I keď sa týka najmä minoritných, slabo chránených serverov, svoj účinok ako súčasť širšej kampane informačnej vojny má.

Poznámky

1) BBN Technologies: The Arpanet; Foreruner of Today's Internet, http://www.bbn.com/Historical_Highlights/ Arpanet.html, cit.: 1. 2. 2006.
2) Podľa webovej encyklopédie Wikipedia, url: [http://en.wikipedia.org/wiki/Defacement], 21. 4. 2005
3) Jírovský, V.: Defacement – internetové graffiti, nebo zbraň terorismu, Pofessional Computing 11/2004
4) V kybernetickom priestore sú black hats považovaní za tých zlých, kým white hats za tých dobrých. Relativisti upozorňujú, že neexistuje úplne čierna ani biela a všetko sa odohráva v rôznych odtieňoch šedi, fundamentalisti odporujú s tým, že byť považovaný za šedého vyhovuje iba čiernemu, nie však bielemu. Každopádne z pohľadu politických stretov možno uvažovať len o šedi, prípadne počkať, kým víťazi napíšu históriu.
5) Italian black hats, ITBH: Ethical Hacking, url:[http://www.blackhats.it/en/ethical.html], 23. 11. 2002
Black Hat Inc.: Consulting Black Hat, url: [http://blackhat.com/html/bh-consulting/bh-consulting-index.html], 31. 3. 2005
6) Anti-israel: miror url: [http://www.zone-h.org/defacements/mirror/id=2205779/], 31. 3. 2005, KHG miror url: [http://www.zone-h.org/defaced/2005/03/22/www.go-israel.com/forum/], 22. 3. 2005, TURKISH HACKERS: miror url: [http://www.zone-h.org/defacements/mirror/id=2159038/], 9. 3. 2005 (Turkish hackers zaznamenali celkovo v marci množstvo úspechov: http://www.uploads.co.il, http://www.romtes.com, http://www.snb.co.il, http://www.kamea.co.il, http://www.ilanascabin.co.il, http://www.loren-lee.com, http://www.gymservice.com, http://www.galimcenter.co.il, http://www.gan-henya.co.il, http://www.emails.co.il, http://www.ehbinc.com, http://www.ecodrive.co.il, http://www.e-studio.co.il, http://www.cir.co.il, http://www.bsd-ins.co.il, http://www.brandup.co.il, http://www.aviv-bakfar.co.il.
7) G00ns: miror url: [http://www.zone-h.org/defaced/2005/04/27/israel.indymedia.org/], 29. 4. 2005
8) http://www.g00ns.com/
9) Podľa internetovej prezentácie http://www.haganah.us
10) Napríklad stránky vyprodukované skupinou BHI ohlasujú: „*fuck to ALL ARABS and who support THEM"*.

Použitá literatúra:

JÍROVSKÝ, V.: *Defacement – internetové graffity, nebo zbraň terorismu*, Professional Computing 11/2004

BURGER, R.: *Das grosse Computer-Viren Buch,* 3.erweiterte Auflage, Data Becker, Dusseldorf, 1988

HARWEY, G.: *Website Defacers – the Grafitti artists of the internet*, Sitepoing 2003

Elektronické zdroje:

Blog Chronwatch, url: http://blogs.chronwatch.com/, cit. 25. 5. 2005

Internet Haganah, url: http://www.haganah.us, cit. 25. 5. 2005

Zone-H3, url: http://www.zone-h.org, cit. 25. 5. 2005

G00ns, url: http://www.g00ns.com/, cit. 25. 5. 2005

Italian black hats, ITBH: Ethical Hacking, url:[http://www.blackhats.it/en/ethical.html], 23. 11. 2002

Black Hat Inc.: Consulting Black Hat, url: [http://blackhat.com/html/bh-consulting/bh-consulting-index.html], 31. 3. 2005

IWS: Information warfare site, url: http://www.iwar.org.uk/index.htm, cit. 25. 5. 2005

Astalavista: url: http://astalavista2.box.sk, cit 25. 5. 2005