INFORMAČNÍ POLITIKA – POSLEDNÍ PŘÍLEŽITOST

CHCETE SE K NĚČEMU VRÁTIT?

Pokud ne, tak…

- … co je podle Vás informační politika?
- … jaká témata IP řeší?
- … jaká témata už znáte a jaká ne dost?
- … jaké úspěchy a jaké neúspěchy IP znáte?
- … nějaké dotazy ke zkoušce?

PROBLÉMY V INFORMAČNÍ SPOLEČNOSTI

Negativní stránka informační společnosti

- Předchozí přednášky pozitiva – teď druhá stránka
- Ohroženi všichni
  - Občané – viz předmět Informační bezpečnost
  - Organizace – ICT stále podstatnější, růst konkurence i v neziskovém sektoru – nutné chránit informace => informační politika instituce
  - Stát – hrozba informační války

INFORMAČNÍ VÁLKA – BUDOUCNOST KONFLIKTŮ

Kdy je státní správa cílem?

- Státní správa největší správce OÚ
- Množství počítačů a techniky k ovládnutí
- Cílem mohou být zaměstnanci jako jiní uživatelé, ale i zesměšnění státní správy či (h)acktivismus
- INFORMAČNÍ VÁLKA

Co je informační válka

- Po každé válce odpor lidí ke konfliktu
- Nezmizí, ale jistě se změní vlivem informační války
- Zohledňováno i ve vojenských dokumentech, např. Joint Vision 2020 v USA
- Informační válka = bojová činnost využívající informace či ICT nebo proti informacím či ICT
- Různé definice, časté dva přístupy – vylepšení klasických X nová forma války

Typy informační války (dle Libického)

- Command-and-Control Warfare – zničení vedení či komunikace s ním
- Intelligence-Based Warfare – zpravodajská válka, např. špionáž, průzkumné akce, senzory statické nebo v komunikaci
- Electronic Warfare – antiradarová, antikomunikační (na úrovni signálů) nebo kryptografie (správně kryptologie)
- Psychological Warfare – manipulace s informacemi, dělení: proti národní morálce, velitelům, vojákům, kultuře
- Hacker Warfare – výhradně činnost hackerů, oproti cyberwarfare mohou být prostředky i fyzické povahy
- Economic Information Warfare – manipulací získání ekonomické převahy; informační blokáda nebo imperialismus
- Cyberwarfare – válka čistě v kyberprostoru; dělení: informační terorismus, sémantické útoky, simulované boje v kyberprostoru, Gibson warfare (ve virtuálních světech, např. sexuální obtěžování, pomluvy…)

Specifika informační války

- Výrazný vliv na vítězství i konvenčně slabší armády
- Využití ovlivněno i (relativně) nízkými náklady na zbraně X prevence velmi drahá, nutné stále udržovat, i když k ničemu nedojde
- Útok někdy těžké rozpoznat – denně tisíce útoků na vojenské cíle bez ambice konfliktu, jen kriminalita
- Vždy podoba války podle zamýšleného cíle – dnes klíčové ICT => vhodná informační válka
- Lze zasáhnout cíl nehledě na geografii (dříve fronta X týl), tím i stírání rozdílu civilní X vojenské cíle, kvůli menší chráněnosti lze napadnout i civilní infrastrukturu
- Cíle: kritické infrastruktury (dodávky energií, vody, informační a komunikační systémy, nouzové služby, zásobování potravinami, státní správa a samospráva…) a kritické informační infrastruktury

Metody informační války - manipulace

- Nejen nástroj informační války
- Nutný správný výběr komunikačních kanálů, záleží na cíli
  - Tradiční média (tisk, televize) pasivní – ideální pro ty, kteří je ovládají (stát)
  - Internet obousměrný – umožňuje rychlou a levnou manipulaci i malými skupinami (IRA, Al Qaeda, neonacisté…), monitorování státem nákladné až nemožné, po zablokování či zničení snadné migrovat a pokračovat
- Př. ve válce ve Vietnamu manipulace médii – pobouření americké veřejnosti televizními záběry – stažení vojsk, tím prohra (zvláštní případ, většinou každý stát svá média využije pro svůj prospěch)

Techniky manipulace (dle Boháčková, s. 56-59)

- Účelová selekce informací
- Řazení informací
- Využití emocí
- Výběr komentátorů
- Kontext sdělení
- Nesrozumitelné zprávy
- Podprahové techniky
- Kombinace výše uvedených

Diskuze – WikiLeaks 2010

- Co je WikiLeaks?
- Co se stalo v roce 2010?
- Lze onu situaci označit za informační válku? Proč?
- Jak na to reagovaly vlády a jak veřejnost?
- Jaký to mělo ohlas v ČR?
- Jak zakladatel dopadl dnes?
- Jste pro nebo proti WikiLeaks a podobným službám?

Použitá literatura

- BASTL, Martin. Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví. Brno, 2007. 153 s. Disertační práce.
- BITTMAN, Ladislav. Mezinárodní dezinformace: černá propaganda, aktivní opatření a tajné akce. 1. vydání. Praha: Mladá fronta, 2000. 358 s. ISBN 80-204-0843-6.Masarykova univerzita, Fakulta sociálních studií.
- BOHÁČKOVÁ, Gabriela. Kvalita a objektivita informací v médiích: pravda versus manipulace a dezinformace. Brno, 2006. 120 s. Diplomová práce. Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví.
- Europe‟s Information Society Thematic Portal [online]. 2009 [cit. 2010-06-26]. Critical Information Infrastructure Protection – a new initiative in 2009. Dostupné z WWW: <http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm>.
- HAENI, Reto E. Information Warfare: an introduction [online]. Washington DC: The George Washington University, 1997 [cit. 2010-04-23]. Dostupné z WWW: <http://www.trinity.edu/rjensen/infowar.pdf>.
- JANCZEWSKI, Lech; COLARIK, Andrew. Managerial Guide for Handling Cyber-Terrorism and Information Warfare. London: IGI Global, 2005. 229 s. ISBN 1591405491.
- JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vydání. Praha: Grada Publishing, 2007. 284 s. ISBN 978-80-247-1561-2.
- Joint Vision 2020 [online]. 2000 [cit. 2010-04-23]. Dostupné z WWW: <http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/joint_vision_2020.pdf>.
- LIBICKI, Martin. What Is Information Warfare? [online]. 1995 [cit. 2010-04-25]. Dostupné z WWW: <http://www.afcea.org.ar/publicaciones/libicki.htm>.
- Ministerstvo vnitra České republiky [online]. 2010 [cit. 2010-06-25]. Pojmy. Dostupné z WWW: <http://www.mvcr.cz/clanek/kritickainfrastruktura.aspx>.
- MLEZIVA, Emil. Diktatura informací: jak s námi informace manipulují. 1. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2004. 133 s. ISBN 80-86898-12-1.
- MOTEFF, John; COPELAND, Claudia; FISCHER, John. Critical Infrastructures: What Makes an Infrastructure Critical? [online]. 2003 [cit. 2010-06-25]. Dostupné z WWW: <http://www.fas.org/irp/crs/RL31556.pdf>.