MASARYKOVA UNIVERZITA

Informační politika - poslední příležitost

13.12. 2013

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?

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 – viz předmět Informační management
  - Stát – hrozba informační války

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

- Podoba války dle cíle – dnes klíčové ICT => informační
- Informační válka = bojová činnost využívající informace či ICT nebo proti informacím či ICT
- Zohledňováno i ve „vojenských/policejních“ dokumentech, např. Joint Vision 2020 v USA (2000), Politika EU pro boj proti terorismu: dosažené úspěchy a budoucí úkoly (2010)
- Cíle: kritické infrastruktury = informační a komunikační systémy, dodávky energií, vody, nouzové služby, zásobování potravinami, státní správa a samospráva…

Specifika informační války

- Výrazný vliv na vítězství i konvenčně slabší armády
- (Relativně) nízké náklady X prevence velmi drahá, nutné stále udržovat, i když k ničemu nedojde
- Útok někdy těžké rozpoznat – denně tisíce útoků bez ambice
- 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

Typy informační války (dle Libického)

- Command-and-Control Warfare – zničení vedení či komunikace s ním
- Intelligence-Based Warfare – zpravodajská válka
- Electronic Warfare – antiradarová, antikomunikační (signály) nebo kryptografie (správně kryptologie)
- Psychological Warfare – manipulace proti národní morálce, velitelům, vojákům, kultuře
- Hacker Warfare – výhradně činnost hackerů, ale prostředky i fyzické
- Economic Information Warfare – informační blokáda nebo imperialismus pro ekonomickou převahu
- Cyberwarfare – čistě v kyberprostoru; dělení: informační terorismus, sémantické útoky, simulované boje v kyberprostoru, Gibson warfare (ve virtuálních světech)

Metody informační války - manipulace

- Nutný správný výběr komunikačních kanálů, záleží na cíli
  - Tradiční média pasivní – pro ty, kteří je ovládají (stát)
  - Internet obousměrný – rychlá a levná manipulace i malými skupinami (IRA, Al Qaeda, neonacisté…), monitorování státem nákladné až nemožné, po zablokování či zničení snadné migrovat a pokračovat
- Techniky manipulace (dle Boháčková, s. 56-59): účelová selekce informací, řazení informací, využití emocí, výběr komentátorů, kontext sdělení, nesrozumitelné zprávy, podprahové techniky, kombinace uvedených
- Př. ve válce ve Vietnamu pobouření americké veřejnosti televizními záběry => stažení vojsk, tím prohra (zvláštní, většinou každý stát svá média pro svůj prospěch)

Úkol č. 10

- Vyplňte do 15. 12 (příp. na druhý termín 19. 12.) dotazník na adrese: http://survs.com/survey/8f37gid4lo
  - Snažte se o konstruktivní kritiku
  - Odpovědi nebudou mít vliv na hodnocení za předmět
  - Úkol splněn za vyplnění všech odpovědí
  - Odpovědi zásadní pro otestování funkčnosti výzkumného nástroje + přenos poznatků do jiných předmětů a mé výuky
  - Po průchodu kontrola vyplnění (pro uznání úkolu), ale v dotazníku neuvádíte jméno

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: 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: 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: 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: http://www.afcea.org.ar/publicaciones/libicki.htm
- Ministerstvo vnitra České republiky [online]. 2010 [cit. 2010-06-25]. Pojmy. Dostupné z: 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: http://www.fas.org/irp/crs/RL31556.pdf