Kybernetické konflikty, kybernetická válka

Národní centrum kybernetické bezpečnosti

Předmět Kybernetická bezpečnost
FSS MU
Podzim 2015

Václav Borovička

Osnova přednášky

- Kybernetické konflikty
- Kybernetická válka
- Hybridní válka
- Případové studie

Trocha teorie

Kybernetický konflikt

- klasická otázka --> co to je?
- Neustálená definice
  - „Stav, kdy národy a nestátní aktéři užívají útočné a obranné kybernetické kapacity k útoku, obraně nebo špehování druhého státu, typicky kvůli politickým nebo jiným národně-bezpečnostním důvodům. Obecně kybernetický konflikt nezahrnuje kybernetickou kriminalitu, ale zato je nadřazeným pojmu ‚kybernetická válka'" (Healey 2013)
  - „Politicky motivované konfliktní jednání velkého rozsahu založené na užití útočných a obranných kapacit s cílem narušit digitální systémy, sítě a infrastrukturu, včetně použití kybernetických zbraní a nástrojů státními, nestátními či transnacionálními aktéry ve spojení s dalšími prostředky dosahování politických cílů" (Mulvenon a Rattray 2013)
  - „Použití kybernetických útoků, které musí zahrnovat útoky proti integritě nebo dostupnosti systému, k dosažení politických cílů" (Lorents a Ottis 2010)

Trocha teorie

(Kybernetický) konflikt

- Obecně lze přejmout definici z konfliktologie, tedy *„střet mezi jasně definovatelnými aktéry, kteří usilují o uplatnění svého zájmu v jedné nebo více shodných oblastech, přičemž tito aktéři pociťují vzájemný střet jako situaci, kdy zisk jedné strany znamená ztrátu druhé“* (Pšeja 2002)

  - musí mít **aktéry**, jimiž jsou standardně státy, třebaže narůstá frekvence případů, kdy se na konfliktech podílejí i aktéři nestátní;
  - musí mít jasně definovatelnou **oblast střetu**, která je náplní konfliktu;
  - musí být přítomno **napětí**, které funguje jako predispozice konfliktu a které je typicky vyjádřeno v postojích, jako je nedůvěra apod.;
  - nutnou složkou konfliktu je pak **jednání**, které má podobu opatření a kroků realizovaných stranami konfliktu (Šmíd 2010).

Trocha teorie

Kybernetický konflikt

- Kybernetický konflikt je podřazen konfliktu obecnému, přičemž uvozuje spíše aktuální škodlivé aktivity mezi jednotlivými aktéry a nelze jej považovat za konflikt sui generis
  - ne latence, často ne ani artikulace, až jednání
- Kybernetická špionáž?
  - dostupnost, integrita, důvěrnost (!)
- Obecně kybernetický konflikt nezahrnuje kybernetickou kriminalitu, ale zato je nadřazeným pojmu ‚kybernetická válka‘.

Trocha teorie

Kybernetická válka

- Aktivity národního státu s cílem proniknout do počítače a sítě jiného národa se záměrem způsobit škodu nebo určité rušení (Clarke a Knake 2010)
- „Jednání národního státu s cílem poškodit nebo rušit počítače a sítě jiného národa, které způsobuje značné poškození nebo ničení – efekty podobné jako při použití tradiční vojenské síly – a je proto považováno za ozbrojený útok. Národ v kybernetické válce je de facto v opravdové válce, což znamená, že v reakci na takový útok může použít smrtící sílu.“ (Healey 2013: 281)
- „Použití počítačů a Internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků.“ (AFCEA 2015)

Trocha teorie

Kybernetická válka

- často užívaný pojem
  - nadužívání – úprava mindsetu?
- nejasné používání
  - cyber war X cyber warfare
- už probíhá? X nastat nemůže?
- Bezpečnostně-vědní chápání -> Clausewitz
  - stav, kdy státy vyvíjí aktivity ke zničení nebo narušení počítačů nebo sítí jiného státu, což by mělo za následek těžké ztráty v důsledcích podobné, jako kdyby byly dosaženy konvenčními silami. Kybernetická válka je de facto vždy klasickou mezistátní válkou, avšak vedena zejména prostřednictvím kyberprostoru.

Trocha teorie

Hybridní válka

- jedna z prvních diskuzí nad tímto pojmem v rámci Libanonské války (2006)
- vysoce integrované použití různých vojenských a nevojenských prostředků s cílem dosáhnout strategického cíle (Sari 2015)

- jakákoli hrozba včetně jakékoli reakce může být hybridní, pokud není limitována na jedinou formu a dimenzi válečnictví

  X

- hybridní je tedy tehdy, pokud využívá plné spektrum technik

- konflikty byly vždy definovány snahou využít zranitelností a slabin protivníka
  - s komplexností roste počet potenciálních zranitelnosti
  - expanze války do dalšího oblastí - cyber

Trocha teorie

Hybridní válka, cyber (a právo)

- cyber
  - důležitou součástí hybridní války
  - využívání charakteristik cyberu
  - využívání právního rámce ve svůj prospěch
    - právní podmínky k použití síly – odstrašení funguje daleko méně
    - zvyšující se důležitost práva v mezinárodních vztazích
  - snaha operovat těsně pod reakční hranicí protivníka !!!
    - mnoho institutů navázáno na „armed attack“ a „use of force“
    - snaha vyhnout se atribuci a odplatě
- hybridní válka systematicky využívá těchto hraničních bodů, chyb a mezer právního rámce
- již nelze rozlišovat mezi válkou a mírem – neustálý stav konkurence

Trocha teorie

Kyberprostor - charakteristiky

i. dostupnost kyberprostoru z různých částí světa
ii. rozšířenost využívání informačních a komunikačních technologií připojených do veřejných sítí
iii. komplexnost
iv. komplikovanost
v. triviálnost
vi. virtuálnost kyberprostoru
vii. aktivizační potenciál

[...]

Trocha teorie

Fenomény

- hacktivismus – politický cíl, primárně neškodící; spíše protest než boj
- kyber-povstalci – pouze koncept; politické cíle, destruktivnější prostř.
- kyber-terorismus – strach, cílení na populaci, politický cíl
- kriminální aktéři – zaměřeno na zisk
- klasický hacking – motivací spíše skill, Solar Sunrise
  - White hats – „etičtí hackeři“, pentesting apod.
  - Black hats – zisk, sláva, skilly, fragy --> cyber-crime?
- patriotický hacking – zapojení obyvatelstva do útoků
  - rozdíl oproti hacktivismu – > v souladu se státem
  - výhodnost pro stát?

Případové studie

Kybernetické konflikty

Estonsko (2007)

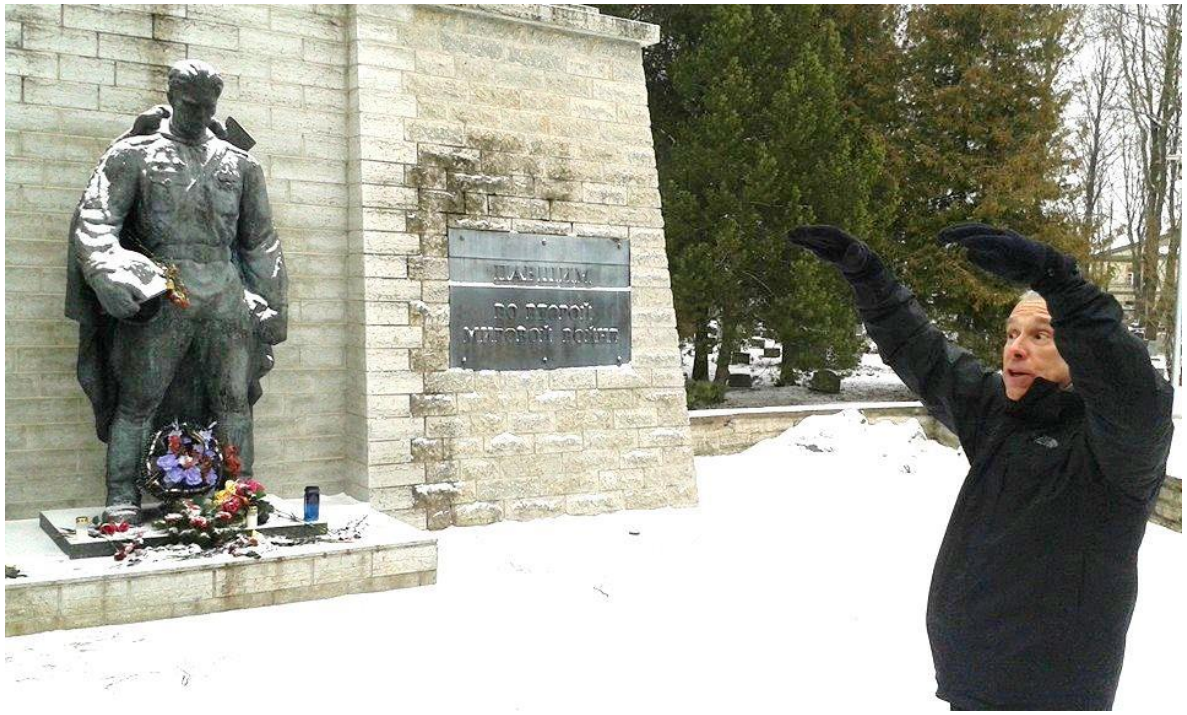
- jedna z vedoucích zemí co se rozvoje ICT a e-governmentu týče
  - důvody?
- geopolitická situace
  - součástí EU, NATO; bývalá země SSSR, sousedí s Ruskou Federací
  - početná ruská menšina, ne celá však integrována
  - spory s RF (ideologické – nahlížení na poválečnou dobu)
- na ICT závislá celá země – kritické subjekty i služby každodenního fungování
- využívání X-Road

- V lednu 2007 oznámila EST vláda úmysl přesunou bronzovou sochu z centra na vojenský hřbitov

Případové studie

Kybernetické konflikty

Estonsko (2007)



Případové studie

Kybernetické konflikty

Estonsko (2007)

- bronzová socha – pomník neznámého sovětského vojáka
  - spor o nazírání na historii
    - Rusové – symbol osvobození, Estonci – symbol okupace
  - návaznost na vrcholící volební kampaň
- při přesunu velké demonstrace
  - 1 mrtvý, stovky zraněných, až 1300 lidí zatčeno
  - trvání v řádu několik dní, škody až 4,5 milionu eur
- zároveň nóta ze strany Ruska + protesty ze strany ruského lidu
  - přijata rezoluce odmítající přestěhování sochy; navrhnut bojkot estonského zboží a služeb
  - pohrůžka přerušení diplomatických styků
- ➢ v pozadí těchto událostí – kybernetické útoky

Případové studie

Kybernetické konflikty

Estonsko (2007)

- 1. fáze útoků (27. dubna – 29. dubna)
    - označována jako „emoční reakce“
    - relativně malá sofistikovanost
- 2. fáze útoků (30. dubna – 18. května)
    - sofistikovaná, cílená, těžká
    - 4 vlny
    - DDoS útoky, defacement, útoky na DNS (ISP), spam
    - využití botnet, webová fóra a jednoduché prográmky
    - patriotický hacking – hacktivismus

Případové studie

Kybernetické konflikty

Estonsko (2007)

- <u>Cíle</u>
  - vládním stránky a sítě
    - weby vlády, premiéra, prezidenta, parlamentu, jednotlivých ministerstev, vedoucí koalice
  - soukromý sektor
    - zpravodajské portál, bankovní sektor
    - telekomunikace (i administrátor národní domény!)
- <u>aktéři</u>
  - zdroj útoku – 178 zemí světa
  - hnutí Naši – přiznání zapojení do útoků
  - sofistikovanost – Rusko?

Případové studie

Kybernetické konflikty

Estonsko (2007)

- využívání národního sentimentu, percepce konfliktu
- dopady
  - odříznutí EST od světa na dobu několika dnů
  - Estonsko – masivní aktivizace společnosti v oblasti kybernetické bezpečnosti
  - wake-up call pro ostatní státy, zejména v rámci NATO
- odpovědnost za útoky?

Případové studie

Kybernetické konflikty

Litva (2008)

- Podobně jako Estonsko, k Ruské Federaci velmi blízko
  - Soused RF, dříve součást SSSR
- Méně etnických Rusů oproti Estonsku – populačně jednotnější
- Menší ICT vyspělost v rozšíření ve společnosti*

- Kybernetické útoky se objevily v době přijetí zákona o zákazu nacistických a sovětských insignií
  - Rusové v Litvě překvapivě nijak zvlášť nereagovali
  - Ruská Federace silné protesty
- plány na vybudování americké protiraketové obrany
- blokování rozhovorů EU-Rusko Litvou

Případové studie

Kybernetické konflikty

Litva (2008)

- 28. června 2008 bylo napadeno výrazné množství litevských webů, současně s útokem vzrostla aktivita na ruskojazyčných webových fórech a diskuzích
- Cílem útoků byly zejména webové portály subjektů ze soukromého sektoru
  - Z vládního sektoru bylo pouze 5% zasažených portálů
- Způsob útoků – jednotvárný, využívající jedné chyby u 1 poskytovatele webhostingu, zejména defacenemt
- Oproti útokům na Estonsko se lišily dobou trvání, použitými technikami a zejména v dopadem na bezpečnost a fungování země
- Aktéři – neznámí, zdroj - neznámý – servery v západní Evropě + východně od Litvy
- Opět využívání sentimentu – širší geopolitické zájmy
  - veřejné ospravedlňování útoků na ruských hackerských serverech
  - *"pokud nic neuděláte, nejste loajální ke své zemi"*

Případové studie

Kybernetické konflikty

Gruzie (2008)

- první případ viditelných kybernetických operací na podporu konvenčních útoků
  - skutečně?
- Kontext:
  - Nezávislost Gruzie na SSSR až v roce 1990
  - Spory mezi Gruzínci a ruským etnikem + problém autonomie oblastí Jižní Osetie a Abcházie
  - 2008 – po sporech mezi Abcházií, Osetií a Gruzií utužování centrální vlády
    - v reakci Rusko navázalo diplomatické styky s těmito oblastmi
    - Gruzie reagovala posílením tlaku
- Eskalace konfliktu na obou stranách
  - Gruzie ignorovala problémy Abcházů a Osetinců
  - Rusko naopak stupňovalo tlak na Gruzii proti sbližování s NATO a EU

Případové studie

Kybernetické konflikty

Gruzie (2008)

- Eskalace až do podoby ozbrojeného konfliktu
  - 1. srpna boje mezi Gruzií a Jižní Osetií, 7 .srpna vpád Gruzinců do Osetie
  - 8. srpna 2008 vpád ruských jednotek
  - válečný stav od 9. do 12. srpna 2008 – ruské jednotky značná převaha
- Vedle ozbrojeného konfliktu další spory
  - geopolitický spor mezi Ruskem a NATO
  - budování ropovodu a potrubí zemního plynu Baku – Tbilisi – Ceyhan
    - oslabení ruské pozice
- Používání ICT v Gruzií nízké, nikoli zanedbatelné
  - zpravodajství, finančnictví, vládní služby
- Nízká konektivita do celosvětové sítě

Případové studie

Kybernetické konflikty

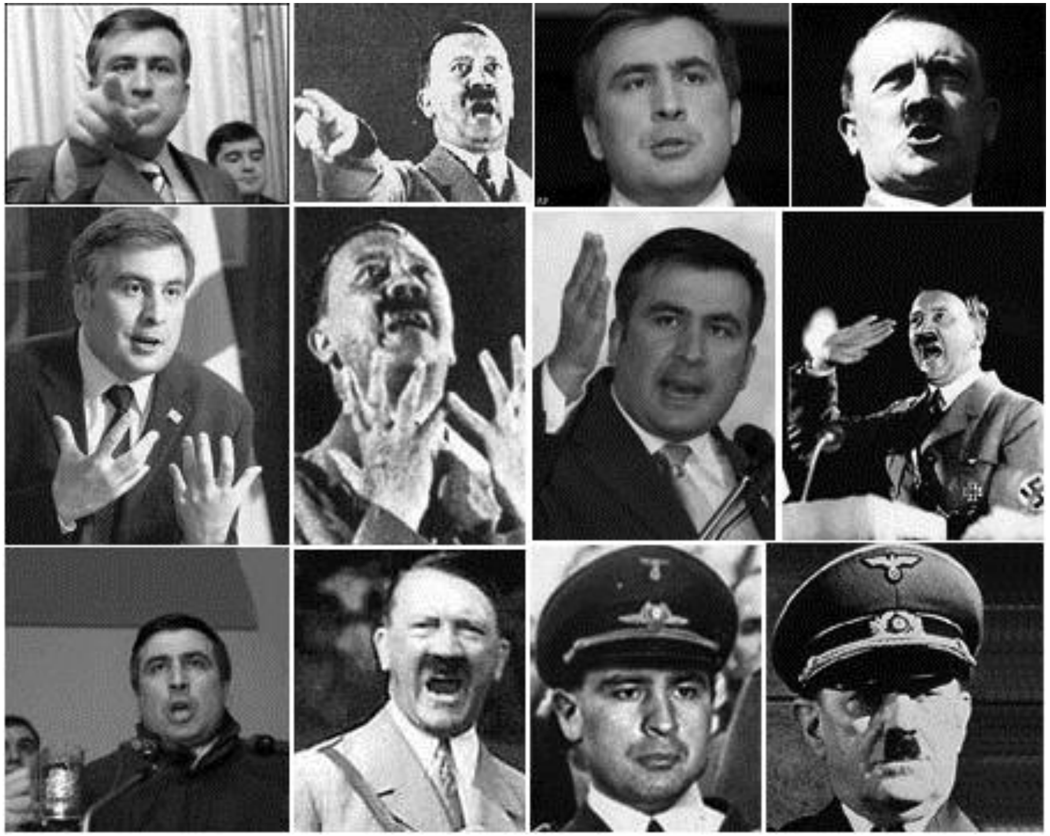
Gruzie (2008)

- Útoky:
  - první signály již několik týdnů předem, poté bezprostředně před
    - stránky prezidenta, informační agentura OSinform
  - hlavní kampaň od 7. srpna
  - V rámci útoků byla mezi jednotlivými daty obsažena i opakující se zpráva „win+love+in+Rusia“
  - Cíle:
    - ISP
    - mobilní telefonie
    - zpravodajských serverů
    - vládní stránky (prezident, parlament, ministerstva)
    - servery podporující záměry či pozice Gruzie (fóra, komunitní portály)

Případové studie

Kybernetické konflikty

Gruzie (2008)



http://randomdrake.com/georgiahitler.jpg

Případové studie

Kybernetické konflikty

Gruzie (2008)

- Způsoby útoků:
  - DoS, DDoS; defacement; spam; malware
  - využití „patriotických hackerů“ – jednoduchý *.bat soubor
  - botnety – pravděpodobné zapojení Russian Business Network
  - špionáž
- Dopady:
  - ztížena komunikace se zahraničím
  - ztížená informovanost vnitrostátně
    - informační výhoda?

- Několik útoků také proti ruským serverům

Případové studie

Kybernetické konflikty

Gruzie (2008)

- Aktéři?
  - opět neexistuje přímý důkaz o zapojení Ruské Federace
  - Russian Business Network, ruští hackeři i „spořádaní“ občané
  - proč by Rusko nepřiznalo kyber kampaň, když konvenční útok byl jasný ??
  - mezinárodní společenství – Google, Polsko, Estonsko, soukromá sféra
- koordinace, načasování – pravděpodobné zapojení vládních/vojenských složek
  - nemožnost si představit tyto aktivity pouze jako aktivity sroceného kybernetické ruské veřejnosti
- Opět využití kyberprostoru pro politické cíle
  - Gruzie vyobrazena jako zločinecký stát – u Rusů úspěch (až 80% souhlasilo s intervencí)
  - Mezinárodně úspěch spíše Saakašvili

Případové studie

Kybernetické konflikty

Gruzie (2008)

Zapojení obyčejných civilistů bylo vzhledem k rozšířenému sentimentu ve společnosti a zároveň rychle rozšířených informací o možnostech „přispět“ k boji velmi pravděpodobné.

Korns a Kastenberg (2009: 65-66) k tomu pak dodávají:

*„Naopak, internetový žurnalista vstoupil na webový portál [na kterém byla ruská hackerská komunita aktivní – pozn. autora] a stáhl si předchystaný software, který mu umožnil, pokud by se rozhodl, se připojit k útokům. Jeho stanovisko: ‚**Za méně než hodinu jsem se stal internetovým vojákem. Nedostal jsem žádné telefonáty ze strany kremelských operativců** ... s paranoiou, že má Kreml své ruce všude, riskujeme podcenění velkého patriotického běsnění mnoha obyčejných Rusů, kteří ... se nepochybně rozhodli jít na internet, aby se naučili, jak učinit nějakou spoušť, tak jako jsem se rozhodl já. **V rámci jedné hodiny se taktéž mohli stát kybernetickými válečníky.**‘“*

Případové studie

Kybernetické konflikty

Kyrgyzstán (2009)

- Kontext:
  - nesousedí s Ruskem, ale významné ruské zájmy
  - prorostení ICT nízké, křehká infrastruktura
  - po Tulipánové revoluci větší spolupráce s USA
  - základna v Manasu (kvůli Afghánistánu mj.)
  - V lednu 2009 rozhodování o budoucnosti základny
    - Rusko tlačilo na uzavření – příslib pomoci
- Cíle:
  - útoky zamířeny na ISP (2 - 3 ze 4)

Případové studie

Kybernetické konflikty

Kyrgyzstán (2009)

- Způsob:
  - DDoS - pravděpodobně pomocí botnet RBN – ruské IP
- Dopady:
  - útoky ovlivnily zejména kyrgyzskou opozici
  - 2 týdenní omezení internetového připojení

- Odpovědnost?
  - Rusko?
  - Kyrgyzstán?

Závěr

Dotazy?

Diskuze?

Anyone?

Závěr

Děkuji za pozornost!