# Kybernetické konflikty v postsovětském prostoru 2007-2009

Tomáš Maďar
t.madar@mail.muni.cz

# Timeline

- Estonsko 2007
- (Bělorusko 2008)
- Litva 2008
- Gruzie 2008
- Kyrgyzstán 2009

# Estonsko

# Estonsko

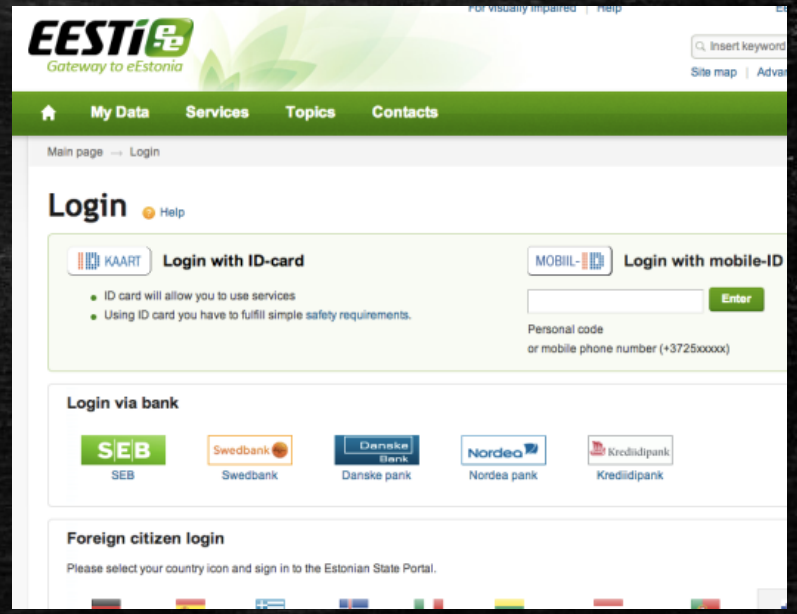

FINLAND
Helsinki
Saint Petersburg
RUSSIA
SWEDEN
Stockholm
Tallinn
ESTONIA
LATVIA

# Estonsko

- Populace: 1 340 000 (2011)
- Národnostní složení (2010):
  1. Estonci 68,8 %
  2. Rusové 25,5 %
  3. Ukrajinci 2,1%
  4. Bělorusové 1,2 %
  5. Finové 0,8 %
- Celková vysoká dostupnost internetu – téměř absolutní penetrace
- Důležitý historický kontext
- Geopolitika

# Průkopník e-Governmentu

- Počátek v polovině 90. let
- Internetové bankovnictví, jízdenky, daně, parkování
- Protokol „pivo a sauna“
- Od r. 2005 online volby (nejprve komunální)
- Kvůli volbám vytvořena pracovní skupina
- Online portál pro kontakt se státní správou
- Bezpapírová vláda od roku 2001



# Historický kontext

- Po porážce Švédska 1721 Nystadská smlouva: Estonsko pod ruskou nadvládou
- 24. únor 1918 – nezávislost
- 1918-1920 Estonská osvobozenecká válka
- Pakt Ribbentrop-Molotov – Estonsko 1940 anektováno SSSR
- 1941 dobyto Třetí říší
- 1944 dobyto zpět Rudou armádou, 46 let okupace
- Opětovná nezávislost vyhlášena 20. srpna 1991
- 2004 vstup do NATO i EU

# Politický kontext útoků

- Přesun památníku Bronzového vojáka součástí předvolební kampaně
- Vítězem Estonská reformní strana v čele s premiérem Ansipem
- Rozhodnuto o přesunu pomníku
- Odmítavá vyjádření ruských představitelů o politizaci historie, prohlášení Putina, vicepremiér Ivanov volá po bojkotu EE zboží
- 26. duben 2007 – protesty a pouliční nepokoje
- 27. duben 2007 – první kybernetické útoky
- Historický význam 9. května
- Problematický vztah s Ruskem, ruský nacionalismus

# Bronzový vojak

# Útoky na Estonsko I.

- Délka trvání: cca 4 týdny (27. duben – 18. květen 2007)
- 2 fáze útoků, několik vln v rámci druhé fáze
- Užité metody:
  1. DDoS
  2. Defacementy webových stránek
  3. Útoky na DNS servery
  4. E-mailový spam
  5. Spam komentářů na zpravodajských serverech
- Desetinásobný nárůst trafficu v zemi, vrcholný útok dosáhl 3 gbps (útok na bankovní sektor, útoky na veřejnou správu o několik řádů nižší)
- Do útoku celkem zapojeny počítače ze 178 zemí

# Útoky na Estonsko II.

- Spektrum cílů:
  1. Servery institucí zodpovědných za internetovou infrastrukturu
  2. Vládní a politické cíle (parlament, prezident, ministerstva, pol. strany, státní agentury)
  3. Služby poskytované soukromým sektorem (banky, zpravodajství)
  4. Osobní a náhodné cíle
- V první, živelné fázi vlastenecky/politicky motivovaný hacking
- Druhá fáze - koordinované útoky prostřednictvím botnetů
- Ruská federace popírá zapojení
- Mládežnické hnutí Naši?

# Útoky na Estonsko – dopady

1. Vnímatelný efekt na fungování domácího hospodářství – útoky postihly sektory obchodu, služeb a státní správy, které spoléhají na ICT.
2. Společenský efekt ve formě narušení komunikace s veřejnou správou.
3. Narušení toku a výměny informací s okolním světem.
4. Vedlejší efekt filtrování dat jakožto prostředku na snižování dopadů útoku: tu a tam odfiltrovány i legitimní požadavky.

# Útoky na Estonsko – protiopatření I.

- Reakce koordinovány národním CERTem (CERT-EE), podpora systémovými administrátory a IT experty z Estonska i zahraničí
- Technická opatření zahrnovala:
  1. Navyšování kapacit infrastruktury (servery, přenosová rychlost)
  2. Filtrování příchozích dat a požadavků
  3. Omezení přístupu z vně země
  4. Instalace bezpečnostních aktualizací
  5. Použití systémů detekujících útoky
  6. „Lite" verze stránek
- Navázání mezinárodní spolupráce estonských expertů s okolním světem – konference TF-CSIRT (Praha) a RIPE (Tallinn)

# Útoky na Estonsko – protiopatření II.

- Oficiální mezinárodní kooperace organizovaná estonským ministerstvem obrany zahrnovala:
  1. Informování partnerů v rámci EU a NATO
  2. Pokus o invokaci článku 5 Washingtonské smlouvy
  3. Žádost o pozorování průběhu a případnou pomoc ve smyslu čl. 4 WS
  4. Pomoc od národních CERTů (USA, Německo, Finsko, Slovinsko) při lokalizaci původců útoku
- Public awareness kampaně a zpravodajství o proběhnuvších incidentech – zpráva, že Estonsko spolupracuje se zahraničními úřady na lokalizaci původců útoku a jejich stíhání snížila počet dobrovolně zapojených útočníků

# Konečné důsledky

- Těžko vyčíslitelné ekonomické škody (ušlé příležitosti, infrastruktura, přesčasy zaměstnanců, zpomalení projektů, přesměrování ruského obchodu)
- Dočasná omezení pro estonskou společnost
- Opakovaná dočasná přerušení chodu služeb státní správy, jakož i některých služeb poskytovaných soukromým sektorem
- Posunutí Estonska blíže do západních struktur (vybudováno NATO CCDCOE, Evropská agentura pro provozní řízení rozsáhlých informačních systémů
- Estonsko vnímáno jako expert na otázky kybernetické bezpečnosti

# Přisouzení útoků Rusku

- Někdy až přehnané reakce politiků, střídmější vyjádření IT expertů
- Logika cui bono?
- Útoky odpovídají ruským zájmům
- Vysledování IP adres
- Zapojení Kremlem sponzorovaného hnutí Naši
- Zapojeny servery, z nichž už ruské útoky probíhaly
- Koordinace a sofistikovanost offline i online protestů
- Útoky pravděpodobně naplánovány předem
- Neochota ruských úřadů spolupracovat při vyšetřování

# Útoky na Estonsko – závěr

- Kybernetické útoky jako nástroj zahraniční politiky a nátlaku?
- Nejasný původce, pravděpodobný však alespoň tichý souhlas vlády a bezpečnostních sborů Ruské federace
- Šedá zóna toho, co je ještě legální v kyberprostoru
- Estonský posun na Západ
- Vytváření a institucionalizace orgánů na zvládání tohoto typu hrozeb (NATO CCDCOE, EU-LISA, estonská CDU)
- Vzájemná podpora a růst spolupráce v oblasti kybernetické bezpečnosti

# Bělorusko 2008

- Třídenní kampaň DDoS útoků na Rádio Svobodná Evropa
- Postižena běloruská odnož rádia (www.svaboda.org) a 7 dalších webových stránek rádia ve střední a východní Evropě
- Rádio mělo zpravovat o demonstraci k výročí 22 let od černobylské jaderné nehody
- Dále útoky na nezávislé běloruské zpravodajské organizace (Charter 97; Belorusskiy Partizan)
- Pravděpodobným původcem či sponzorem běloruská vláda, případně politicky motivovaní jedinci/skupiny

# Litva 2008

# Litva 2008 – Historický kontext

- Velmi podobný historický vývoj vztahů s dnešním Ruskem jako Estonsko – od 18. stol. součást carského Ruska, krátká nezávislost, anexe SSSR, pod nadvládou Třetí říše 1941-44, poté v područí SSSR
- Nezávislost vyhlášena 11. března 1990, SSSR neuznává
- 13. leden 1991 incident u Vilniuské televizní věže – 14 mrtvých, stovky zraněných
- Nezávislost vzápětí umožněna rozpadem SSSR
- Od roku 2004 členem NATO i EU
- V rámci EU pravděpodobně nejostřejší rétorika vůči Rusku

# Litva 2008 – Politický kontext

- Ruská menšina v zemi nižší než v EE – 5,8 % populace
- Litva měla poměrně vyspělé služby, nepříliš dobrou úroveň kybernetické bezpečnosti (nízká míra koordinace, nedostatečná spolupráce mezi soukromým a veřejným sektorem, nedostatečná regulace bezpečnosti řízení informací)
- Bezprostřední příčinou útoků přijetí novely zákona o sdružování – zákaz použití nacistických a sovětských insignií na veřejných shromážděních
- Litevští Rusové v klidu, vokální reakce představitelů RF
- Dalšími tématy litevská nabídka na umístění protiletadlové základny či tvrdá pozice Litvy v rámci jednání EU-Rusko

# Litva 2008 - Útoky

- Předehrou útoků výrazná aktivita na ruskojazyčných webových fórech
- 28. červen 2008 – útoky na litevské weby, do 2. července 2008
- Intenzitou útoky nedosahují úrovně útoků na Estonsko 2007
- Drtivá většina cílů ze soukromého sektoru, vládní portály cíli pouze v 5 % případů (CERT-LT vydal varování, veřejná správa se připravila)
- Všechny cíle u jednoho webhostingového providera, útočníci zneužili známou bezpečnostní zranitelnost, která nebyla opravena
- Útok tak byl poměrně neselektivní, především defacementy webů a DDoS, spam e-mailů

# Gruzie 2008


RUSSIAN FEDERATION
GEORGIA
ABKHAZIA
SOUTH OSSETIA
NORTH OSSETIA
AJARA (AJARIA)
BLACK SEA
TURKEY
ARMENIA
AZERBAIJAN
Karachayevsk
Mozdok
Prokhladnyy
Nal'chik
El'brus 5642 m
Kodori Gorge
Roki Tunnel
Vladikavkaz
Gagra
Pskhu
Pitsunda
Gudauta
Novyy Afon
Sukhumi
Gulripsh
Ochamchira
Gali
Pichori
Anaklia
Lata
Otap
Omarishara
Mestia
Khaishi
Tqvarcheli
Jvari
Lentekhi
Tsalenjhikha
Zugdidi
Khobi
Senaki
Tskhaltubo
Poti
Samtredia
Lanchkhuti
Chokhatauri
Ozurgeti
Kobuleti
Batumi
Keda
Khulo
Bakhmaro
Abastumani
Atskuri
Akhaltsikhe
Vale
Khvanchkara
Ambrolauri
Tqibuli
Kutaisi
Chiatura
Zestaponi
Baghdati
Khashuri
Borjomi
Bakuriani
Akhalkalaki
Ninotsminda
Kvaisi
Tskhinvali
Mleta
Kurta
Pasanauri
Akhalgori
Dusheti
Archilo
Gori
Mtskheta
T'bilisi
Akhmeta
Qvareli
Telavi
Lagodekhi
Gurjaani
Balakän
Zaqatala
Tsnori
Rustavi
Marneuli
Bolnisi
Kazreti
Dedoplis Tsqaro
Agstafa
Vanadzor
Gyumri
Hrazdan
Sevan
Lake Sevan
Gäncä
Zod
Mingachevir Reservoir
Kür (Kura)
Mtkvari (Kura)
Alazani
Aragvi
Iori
Lake Tabatskuri
Lake Paravani
Rioni
Kodori
Inguri
Kuban'
Terek
Psou
Lake Ritsa
Bzyb'
Qvirila
Supsa
National capital
Autonomous republic capital
Town, village
Major airport
International boundary
Autonomous republic boundary
Main road
Secondary road
Railroad
0 25 50 75 km
0 25 50 mi
40°
41°
42°
43°
44°
45°
46°

# Historický kontext

- Gruzie do konce 18. stol. samostatná království, během první pol. 19. stol. postupně anektována Ruskem
- 26. května 1918 vyhlásila Gruzie nezávislost
- 1918-1920 „pod ochranou Britů“, 1921 dobyta Rudou armádou
- 9. duben 1991 Gruzie opět vyhlašuje nezávislost
- Převrat a občanská válka 1991-1995
- Výsledek: Abcházie a Jižní Osetie de facto nezávislé na Gruzii
- 2003: Růžová revoluce – svrhnutí prezidenta Ševardnadzeho, nástup Saakašviliho

# Politický kontext

- Problematický historický vztah s Ruskem, ekonomické sankce
- Ruská podpora separatistických území, ochrana ruských občanů
- Údajné gruzínské zapojení do druhé čečenské války
- Údajná gruzínská podpora čečenským teroristům a warlordům
- Údajná ruská bombardování gruzínského území
- Snaha Ruska udržet si vliv v příhraničních regionech a v tradičních sférách vlivu – vojenské cvičení Kavkaz v druhé polovině července 2008
- Snaha Gruzie zajistit si bezpečnost vstupem do NATO
- Ropovod Baku – Tbilisi – Ceyhan

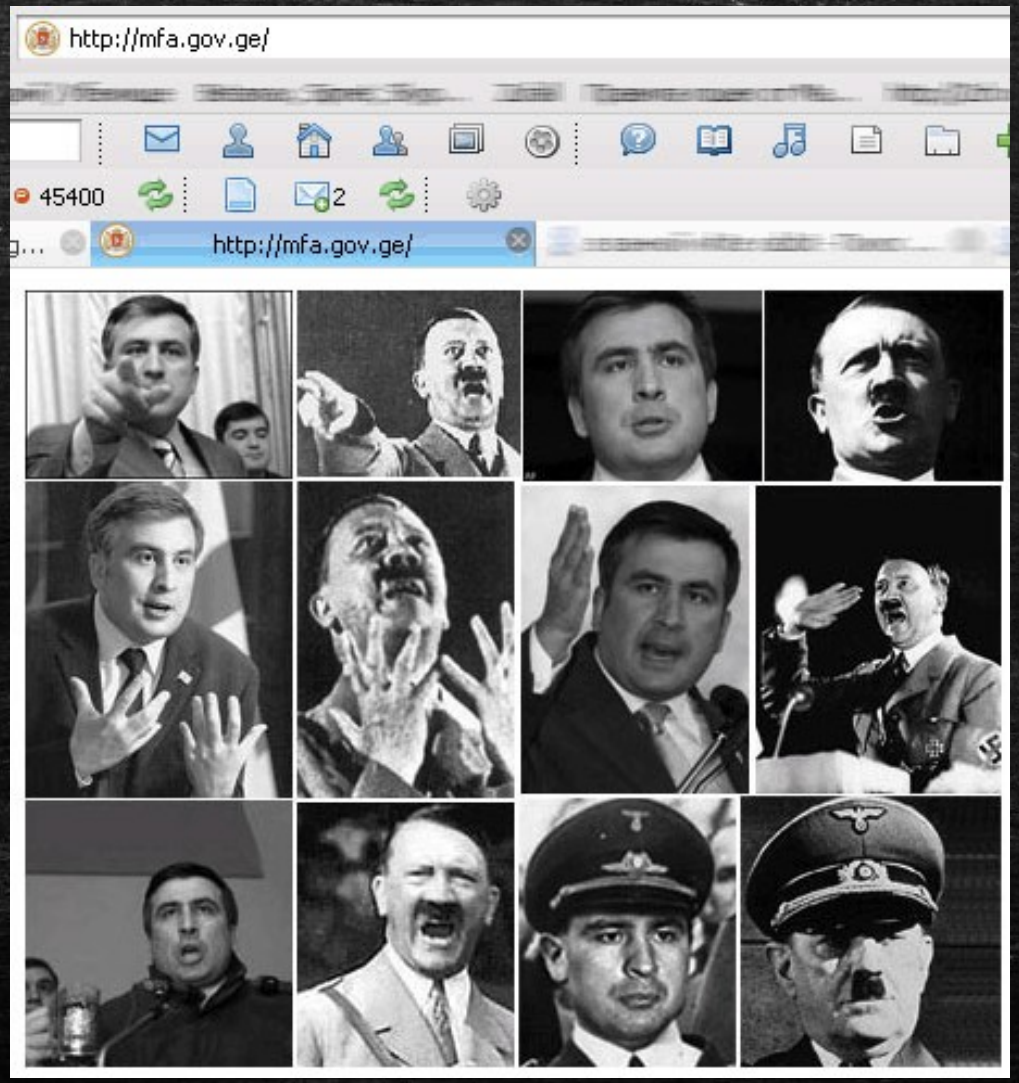
# Útoky na Gruzii 2008

- Předehrou několik případů útoků na gruzínské vojáky a dron, finální rozbuškou bylo údajné bombardování gruzínských vesnic separatisty z jižní Osetie
- Gruzínská armáda 7. srpna vstupuje do Jižní Osetie, Rusko 8. srpna odpovídá
- Gruzínci poraženi, 12. srpna podepsáno příměří
- Prakticky okamžitě po vstupu RF do konfliktu kybernetické útoky zaměřené na degradaci a znepřístupnění gruzínských komunikačních systémů
- Hlavním důsledkem neschopnost gruzínské vlády komunikovat po internetu se svou populací a okolním světem, narušení morálky?

# Předpřipravená kampaň?

- Testovací útoky už 19. července
- Předpřipravené seznamy cílů a návody, jak se do kampaně zapojit
- Součinnost s kinetickou kampaní, adaptace cílů podle potřeby
- Použity DDoS, SQL Injection, cross-site scripting, e-mail spam a defacement
- Útoky na weby institucí, zpravodajské organizace, bankovní sektor (kromě ztráty kontaktů se zahraničními bankami např. problém s přístupem k penězům).
- Informační kampaň – comment spam a voting spam na webech světových zpravodajských organizací (CNN apod.)

# Příklad defacementu



# Protiopatření

- Protiopatření koordinována CERTem z gruzínského akademického sektoru
- Státem schválené odmítnutí přístupu na a z ruských adres
- Přesměrování služeb do zahraničí:
  1. Pomoc od jednotlivců i organizací (Gruzínec v USA, Google)
  2. Pomoc Polska a Estonska

- Omezené pokusy gruzínských hackerů odpovědět – útok na RIA Novosti či podvržený DDoS tool

# Přisouzení útoků

- Původ útoků na webových fórech StopGeorgia.ru, hacker.ru, stopgeorgia.info.

- FSB
- Ruští patriotičtí hackeři
- Ruský organizovaný zločin (RBN?)

- Zapojení dalších dobrovolníků – ruští patriotičtí hackeři či sympatizanti z Ukrajiny a Lotyšska?

# Kyrgyzstán 2009

# Kyrgyzstán 2009

- Země přímo nesousedící s dnešním Ruskem
- Součást carského Ruska od 1876
- Poté pod SSSR, nezávislost 31. srpna 1991, nadále spojencem RF
- Početné menšiny Uzbeků a Rusů – etnické nepokoje, emigrace
- Problematičtí lídři (Akajev, Bakijev)
- Soupeření o vliv – USA vs. Rusko
- Americká letecká základna v Manasu
- Otázka prodloužení nájmu (2005, 2009)

# Kyrgyzstán 2009 - ICT

- V zemi 4 provideři internetu
- Celková penetrace internetu v rámci populace: 17 %
- Relativně nízká úroveň rozvoje – křehká infrastruktura
- Ohrožení i malého množství subjektů tak může být kritické

# Kyrgyzstán 2009 - Útoky

- Počátkem 18. leden 2009, doba trvání: 2 týdny
- Útoky právě na ISPs. Zasaženi dva nebo tři?
- Masivní DDoS útok, zásadní omezení možnosti připojení na internet, omezené narušení fungování mobilních telefonních služeb
- Politický efekt na kyrgyzskou opozici – vláda internet takřka nepoužívala
- Omezený ekonomický efekt – v Kyrgyzstánu internet využíván spíše sporadicky
- Smlouva s USA nakonec prodloužena až do r. 2014

# Kyrgyzstán 2009 – Přisouzení útoků

- Drtivá většina IP adres pocházela z Ruské federace
- Nulové zapojení dobrovolníků do útoků
- Pravděpodobně botnety patřící Russian Bussiness Network
- Pravděpodobné předpřipravení útoku

- 2 možné scénáře:
  1. Ruský nátlak na kyrgyzskou vládu, aby USA neprodloužila nájem základny.
  2. Útok na opozici objednaný vládou prezidenta Bakijeva.

# Otázky?

Díky za pozornost.