SOUČASNÉ TRENDY A AKTÉŘI V KONTEXTU KYBERNETICKÉ BEZPEČNOSTI: KYBERTERORISMUS

Roman Pačka
Národní centrum kybernetické bezpečnosti

Globální posun ve vnímání kybernetických hrozeb I.

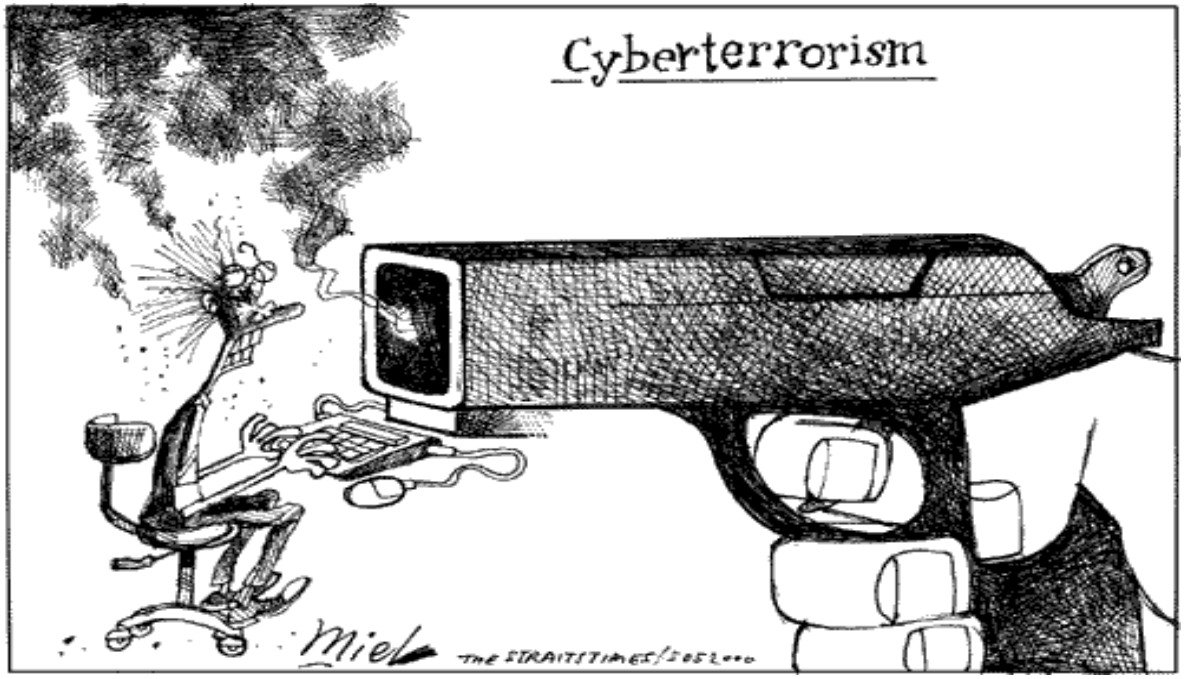
- Závěry **NATO** summitu ve Walesu (2014): kybernetické útoky mohou aktivovat článek 5 Washingtonské smlouvy o kolektivní obraně
- **EU**: finalizace návrhu směrnice NIS, která zavede minimální úroveň zabezpečení digitálních technologií, sítí a služeb v členských státech. Jedná se o historicky první závazný právní předpis členským státům týkající se kybernetické bezpečnosti
- **OBSE** (2013): přijata 1. sada opatření pro zvyšování důvěry mezi státy v kyberprostoru (CBMs), práce na 2. sadě probíhají

Globální posun ve vnímání kybernetických hrozeb II.

- **Hack společnosti SONY jako precedens** (2014): 1. kybernetický útok, který byl (ze strany liberálně demokratické země) otevřeně politicky přisouzen vládě cizího státu, dle Spojených států narušil jak státní suverenitu, tak i porušil mezinárodní právo
  → uvaleny sankce na Severní Koreu

KYBERTERORISMUS

- Podmnožinou terorismu (kyberprostor+terorismus)
- Široké vs. úzké pojetí
- Znaky: užití/zneužití ICT, násilí, škody, publicita, strach, politické/náboženské cíle



Kyberterorismus jako hypotetický fenomén? I.

- D. Denning (2011): *Útoky ještě nedosáhly takové úrovně, aby mohly být nazvány kyberterorismem. Žádný dosavadní útok nedosáhl dostatečné intenzity, rozsahu škod a obětí na životech, aby vskutku generoval strach srovnatelný například s bombovými teroristickými útoky.*
- J. Drmola (2013): *„obrovské množství elektronických aktivit, které je rutinně označováno jako kyberterorismus, nemá s terorismem prakticky vůbec nic společného“*
- 2015?

Kyberterorismus jako hypotetický fenomén? II.

Drmola (2013) vs. současnost

1. ty nejcitlivější systémy nejsou vůbec k internetu připojeny a jsou zabezpečeny pomocí tzv. air-gap a útok by tak obvykle vyžadoval fyzickou přítomnost,
2. sofistikované útoky na průmyslová nebo vojenská zařízení vyžadují detailní přehled o cílovém systému, dlouhou a náročnou přípravu a velmi pokročilé znalosti z oboru
3. elektronické útoky pro „tradiční teroristy“ postrádají silný dramatický a symbolický efekt, kterého mohou dosáhnout pomocí výbušnin a excesivního násilí,
4. elektronické útoky vyžadují informační infrastrukturu, kterou rozvojové země (obzvláště mimo města) často postrádají,
5. „subkultura hackerů“ obvykle nemá zájem, odhodlání a potřebný ideologický zápal se do těchto rozsáhlých útoků pouštět.

Historie kyberterorismu (?)

- od 1980s – Zvýšený zájem o kyberterorismus
- 2000 – Strach z Millennium bugů
- 2001 – CIA objevila Al-Kaida modely vodních přehrad spolu se software, který simuloval jejich katastrofická selhání
- 2004 – hack počítačů, které kontrolovaly životní systémy na výzkumné stanici v Antarktidě
- 2004 – Maroochy Shire , Queensland – hack čističky odpadních vod
- 2007 – Estonské kybernetické útoky jako kyberterorismus?
- …

ISIS: Základní přehled

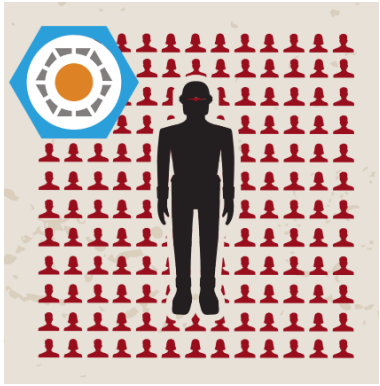
- ISIS jako stát (6,5 mil obyvatel; 300 000 km^2 – vlastní území, finanční soběstačnost)
- Srovnání: Al-Qaeda vs. ISIS („hit and run“ vs. „grab land, consolidate and expand“)

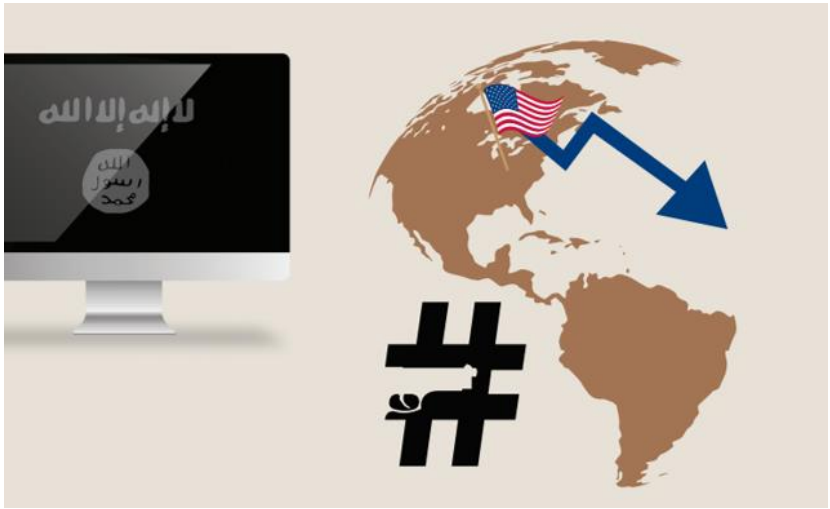
  → Zcela odlišné, unikátní pojetí teroristického boje
- Digitální identita a využívání ICT důležitou součástí – PARADOX?
- První významná džihádistická organizace, která hojně využívá potenciál internetu

ISIS: Marketing terror I.

- Tisíce účtů na Twitteru, Facebook, atd.
- Přes 94 000 tweetů každý den (posun od Al-Kaidy)
- Hijacking Twitter storms
- „Propagande par le fait“
- Radikalizace skrze App? (Dawn of Glad Tidings)

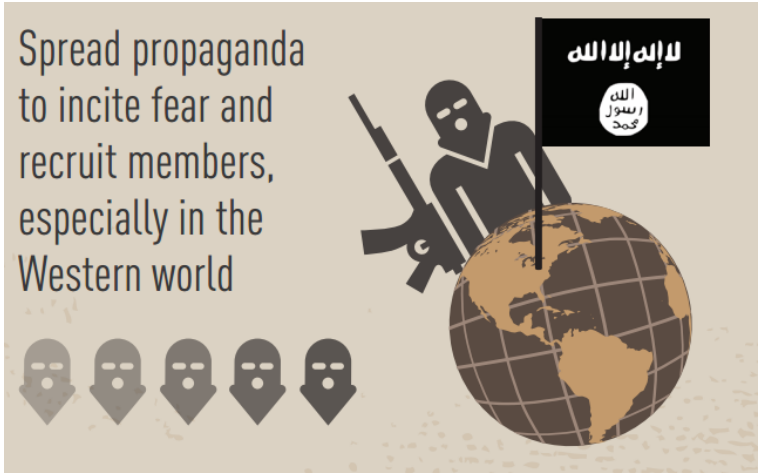
  = Social bot armies
- → Přehlcení zpravodajských služeb i občanů informacemi





ISIS: Marketing terror II.

- Network hopping
- Specialisté na PR a IT – dobrá komunikační strategie, publikování sofistikovaných/profesionálních filmů, dokumentů a videí v HD
- ISIS brand – Prezentace jako „stabilní stát“ (srov. Irák, Libye, Jemen, Sýrie, či Egypt)



ISIS: Kyberkalifát

- Vytvořeno na podzim roku 2014
- Leden 2015 – vyhlášení kyberválky USA
  + hack Pentagonu (CentCom)
- Velmi aktivní na sociálních sítích – na Twitteru 110 000 followers
- Struktura skupiny neznámá, známý pouze velitel Junaid Hussain (†26.srpna 2015, Rakka)


CyberCaliphate
you isis
CyberCaliphate
i love you isis
TWEETS 3,671
FOLLOWING 1,268
FOLLOWERS 109K
FAVORITES 30
Follow
U.S. Central Command
@CENTCOM
Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.
MacDill AFB, Tampa, FL
centcom.mil
Joined March 2009
Tweet to U.S. Central Com...
Tweets
Tweets & replies
Photos & videos
U.S. Central Command @CENTCOM · 4m
AMERICAN SOLDIERS,
WE ARE COMING, WATCH YOUR BACK. ISIS.
#CyberCaliphate
13
1
U.S. Central Command retweeted
CJTF-OIR @CJTFOIR · Jan 7

ISIS – Vybrané kybernetické útoky

- Kybernetické útoky na twitter a youtube účet Pentagonu – odcizení a zveřejnění osobních dat amerických vojáků skrze kyberprostor a podněcování násilí proti příslušníkům americké armády v USA
- DoS/DDoS a defacement francouzských webových stránek (od turismu po MoD)
- Kybernetické útoky na francouzskou televizní stanici TV5MONDE (přerušení TV vysílání, napadeny sociální sítě a webové stránky)
- Odcizení informací z emailových účtů řady členů britské vlády včetně ministryně vnitra Theresy May k zosnování atentátu
- Pokusy hackovat energetické společnosti v USA

Junaid Hussain: první kyberterorista? I.

- 21-letý kybernetický emír
  Abu Hussain al-Britani
- 2012 v Británii odsouzen k šesti měsícům vězení za kybernetickou krádež
  a zveřejnění adresáře Tonyho Blaira
- Byl součástí hackerské skupiny
  Team Poison (TeaMp0isoN)
- 2012: *"Terorismus neexistuje.*
  Je vykonstruován pouze k tomu, aby démonizoval určitou víru."
- 2013 z neznámých důvodů silná radikalizace a útěku do Sýrie, kde se připojil k bojovníkům ISIS → díky svým počítačovým schopnostem se zanedlouho ujal vedení kyberchalifátu
- Zemřel při dronovém útoku spojenců (†26. srpna 2015, Rakka, Sýrie)

Junaid Hussain: první kyberterorista? II.

- Vylepšil ochranu komunikace ISIS na internetu tak, že ji zpravodajské služby nemohly tak snadno sledovat
- Navyšoval digitální hygienu mudžáhidů – určoval pravidla, jak se bezpečně pohybovat v kyberprostoru
- Vytvářel také malware a učil ostatní členy IS, jak podobné penetrační nástroje používat.
- Byl významnou osobností na sociálních sítích, podněcoval násilí proti obyvatelstvu a propagoval ISIS/rekrutoval bojovníky

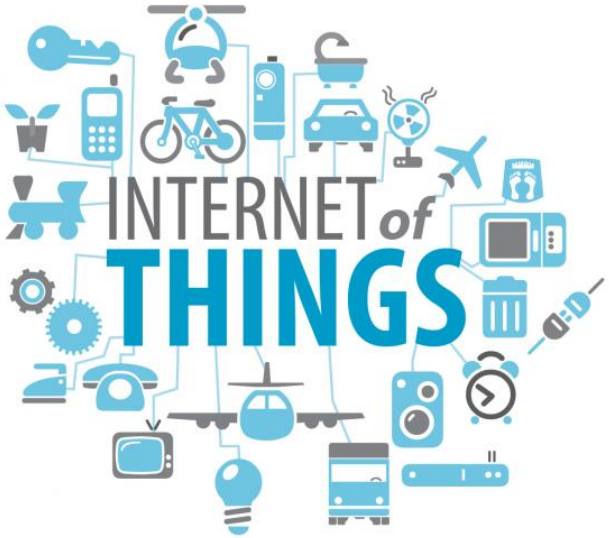
Junaid Hussain: první kyberterorista? III.

- Kyberteroristou nebyl, avšak usiloval o tento status
- Pod jeho vedením kyberkalífát podnikl mnoho úspěšných kybernetických útoků, které ostatní teroristické skupiny nebyly dlouhá léta vůbec schopny uskutečnit
- Určoval digitální identitu a vylepšil kybernetickou bezpečnost ISIS
- Pro spojence představoval natolik významnou hrozbu, že se přistoupilo k jeho eliminaci
- Usmrcení bojovníka zabývajícího se pouze hackingem a internetovou propagandou by mohlo představovat důležitý precedens
- ISIS jeho smrtí utrpěl těžkou ztrátu (?)

Listopad 2015: Hack 54 000 twitter účtů + zveřejnění osobních údajů velitelů CIA, FBI a NSA

CÍLE KYBERTERORISMU ?

- Vojenská technika
- ICS/SCADA
- IoT



Vybrané případy: Hack protiraketového systému Patriot

- Objevena a využita zranitelnost v německém protiraketovém systému Patriot na turecko-syrských hranicích (2015)
- Vojenská baterie obdržela z neznámého zahraničního zdroje určité příkazy
- Spekulovalo se, zdali nedošlo i k výstřelu, což bylo záhy vojenským vedením popřeno
- Závěry:
  - ICT ve stále větší míře pronikají do systémů, sítí i samotné techniky obranných složek státu
  - Do budoucna nelze vyloučit vypálení rakety/zneužití vojenské techniky
  - Možný terč kyberteroristických útoků

Vybrané případy: Stuxnet a Německá ocelárna I.

Stuxnet (2009)

- Nejznámější virus, který útočil na systémy SCADA
- Jeho použití mělo fyzický dopad na zařízení laboratoře na obohacování uranu
- Zpomalil o několik let íránský jaderný program

Německá ocelárna (2014)

- Kybernetický útok na ocelárnu v Německu.
- Hackeři znemožnili obsluze ocelárny vypnout jednu z vysokých pecí a tím jí vážně poškodili
- Do kontrolního průmyslového systému ocelárny se útočníci dostali skrze selhání lidského faktoru, metodou tzv. sociálního inženýrství

Vybrané případy: Stuxnet a Německá ocelárna II.

Závěry:

- ICS / SCADA – kritická zařízení pro odvětví jako jsou výroba, energie, voda, doprava, apod.
- Kvůli komplexnosti a různorodosti technologického řešení ICS /SCADA jsou oproti ostatním ICT zařízením typicky min. 10 let pozadu v řešení zabezpečení proti kybernetickým útokům
  = nízká míra zabezpečení
  + vysoká zranitelnost
  + závažné následky při selhání
- Hrozí např. ekologické katastrofy, dopravní kolaps a dokonce i ztráty na životech

Vybrané případy: Miller a Valasek I.

Miller a Valasek – Jeep Cherokee (2015)

- Hackeři Miller a Valasek na dálku ve 100km/h rychlosti ovládli přes multimediální systém Uconnect automobil Jeep Cherokee i s řidičem
- Postupně převzali plnou kontrolu nad stěrači, rádiem, klimatizací a nakonec i brzdami a motorem – s autem pak sjeli demonstrativně do příkopu
- V Americe bylo svoláno do servisů 1,4 milionu aut k úpravě softwaru systému Uconnect

Vybrané případy: Miller a Valasek II.

- Jeep Cherokee však není výjimkou
- V návaznosti na tuto událost server DailyDot.com uveřejnil žebříček 5 nejsnadněji napadnutelných automobilů:
  1. Jeep Cherokee (2014) – veškeré systémy
  2. Cadillac Escalade (2015) – wifi / bluetooth / bezdrát.klíč
  3. Infiniti Q50 (2014) – rádio / Infinity Connect systems / Bluetooth
  4. **Toyota Prius** (2010 a 2014) – radio / Bluetooth
  5. **Ford Fusion** (2014) - wifi / bluetooth / radio / Ford SYNC systems

ISIS a kyberterorismus

- UK: "They do not yet have that capability. But we know they want it, and are doing their best to build it.„
- „…hypothetical catastrophic examples of IS gaining control of air traffic control are still well out of the terrorist's reach - it's not beyond imagination and certainly not beyond theirs."
- FBI: „IS has a strong intent. Thankfully, low capability … But the concern is that they'll buy that capability."
- Berger: „They have not yet been extremely visible carrying out more sophisticated activities such as high-level cybercrime or more destructive attacks, but I suspect this is just a matter of time "

KYBERTERORISMUS: Shrnutí I.

- Teroristé v kyberprostoru zažívají v poslední době nebývalý rozmach. Roste počet kybernetických útoků i jejich intenzita.
- Narůstá i profesionalita teroristů a schopnosti působit v kyberprostoru
  → Teroristické útoky v Paříži byly umožněny i kvůli silné kryptografické ochraně komunikace v kyberprostoru, kterou se teroristé naučili používat
- Zvýšená závislost společnosti/lidí na ICT a kyberprostoru a zvýšená kritičnost selhání
  → narůstá počet možných cílů kyberterorismu i šance na úspěch

KYBERTERORISMUS: Shrnutí II.

- ISIS se jeví jako jediná schopná/ochotná teroristická organizace do kyberteroristických útoků investovat a provádět je
- ISIS se profiluje jako elitní hackerská organizace
  → realita je jiná, ISIS používá kyberprostor především k propagandě, radikalizaci a plánování operací
- K provedení sofistikovaných útoků je potřeba značných investic
  → prioritou stále zůstává konvenční boj

http://www.liveleak.com/view?i=01f_1431632527

Děkuji za pozornost!

Roman Pačka

r.packa@nbu.cz

www.nbu.cz

www.govcert.cz