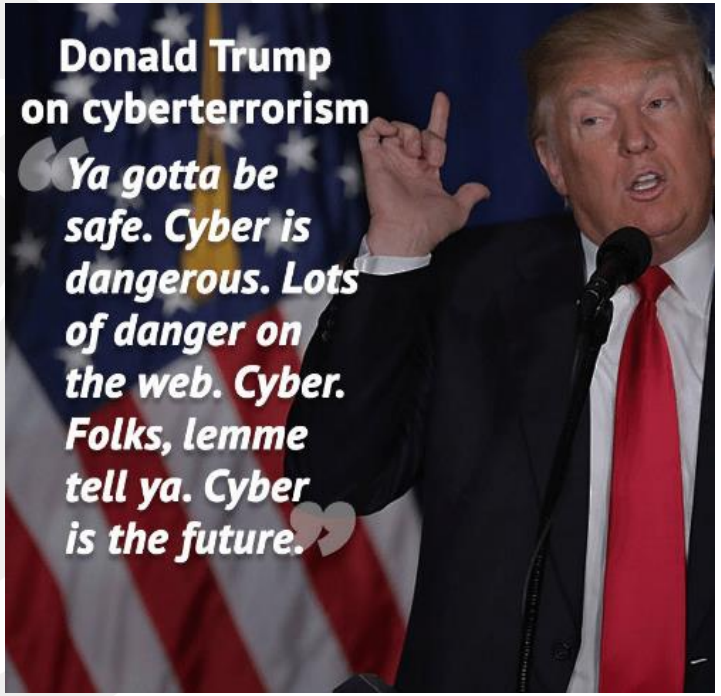
Daeš a kyberterorismus: No need to panic. Yet.

Michaela Semecká
Oddělení strategických informací a analýz

NÚKIB

Kyberterorismus

- Neexistuje shoda o tom, co to kyberterorismus je
- Co organizace, to definice kyberterorismu



Kyberterorismus

- CO
- ZÁMĚR
- JAK
- KDO

Kyberterorismus

Audit národní bezpečnosti ČR

„Kyberterorismus zahrnuje agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, a jehož prostřednictvím je dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy.“

FBI

“Premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.”

Kyberterorismus

Teroristický útok podle českého trestního zákoníku

- (1) Kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla,

E. vložením dat do počítačového systému nebo na nosič informací anebo vymazáním nebo jiným zničením, poškozením, změněním nebo potlačením dat uložených v počítačovém systému nebo na nosiči informací, snížením jejich kvality nebo učiněním jich neupotřebitelnými provede útok proti počítačovému systému, jehož narušení by mělo závažný dopad na fungování státu, zdraví osob, bezpečnost, hospodářství nebo zajištění základních životních potřeb obyvatel, útok s dopadem na větší počet počítačových systémů s využitím počítačového programu vytvořeného nebo přizpůsobeného pro takový útok anebo útok, kterým způsobí značnou škodu, bude potrestán odnětím svobody na tři až dvanáct let, popřípadě vedle tohoto trestu též propadnutím majetku

Kyberterorismus?

Stuxnet

Kyberterorismus?

Kybernetické útoky na Estonsko v roce 2007

Prohlášení estonského ministerstva obrany:

„Kybernetické útoky proti Estonsku byly skutečnými akty kybernetického boje a **kybernetického terorismu**, jež nemají na svědomí amatérské skupiny disponující omezenými zdroji, nýbrž velmi schopní specialisté na kybernetické útoky s velmi účinnými prostředky k boji.“

NÚKIB

Kyberterorismus?

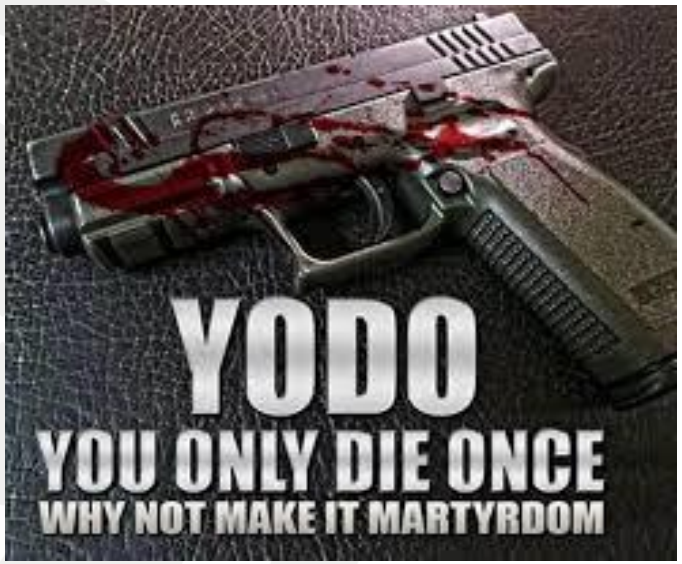
Jeep Cherokee hack
(Miller a Valasek)

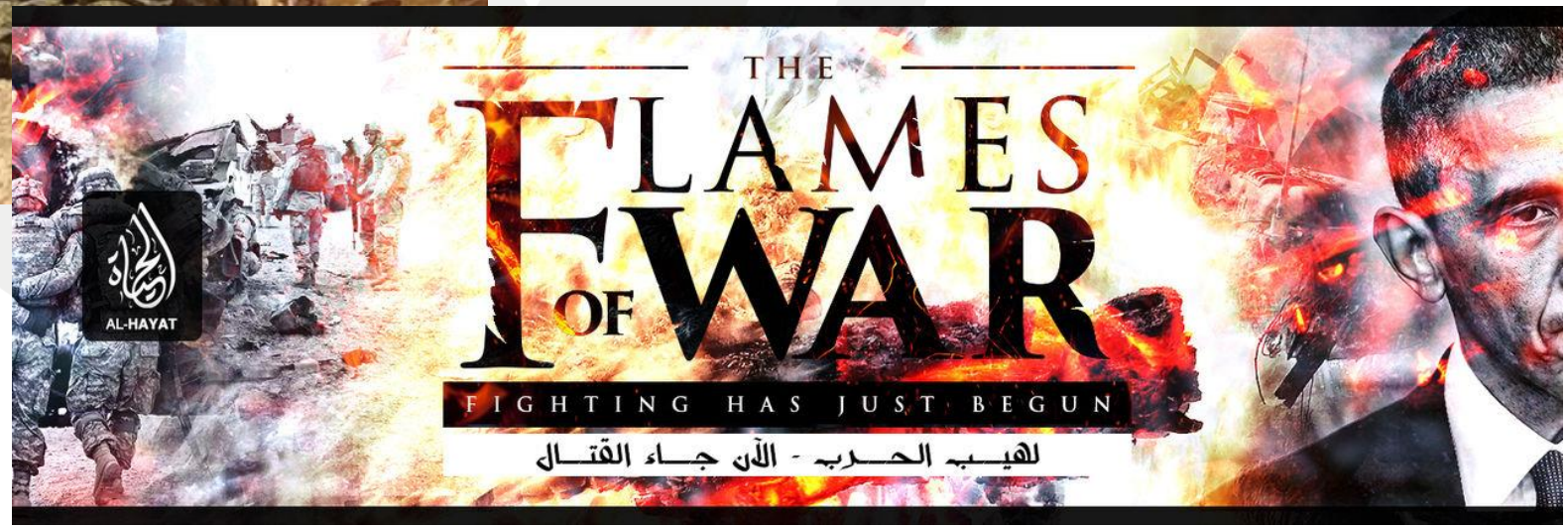
Kyberterorismus?

Tariq ad-Daour

- Kybernetická krádež peněz za účelem financování operací Al-Qaedy

Kyberterorismus?





Kyberterorismus!

NÚKIB

Hrozba kyberterorismu

Kyberterorismus jako skutečná hrozba

X

Kyberterorismus jako zveličená hrozba

Kyberterorismus – empirický výzkum

Max Kilger (University of Texas at San Antonio)

- Výzkum, kterého se účastnilo 1099 studentů ze Spojených Států, Taiwanu a JAR
- Fiktivní scénář: Země Bagarie nedávno přijala kroky a podnikla fyzické akce, které mají pro vaši vlast negativní dopady a výrazně ztěžují život jejím obyvatelům. Jak se zachováte?
- Dva možné scénáře odpovědi – fyzické a kybernetické

Kyberterorismus – empirický výzkum

Možnosti fyzických akcích:

- Do nothing - let your country work it out on its own
- Write a letter to government of Bagaria protesting their actions
- Participate in a protest at an anti-Bagaria rally
- Travel to Bagaria and protest at their country's capitol building
- Travel to Bagaria and confront a Bagarian senior government official about their policies
- Travel to Bagaria and sneak into a military base to write slogans on buildings and vehicles
- Travel to Bagaria and physically damage an electrical power substation
- Travel to Bagaria and damage a government building with an explosive device

Kyberterorismus – empirický výzkum

Kybernetické možnosti:

- Do nothing - let your country work it out on its own
- Post a comment on a social networking website like Facebook or Twitter that criticizes the Bagarian government
- Deface the personal website of an important Bagarian government official
- Deface an important official Bagarian government website
- Compromise the server of a Bagarian bank and withdraw money to give to the victims of their policies and actions
- Search Bagarian government servers for secret papers that you might be able to use to embarrass the Bagarian government
- Compromise one or more Bagarian military servers and make changes that might temporarily affect their military readiness
- Compromise one of Bagaria's regional power grids which results in a temporary power blackout in parts of Bagaria
- Compromise a nuclear power plant system that results in a small release of radioactivity in Bagaria

Kyberterorismus – empirický výzkum

Výsledek:

→ 1-2% si vybralo nejradikálnější kybernetickou možnost

→ větší procento než u nejradikálnější fyzické možnosti

→ cesta ke kyberterorismu jednoduší než ke klasickému terorismu


لا إله إلا الله
محمد رسول الله

Daeš: Kybernetické kapacity

- Daeš má minimální ofenzivní kybernetické kapacity
- Útoky spojované s Daeš jsou připisovány hackerským skupinám, které Daeš jednostranně podporují

Daeš: Modus operandi

Navzdory relativně vysokému počtu hackerských skupin podporujících Daeš je jejich modus operandi podobný:

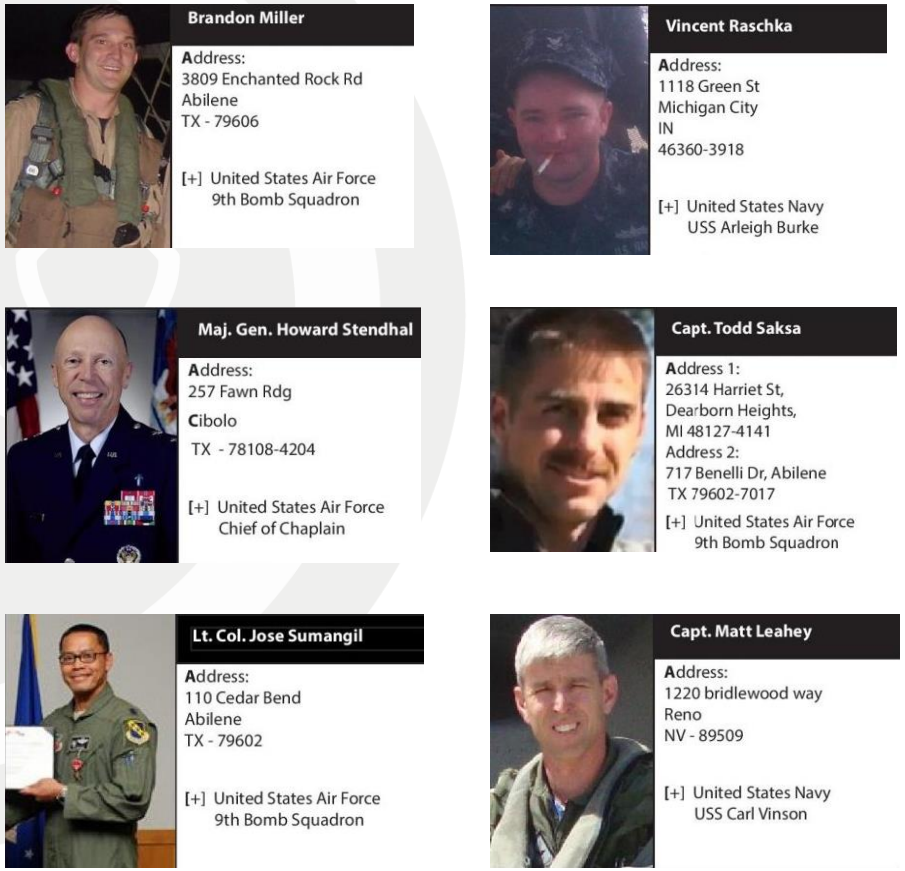
- Zveřejňování kill listů
- Defacementy
- Prolomení účtů na sociálních sítí

Daeš: Kill listy

- Jeden z hlavních nástrojů
- Dosud byly řádově zveřejněny desítky kill listů se jmény desítek tisíc jednotlivců
- Cílí na vyvolání strachu

„O Crusaders, …. we are in your emails and social accounts, we are extracting confidential data and passing on your personal information to the soldiers of the Khalifah, who soon, with the permission of Allah, will strike at your necks in your own lands! So wait; we too are waiting!"

Islamic State Hacking Division kill list



Zdroj: Xebercom

NÚKIB

Daeš: Defacementy

- Podle zprávy FBI napadené webové stránky měly stejnou zranitelnost (WordPress)
- Indiskriminace pravděpodobnější než cílení na konkrétní stránky

Daeš: Prolomení účtů na sociálních sítích

Prolomení oficiálních účtů US CENTCOM

- Leden 2015
- Twitter a YouTube
- Mluvčí US CENTCOM označil incident za „kybervandalismus“

Kybernetické a teroristické organizace: Korelace?

- Aktivita hackerských skupin se výrazně nezvyšuje v období okolo teroristických útoků
- Země, které jsou častým cílem teroristických útoků, výrazně nevyčnívají ze seznamu cílů

Daeš: Členové hackerských skupin

- Většina nezkušených kluků
- Jejich identity lze dohledat pomocí OSINT nástrojů

Daeš: Členové hackerských skupin

Pár technicky zdatných členů

Junaid Hussein (Abú Husajn al-Britání)

- Hlava Kybernetického chalífátu
- Prolomil email osobní asistentky T. Blaira
- Navyšoval digitální hygienu mudžahidinů
- Vytvářel malware a učil ho používat ostatní

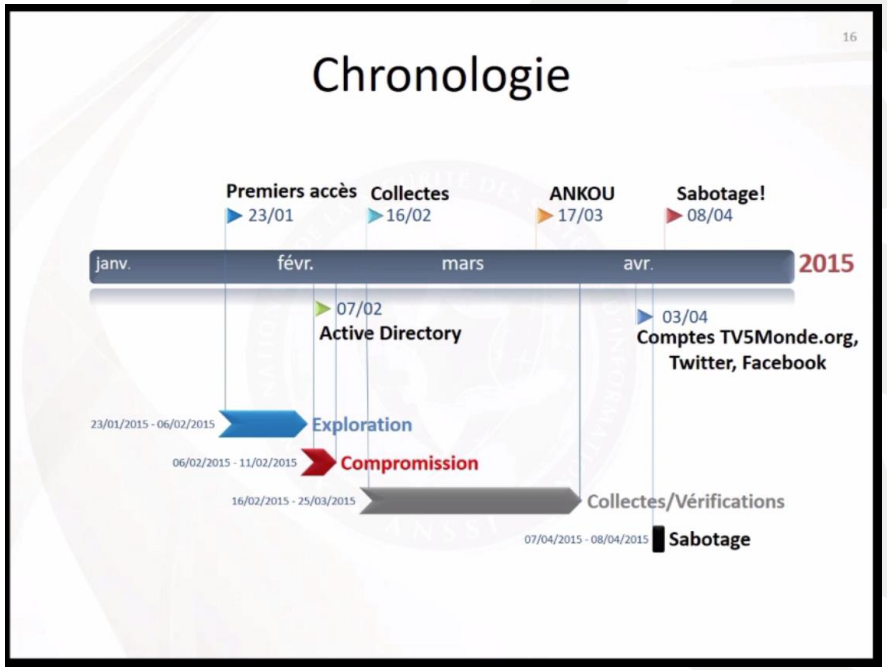
Ardit Ferizi

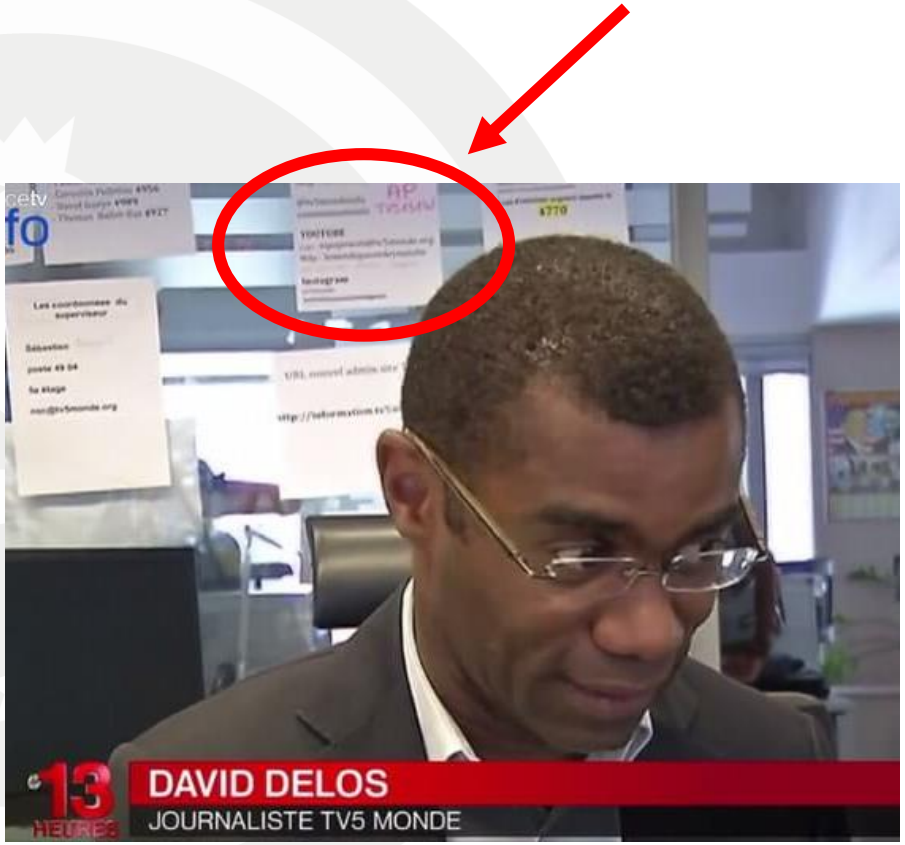
- Kosovský hacker
- Prolomil systémy amerického vládního kontraktora
- Prodal osobní informace 1000 amerických vojáků Junaidu Husseinovi

Daeš: False-flag operace

- Výhružky manželkám amerických vojáků pod hlavičkou Kybernetického chalífátu
- Únor 2015
- Stopy z vyšetřování vedou k ruské APT 28

Daeš: False-flag operace





NÚKIB

Daeš: Budoucí trendy pro KT

Konvenční terorismus bude pravděpodobně méně nákladný a bude teroristům přinášet více užitku

Několik aspektů, které mohou teroristy odradit od investování do vývoje prostředků pro KT:

- Nedostatek dramatického efektu
- Nedostatek pozornosti médií
- Časová náročnost
- Finanční náročnost

Hacktivismus

Hacktivismus

- Sloučení hackování a aktivismu
- Útoky motivované politickou, ideologickou nebo sociální změnou
- Na rozdíl od kyberterorismu nezpůsobuje velkou škodu

Hacktivismus x Aktivismus

- Normální využití internetu, jako např. vyvěšování materiálů na webových stránkách, diskuze na fórech, atd.

Hacktivismus x Kyberterorismus

Hacktivismus

- Anonymní hnutí bez vedení a struktury
- Vzniklo v roce 2003
- Pohybuje se na pomezí single-issue aktivismu a anarchismu
- Nejčastější metody: DDoS, defacement, nabourávání se do účtů na sociálních sítích

Hacktivismus: Anonymous a Los Zetas

- Člen Anonymous v roce 2011 unesen Los Zetas
- Hnutí hrozilo doxingem v případě, že ho nepropustí
- Člen Anonymous byl propuštěn, ale #OpCartel skončila kvůli strachu z násilí ze strany Los Zetas

Hacktivismus: Česká odnož Anonymous

Česká odnož Anonymous aktivní od roku 2012

- DDoS na webové stránky OSA
- Prolomení databází ODS a zveřejnění osobních údajů jejích členů

Po několika letech nečinnosti začalo hnutí ožívat v roce 2016

- #OpBlokáda

NÚKIB

Hacktivismus v ČR

NÚKIB

@

m.semecka@nukib.cz

NÚKIB