Nestátní aktéři Kybernetických konfliktů

Tomáš Maďar
t.madar@mail.muni.cz

Historie

- Počátek v 2. pol. 20. stol.
- Boom především v druhé polovině nultých let
- Dnes v téměř každém konfliktu s kybernetickou dimenzí
- Počet útoků vs. informovanost
- Ve stínu státem sponzorovaných útoků?

Typologie

- Kybernetické milice a patriotičtí hackeři
- Kybernetičtí zločinci
- Hacktivisté a online aktivisté
- Kybernetický terorismus
- Advanced Persistent Threats

Kybernetické milice I.

- Problém s konceptualizací
- Milice tradičně spjaty s teritoriem
- Pernica (2007): Milice definovány jako "organizační prvky ozbrojených sil složené z neprofesionálních vojáků vykonávajících vojenské činnosti dobrovolně nebo na základě donucení."
- Milice někdy také obecně ztotožňovány s paramilitarismem (Mareš 2012)

Kybernetické milice II.

- Jak definovat kybernetické milice?
- Přesah definičních znaků s dalšími nestátními aktéry (terorismus, org. zločin, hacktivismus)
- Dobrovolnický základ, ne vojáci z povolání
- Politicky motivované útoky či obrana systémů a sítí
- Organizace a chain of command (?), odpovědnost (?)
- Rain Ottis (2010): "farmáři s vidlemi" - obecně spíše méně sofistikované útoky

Ofenzivní aktivity kybernetických milic

- Mexiko 1998 - Zapatova armáda nár. osvobození
- Indie a Pákistán, Izrael et al.
- Fenomén Čína - koncept lidové války
- Ruské milice v období 2007-2009
- Írán a Sýrie

Defenzivní kybernetické milice?

- Estonsko 2007
- "Saunová diplomacie"
- Küberkaitseliit
- Zvažováno či navrhováno kupř. také ve Velké Británii (rezervisté) či Japonsku

Case study - Küberkaitseliit

- Vznik následkem útoků na jaře 2007
- Součást Estonian Defense League (Kaitseliit)
- Dobrovolně sdružení estonští IT specialisti
- Podpůrné schopnosti v případě vzniku krize
- Podpora public-private partnerships
- Vzdělávání, awareness, předcházení incidentům

Kybernetický zločin

- V kontextu zapojení do kybernetických konfliktů především Rusko a Čína
- Gruzínská válka 2008
- Russian Business Network a čínská průmyslová špionáž
- Ambivalentní postoj Ruska a Číny ke kybernetickým úmluvám

Case study - Nexus vláda-kybernetický zločin v Rusku

- Východiska kyb. zločinu po rozpadu SSSR:
- 1. Mocenské vakuum
- 2. Slabý trestní řád a nedostatečná kvalifikace strážců zákona
- 3. Kvalitní technické obory
- 4. Nezaměstnanost a nízké platy mladých IT odborníků
- 5. Existující podhoubí organizovaného zločinu

Case study - Nexus vláda-kybernetický zločin v Rusku

- Do poloviny nultých let - etablování se jednotlivých aktérů, pronikání tradičních struktur do kyberzločinu
- Protekce za laskavosti a podíl na zisku?
- Gruzínská válka 2008
- Vztahy s polotiky či FSB?
- Parlamentní volby 2011 a prezidentské volby 2012
- Hacking as a Service (HaaS)

Hacktivismus

- Aktivistická uskupení podnikající politicky motivované kybernetické útoky s cílem naplnit svoji agendu
- Počátky v 90. letech, někdy chybně označováno za kybernetický terorismus
- Kořeny v hackerské kultuře a etice
- Cíle: svoboda slova, lidskoprávní tématika, svobodný přístup k informacím, různá single-issues, "the lulz"
- Ale také regionální politické cíle: Palestina, Írán, Arabské jaro

Case study - Anonymous I.

- Vznik 2003 - 4chan
- Proslulost od 2008 - Project Chanology
- Operace Payback is a Bitch, Avenge Assange, útok na HBGary
- Útoky na vládní agentury (USA, Izrael, další), vybrané církve (scientologové, Westboro), korporace PayPal, Visa, Sony, MasterCard)
- Podpora WikiLeaks a hnutí #Occupy
- Útoky na osoby šířící dětskou pornografii - Op Darknet

Case study - Anonymous II.

- Úpadek hacktivismu?
- Roztříštěnost
- Množství projektů všude po světě
- Klesající efekt a dopad

Kybernetický terorismus

- "Terorismus je použití agresivního a excesivního násilí (anebo hrozba použitím takového násilí), které je naplánováno s dominantním účelem vyslat vážné zastrašující poselství zřetelně většímu počtu lidí (cílovému publiku)1 než pouze těm, kteří jsou primárními násilnými akty nebo hrozbami bezprostředně poškozeni." (Mareš 2005)
- Waldmannův teroristický kalkul: násilný akt, emecionálni reakce, výsledkem (ukvapená?) reakce a protiopatření

Kybernetický terorismus

- Zatím pouze jako koncept
- Problematické naplnit především požadavek excesivního násilí
- Teoreticky možné při útoku na kritickou infrastrukturu
- Absence spektakulárnosti?
- Aktivity teroristických skupin na sítích omezeny spíše na rekrutaci, zisk finančních prostředků či informační operace

Advanced Persistent Threats

- Termín 2006, počátky již 1998 (Moonlight Maze) či 2003 (Titan Rain)
- Nejčastějšími původci: Čína, Rusko, USA, Izrael
- Olympic Games (Flame, Duqu, Stuxnet)
- Obvykle zaměřeny na exfiltraci dat

Advanced Persistent Threats

- Kritéria:
- 1. Zdroje
- 2. Výběr cílů
- 3. Úmysly
- 4. Schopnosti a zkušenosti
- 5. Vytrvalost
- 6. Dodržování taktiky a postupů, vzorce chování

Advanced Persistent Threats

- Otázka státního sponzoringu
- Často omezené důkazní prostředky, obykle nepřímý charakter
- Zero days a technická sofistikovanost
- Použité servery a čas, kdy byl kód kompilován
- Chyby hackerů