

IT a stát:

Přesuňme mezinárodní konflikty do kyberprostoru

414877 Alžběta Bajerová

427441 David Janošek

414751 Tomáš Lalkovič

427432 Šimon Šoka

Proč podpořit přesun konfliktů do kyberprostoru?

- Pozitiva pro stát i civilní obyvatelstvo
- Kybernetická válka jako „Clean warfare“:
 - Humánnější, méně destruktivní, méně ekonomicky náročná
- Příklady mezistátního soupeření v kyberprostoru



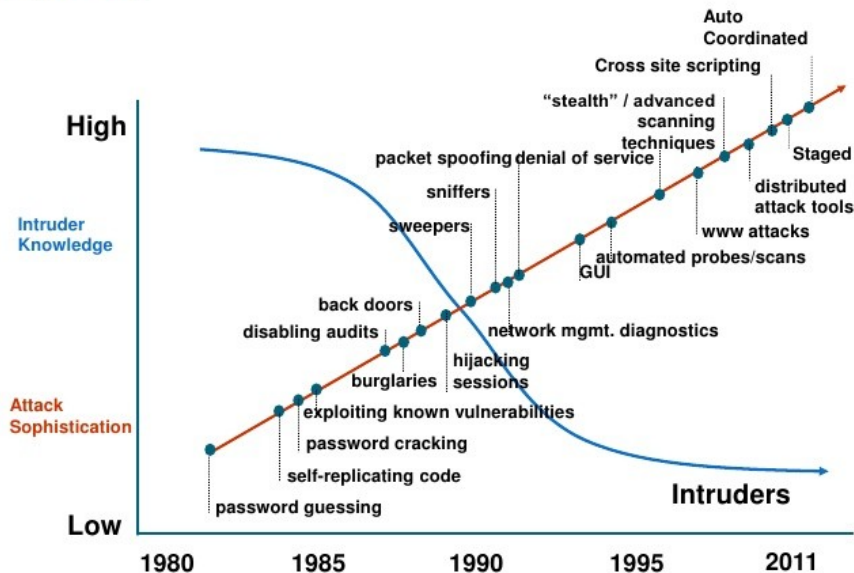
VS.



Současnost

Attack Sophistication vs. Intruder Technical Knowledge

Courtesy Emil on security



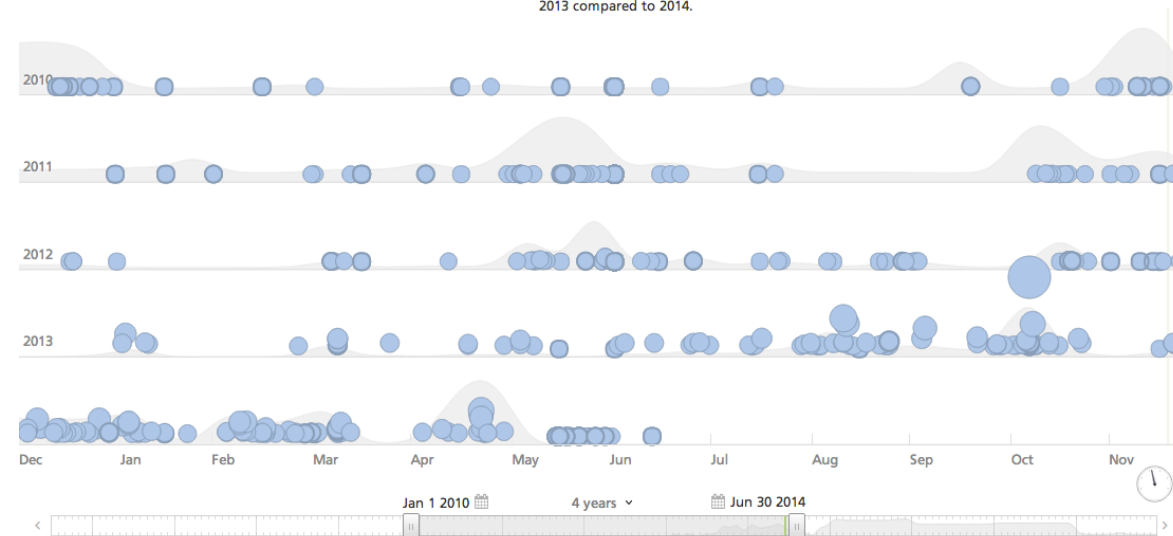
TULIP
making it possible

- Klesá nedostupnost technologií a know-how
- Klesá potřebná úroveň vzdělání útočníků
- zvyšuje se počet aktérů využívajících kybernetické zbraně
- Zvyšuje se sofistikovanost kybernetických hrozeb

Současnost

Cyber Attack Activity Since 2010

Note the increase of cyber attacks year after year. For example, look at the beginning of 2013 compared to 2014.



- Zvyšuje se počet kyberútoků
- Zvyšuje se ohrožení států kyberútoky
- Strany konfliktů již operují v 5. doméně a poměr jejího využití se zvýší

Současnost



Is there really any choice?

- Zvyšuje se počet kyberútoků
- Zvyšuje se ohrožení států kyberútoky
- Strany konfliktů již operují v 5. doméně a poměr jejího využití se zvýší

VÝHODY PRO STÁT

Míra nákladů x užitek

Preciznost zaměření

Množství potencionálních cílů

Preciznost + cíle » obrovský rozsah možných akcí

Zisk operačních, taktických i strategických výhod

Utajení a nízká míra detekce

Odhalení a přisouzení útoků

Utajení, detekce, odhalení, přisouzení » velké škody za značného omezení rizik a dopadů

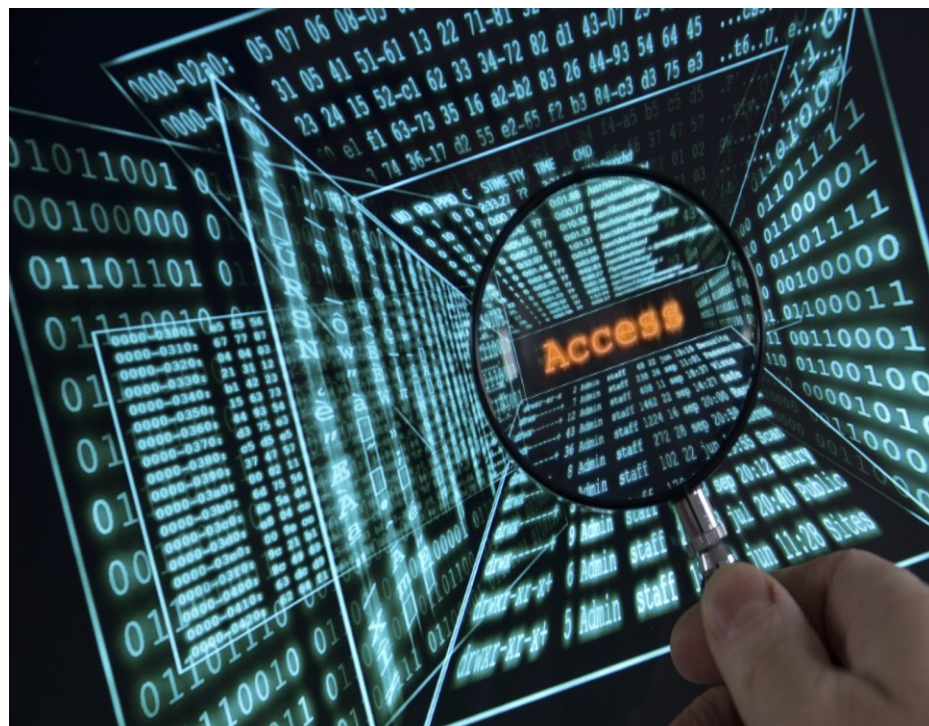
“Nations don’t need expensive ground stations, satellites, airplanes or ships to spy. Global intelligence capabilities now just need a few laptops and a high-speed connection.”

(Singer, Friedman 2014)

Špionáž

Dlouhodobost

Aktivita operativce vs. kyber prostor



Výhody pro civilní obyvatelstvo

Přesné zacílení → méně obětí

Vyřazení z provozu místo destrukce → zachování infrastruktury

Nabourání domácí propagandy nepřítele



PŘÍKLADY

Špionáž

Sabotáž

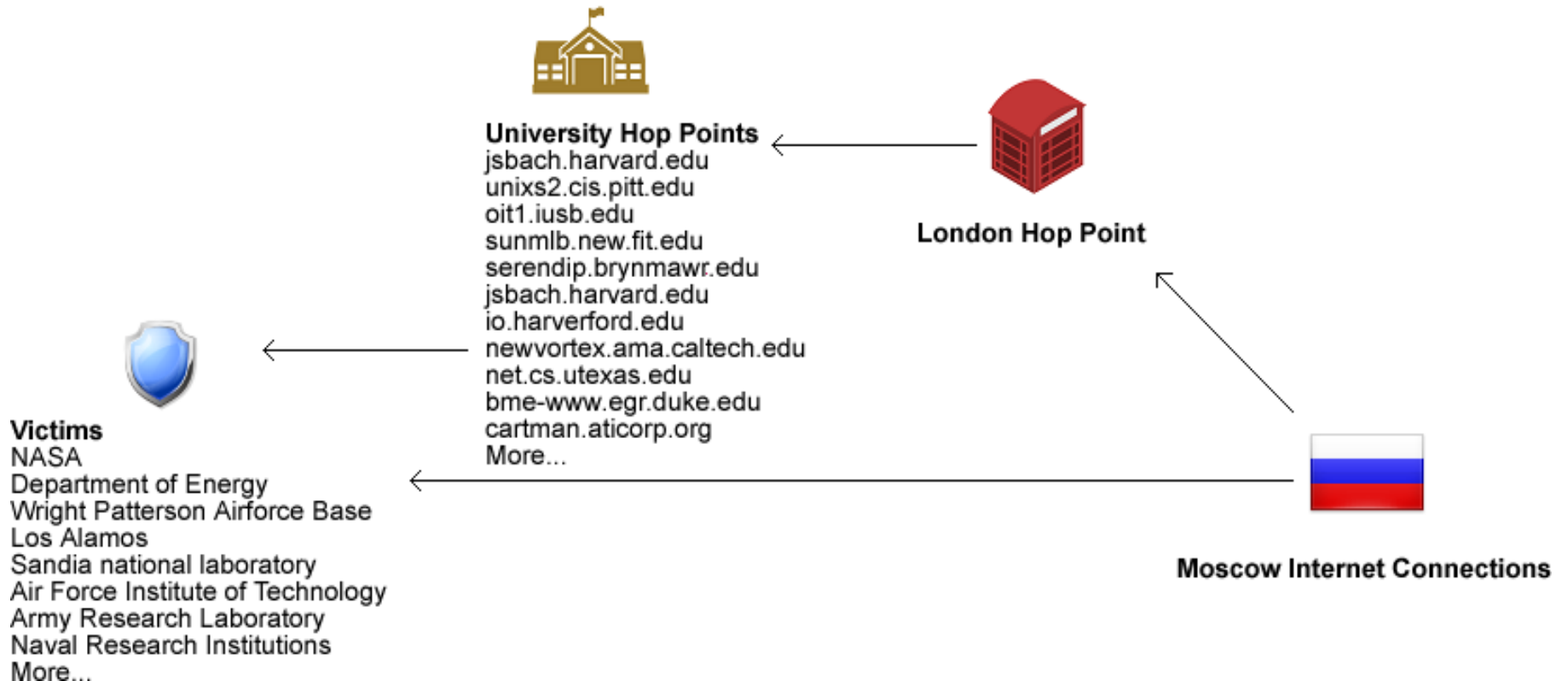
Politický nátlak

Moonlight Maze (1998)

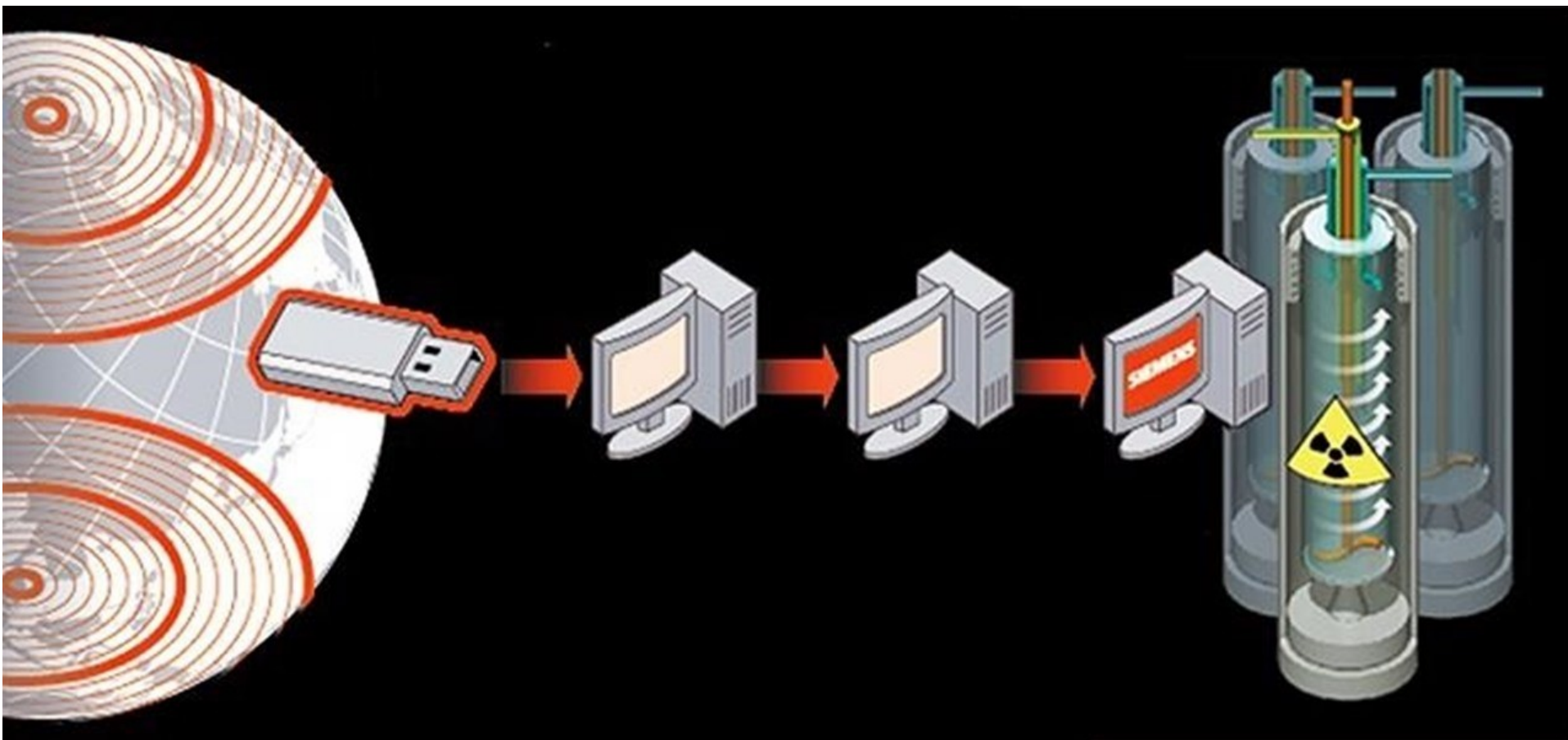
NASA, Department of Energy, Los Alamos, Wright Patterson AFB, laboratoře, výzkumné instituce

Titan Rain (2004)

Série útoků s původem v Číně



Stuxnet



Estonsko

- 2007 – přesun památníku sovětským vojakům
- série útoků (distributed denial of service) na stránky parlamentu, bank, ministerstev a médií



Děkujeme za pozornost.

Seznam použitých zdrojů:

Bartos, Ch. A. (2016): Cyber weapons are not created equal. In: *U.S. Naval Institute Proceedings*. June 2016, Vol. 142, no. 6, pp. 30-33.

Libicki, M. (1995): What Is Information Warfare? [online]. 1995 [cit. 2016-10-15]. Dostupné: (<http://handle.dtic.mil/100.2/ADA367662>).

Lilienthal, G – Ahmad, N. (2015): Cyber-attack as inevitable kinetic war. In: *Computer Law & Security Review: The International Journal of Technology Law and Practice*, June 2015, Vol. 31, no. 3, pp. 390-400.

Petr, J. (2016): *Cloud computing ve státní správě*, online text (<http://petr.blog.ihned.cz/c1-65294130-cloud-computing-ve-statni-sprave>). Ověřeno ke dni 15.10.2016.

Schreier, F. (2015): *On Cyberwarfare*. DCAF Horizon Working Paper, No. 7.

Singer, P., W., Friedman, A. (2014): *Cybersecurity and Cyberwar: What Everyone Needs To Know*. New York: Oxford University Press.

Technet.cz (2015): *Firmy bojují o ovládnutí internetu věcí. Uživatel může prodělat*, online text (http://technet.idnes.cz/souboj-internetu-veci-iot-097-/hardware.aspx?c=A150316_161724_hardware_vse). Ověřeno ke dni 15.10.2016.