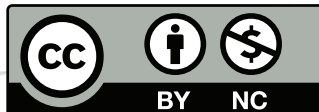


The Economics of Cyberwar

Steven M. Bellovin

<https://www.cs.columbia.edu/~smb>



Effort

- ◆ How hard is it to launch serious attacks?
- ◆ This translates very directly into “who can launch them?”
- ◆ Can a bored teenager launch a cyberwar? A terrorist group? A minor country?

Cyberweapons Aren't Easy

- ◆ Stuxnet, Flame, and Gauss took a *lot* of work
- ◆ Stuxnet used four “0-days”, bugs that might sell for \$100,000 on the open market, to penetrate a hardened target
- ◆ Flame used a previously-unknown cryptanalytic technique —that takes a *major* intelligence agency
- ◆ Gauss was so heavily obfuscated that it's been impossible to understand

Intelligence

- ◆ All three showed possession of very precise information about the target
- ◆ Spying? Cyberspying? Other technical intelligence? Good analysis?
- ◆ All of these are earmarks of a major government

Effectiveness

- ◆ How effective are cyberweapons?
- ◆ Are they hand grenades, conventional bombs, or nuclear weapons?
- ◆ In other words, how can they be employed?

They're Fragile

- ◆ Hacking—even government-sponsored hacking—is crucially dependent on the precise configuration of the targets
- ◆ Small changes to a site can utterly protect it (or can leave it fully exposed)
- ◆ Sysadmins can often recover rather quickly
- ◆ For these reasons, cyberweapons are best employed as *tactical* weapons and not as replacements for cruise missiles and ICBMs.

Staying in Touch

- ◆ Persistent code can stick around and watch what changes
- ◆ It can also download new attack code when and as needed
- ◆ This is more detectable, though, and the defender may have years to spot it
- ◆ High-end attackers can create persistent code, but high-end defenders can spot it

Conclusion

- ◆ Cyberwar isn't as easy as some people say
- ◆ Cyberweapons *can* be very useful if used properly (e.g., the Israeli air attack on the Syrian nuclear reactor)
- ◆ The biggest risk is from persistent code, but that opens up new avenues for the defense