Cyberwar: a Matter of Logistics and Privilege

Marcus J. Ranum

<mjr@tenable.com>

CSO, Tenable Network Security, Inc.

Who Am I?

- Industry insider for the last 25 years
  - Early innovator in firewall, VPN, and IDS technology
  - Started as a software engineer
  - Have held every position possible in high-tech start-ups from system administrator to marketing, sales, presales, director of engineering, CTO, CSO, CEO
  - Currently CSO of Tenable

Why This Talk?

- Cyberwar is now becoming an important part of the cyber-security industrial complex
  - At least, financially
- We don’t want to be like the atom bomb builders, standing around years later asking “what did we do wrong?” Do we?

I Agree

"Countries or individuals that engage in cyber-attacks should face consequences and international condemnation” ... "In an Internet-connected world, an attack on one nation's networks can be an attack on all."

- US Secretary of State Hillary Clinton

Some Things We Now Know

- Who said this?

  “The United States is fighting a cyber-war today, and we are losing. It's that simple. “

  A) Mike McConnell - former head of NSA, DNI, 2010

  B) The guy who green-lighted Stuxnet

  C) All of the above

More

- “The cyber-war mirrors the nuclear challenge in terms of the potential economic and psychological effects. So, should our strategy be deterrence or preemption? ***The answer: both***. Depending on the nature of the threat, we can deploy aspects of either approach to defend America in cyberspace. “ - Mike McConnell

Historical Perspective

- The problem with approaching cyberwar historically is that every attempt in history to oppose militarization has failed
  - Consistently violated by the powerful whenever it’s to their advantage
  - Regulation, in fact, is in service of the powerful (e.g.: nuclear non-proliferation)

Philosophical Arguments

- Approaching war philosophically becomes an exercise in the obvious:
  - It’s immoral
  - Involving civilians ought to be avoided
  - etc.
- These are statements of the obvious, and the fact that they’re consistently ignored is equally obvious

The Elusive “Terrorism”

- Terrorism is either:
  - A crime
  - A violation of the laws of war
- I don’t want to try to resolve this one because it’s actually not relevant
  - Because *either way* the international community has mechanisms for dealing with it

In Other Words...

- The line between “state-sponsored terrorism” and “armed conflict” is a bit brighter and clearer
  - A philosopher might argue that the issue is *attribution* - an “armed conflict” involves the notion that ***you know who’s attacking*** you, whereas “state-sponsored terrorism” attempts to destabilize the target without attribution of the attack

State-Sponsored Terror

- Thus we argue that “state-sponsored terror” is when a state adopts the technique of terror rather than armed conflict
  - Corollary: a terrorist operating within a state that repudiates their actions will either be thought to be a “terrorist” or “state-sponsored” to the degree to which they can be attributed as an agent of the state

Stuxnet

- Was Stuxnet:
  - State-sponsored terrorism
  - A violation of international humanitarian law
  - Both
  - Neither

Reprisal

- During conflict (not necessarily a declared state of war) under the GC a limited deliberate violation of the laws of war may be taken in *reprisal*
  - Not to be confused with *retorsions* which are legal retaliations like punitive tariffs
  - Generally reprisals are limited by *proportionality* because of the danger of involving civilians

Reprisal for Stuxnet?

- Would Iran be justified in launching a cyber attack against the US or Israel in response to Stuxnet?
  - This is a serious question
  - Especially if the answer is “yes”

- Let’s dismiss that as a hypothetical, though

Stuxnet a War Crime?

- It was either:
  - State-sponsored terrorism
  - War crime

- There is ***no*** 3rd alternative
  - Arguing it was state-sponsored terrorism (I.e: outside of an armed conflict) is “better” because it removes justification for reprisal

Oops...

- If Stuxnet was not released as an attributed attack (I.e.: it was done sneakily by ‘anonymous’ members of a state-run operation)
  - Wouldn’t those attackers be “illegal combatants” under the US’ current doctrine on what constitutes legitimate use of force?

Here’s the Problem

- Cyberwar cannot, will not, ever be fought over military networks
  - Components of civilian infrastructure will carry the data
  - Components of civilian infrastructure will be some of the targets

Again: International Law

- "The parties to the conflict must at all times distinguish between civilian objects and military objectives. Attacks may only be directed against military objectives. Attacks must not be directed against civilian objects."*

* Rule 7
Customary International
Humanitarian Law, ICRC

The Dangerous and Likely Outcome

- My fear* is that “cyberwar” will become a plaything of the powerful
  - *A weapon of privilege*
  - *We* will use it on *you* but don’t you ***dare*** use it on us

“If you shoot me in a dream, you’d better wake up and apologize”
- Mr. White, “Reservoir Dogs”

* prediction, actually

Current News

- DARPA Plan X (BAA 13-02) Foundational Cyberwarfare
  - Address the need for tools to help map networks
  - Simulate and understand damage to them
  - Is this defense or offense?

Why It's Dangerous

- Use of main force is great when you're the top dog
  - … But you know that eventually you will find yourself unable to retaliate, and without a shred of moral high ground to complain from

Conclusions

- We are at a crucial time in the militarization of cyberspace
  - What example will security practitioners set?
  - Engaging purely in defensive operations is the only position without moral onus

Conclusions

- What does it look like to break free of the US internet infrastructure?
  - Do you need your own DNS? Yes
  - Do you need your own Gmail? Yes
  - Do you need your own Linux? Maybe
  - Do you need your own Oracle? Sun? Microsoft?
  - Do you need your own Facebook, Amazon, Ebay, Twitter?

"If you shut down our power grid, maybe we will put a missile down one of your smokestacks.”

- Pentagon Spokesman