
Cyber Conflict
John E. Savage
Brown University
Outline

• Definitions of cyber penetration, exploitation, cyber and cyber-physical attack, and conflict
• Types of cyber attack and warfare
• Norms of behavior during cyber conflict
• Law of Armed Conflict applied to cyber
• Avoiding cyber conflict
• Research to harden targets and reduce risk.
Definition of Terms

• A **cyber-penetration** is a penetration of an information technology infrastructure without permission.

• A **cyber-exploitation** is a cyber-penetration designed to extract information.
How is Cyber Conflict Defined?

• A **cyber-attack** is a cyber-penetration designed to destroy, degrade or seriously disrupt an information technology infrastructure or data therein.

• A **cyber-physical attack** is a cyber-penetration designed to cause damage to an attached physical system, as in the Stuxnet attack.
How is Cyber Conflict Defined?

• **Cyber war** is a campaign of pure cyber- or cyber-physical attacks designed to cause serious long-lasting damage to an adversary.

• Attacks and exploitations differ in intent and are difficult to distinguish.

• Both implant a *remote administration tool* (RAT) that can be used to exfiltrate, alter or destroy data or degrade or destroy attached systems.
Potential Impacts of Cyber-Attacks

• In principle, pure cyber-attacks are self-depleting
  – Vulnerabilities can be patched once discovered.
  – 0-days can be expensive. Can we incentivize reporting?

• While cyber-attacks may be temporary, they can be costly. Examples of potentially serious attacks:
  – Destruction of the CHIPS bank clearance system
  – Erasure of memories of many FANNIE MAE data servers
  – Loss of electricity for months to many cities
  – Destruction of ~500,000 miles of US pipelines
Cyber-Attacks In Practice

• No pure cyber-attack has been the equivalent of an important kinetic attack.
• But attacks can cause serious or expensive damage
  – Shamoon wiped > 30,000 Saudi Aramco comptrs on 8/12
• Cyber-physical attacks likely to be more serious.
  – Stuxnet was a cyber-physical attack comparable to kinetic
  – Android app* to control of airplane described (4/10/13)

* http://www.computerworld.com/article/2475081/cybercrime-hacking/
  hacker-uses-an-android-to-remotely-attack-and-hijack-an-airplane.html
Attribution of Cyber-Attacks

• Attribution is difficult and deniable.
  – But in a real conflict, adversaries are likely to be known.

• Directed cyber-attacks and exploitations are often complex to plan and execute.
  – See Mandiant’s excellent report* for a description of the techniques, tactics and procedures (TTP) used.

* APT1: Exposing One of China’s Cyber Espionage Units, Mandiant
Mandiant tracks dozens of APT teams worldwide
APT1, 1 of 20 based in China, is the most prolific team
It is in the same location in the Pudong New Area of Shanghai as PLA Unit 61398
Same as “Comment Crew” and likely same as “Shady Rat”
APT1 Life Cycle

- Its lifecycle was perfected over about 10 years
- Typically starts with aggressive spear phishing
- Followed by deployment of custom weapons
- Ends by exporting compressed bundles of files

- Very persistent: Access to one victim lasted ~5 years
- Command and control hidden as HTML comments
- Attackers employ good English and slang in emails
- Attacked Obama’s 2008 presidential campaign

The Nature of Cyber-Attacks

• It is difficult to limit collateral damage.
• Cyber-attacks are likely to occur at start of a conventional conflict.
• Pure cyber war is not likely to occur because
  – It would destroy economies and
  – Is likely to blow back on the attacker
Possible Uses of Cyber-Attack

- Suppression of air defenses
  - 2007 Israeli attack on suspected Syrian nuclear reactor
- Blinding an opponent at the start of conflict
  - Knock out communications at start of a campaign
- Disrupting military supply/communication system
  - Blind HQ to activity in the field, disrupt logistics supply
- Sowing distrust in field reports
  - Feeding false information to headquarters

- Influencing outcome of an election
- Changing medical records of leaders
Types of Cyber Warfare*

• Strategic – designed to affect the will and capabilities of adversary.
  – Goal may be to cripple an adversary or delay the adversary so that an attack is a fait accompli
• Deterrence – attack designed to warn that an attack will be costly
• Operational – designed to affect conventional physical capabilities of an adversary

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010 NAS Workshop on Deterring Cyberattacks.
Types of Cyber Warfare*

• Targeted – e.g. damage a state’s nuclear weapons production, take down a website.
• Active defense – techniques designed to limit an active attacker’s abilities.
  – “Hacking back” is an example of active defense.
• Libicki* does not include cyberexploitation under the heading of cyberwarfare.

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.
Norms of Deception*

• Laws of armed conflict frown on making military operators look like civilians.
• But, deception is sine qua non of cyberwarfare.
• Does the military use of civilian communication networks present a problem?

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.
Proportionality Norms*

• In international law civilian injuries and deaths are tolerable if proportionate to the military advantage gained.

• In cyberspace the effects of a cyberattack are much harder to calibrate.

• How should the issue of proportionality for cyberspace be handled?

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.
Military Necessity & Collateral Damage*

- Although desirable to avoid gratuitous harm, it’s hard to predict which civilian systems affected.

- Do you think that a state that anticipates that it will engage in a cyber conflict has an obligation not to co-mingle civilian and military systems?

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.
Law of Armed Conflict (LOAC)

• It has two major components
  – *Jus ad bellum* when is it appropriate to resort to war
  – *Jus in bellow* governs conduct during hostilities

• Is cyber action more like war or mere coercion?
  – UN Charter defines some coercion as “use of force”

• Authors of Tallinn Manual* on cyber warfare argue that LOAC apply to cyberspace

Law of Armed Conflict (LOAC)

• States must ask if weapons systems satisfy LOAC
  – What are examples of cyber weapons?
  – Would they satisfy LOAC?
• The Schmitt* test for use-of-force (see following)
  – Severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumption of legitimacy.

Schmitt Test for Use-of-Force

• **Severity**: Cyber operations that threaten physical harm more closely approximate an armed attack. Relevant factors include scope, duration, and intensity.

• **Immediacy**: Consequences that manifest quickly without time to mitigate harmful effects or seek peaceful accommodation more likely to be viewed as a use of force.

• **Directness**: The more direct the causal connection between the cyber operation and the consequences, the more likely states will deem it to be a use of force.
Schmitt Test for Use-of-Force

• **Invasiveness**: The more a cyber operation impairs the territorial integrity or sovereignty of a state, the more likely it will be viewed as a use of force.

• **Measurability**: States are more likely to view a cyber operation as a use of force if the consequences are easily identifiable and objectively quantifiable.
Schmitt Test for Use-of-Force (cont)

• **Presumptive legitimacy:** To the extent certain activities are legitimate outside of the cyber context, they remain so in the cyber domain, for example, espionage, psychological operations, and propaganda.

• **Responsibility:** The closer the nexus between the cyber operation and a state, the more likely it will be characterized as a use of force.
Neutrality Norms*

• Geographical distribution of servers and cloud computing complicate sovereignty issues.
• In normal war neutrals who allow belligerents to pass are viewed as complicit.
• In cyberspace, the situation appears different.
  – Is it different?
  – What does the Tallinn Manual say?

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.
Cyber Network Exploitation (CNE) Norms*

- States should disassociate themselves from criminal or freelance hackers.
  - A strategically deceptive practice
  - Corrupting because state may overlook other crimes
- Difference between state and other espionage
  - State-on-state spying can contribute to stability
  - Commercial espionage is destabilizing.
- Nice to distinguish between espionage and attack.
- If attack against system is off-limits, so is spying.

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.
Libicki’s Reversibility Norm*

• Every attack not intended to break something has an antidote.
  – If data has been encrypted, then provide the key
  – If data corrupted, provide original data 😊

• This norm would prohibit an attack if an antidote cannot be provided.

• Do you agree that every attack has an antidote?

• Will an attacker without an antidote, not attack?

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.
Hack-Back Defense*

• What is hack-back?
  – The victim uses attacker-like tools, techniques and procedures (TTP) to penetrate & control attacker.

• An attacker may execute a hack-back via a proxy

• Is hack-back legal under US law?

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.
Defense Against Attacks Is Hard
US Defense Science Board Assessment*

• The cyber threat is serious – similar to nuclear threat during Cold War

• DoD not prepared to defend with confidence against most sophisticated cyber attacks

• It will take years for DoD to respond to threat

• In the interim, be prudent

Avoiding Cyber Conflict*

• Create threat reduction centers
• Reduce number of compromised computers
• Prevail on vendors to improve security
• Sell cyber insurance to encourage security
• Use other economic incentives/intermediaries

• News report: In June 2013 US & Russia agree to install Cybewar-Hotline.

Fund Innovative Research*

• Find solutions to standard malware techniques
• Deploy moving targets technologies
• Collect and use blacklists of compromised sites
• Make standard technologies more robust
• Create domestic high-assurance providers of hardware and software

Novel Research Results

- **Computational Integrity (CI)**
  - To run program on un-trusted cloud, modify it.
  - Cloud returns transcript of computation that customer can quickly check for correctness

- **Secure Computation (SC)**
  - To keep data private, encrypt before sending to cloud
  - Special encryption permits computation by cloud
  - Results decrypted at customer

- CI is now efficient, SC less so but improving
Review

- Definitions of cyber penetration, exploitation, cyber and cyber-physical attack, and conflict
- Types of cyber attack and warfare
- Norms of behavior during cyber conflict
- Law of Armed Conflict applied to cyber
- Avoiding cyber conflict
- Research to harden targets and reduce risk.