

CSCI 1800 Cybersecurity and International Relations

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.
- 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 many of the ~500,000 miles of US pipelines

Cyber-Attacks In Practice

- No pure cyber-attack has been the equivalent of an important kinetic attack.
- Pure cyber-attacks are self-depleting. 0-days will be patched eventually.
 - 0-days are expensive. Is giving one away a measure of intent?
- Cyber attacks can cause serious or expensive damage.
 - Memories of > 30,000 Saudi Aramco computers wiped in 8/12. Restoring them took ten days.
- Cyber-physical attacks likely to be more serious.
 - Stuxnet was a cyber-physical attack comparable to kinetic
 - Android app designed to take control of an airplane (4/10/13)

Attribution of Cyber-Attacks

- Attribution is difficult and deniable.
 - But in real conflict, adversaries are likely to be known.
- Directed cyber-attacks and exploitations are often complex to plan and execute.
 - See Appendix B of Mandiant report for tactics used.
- It is difficult to limit collateral damage.
- Cyber-attacks likely to occur at start of conventional conflict. Pure cyber war is not likely.

Possible Types of Cyber-Attack

- Suppression of air defenses
- Blinding an opponent at the start of conflict
- Disrupting military supply/communication system
- Sowing distrust in field reports

- Influencing outcome of an election
- Changing medical records of leaders
- Disrupting adversary's censorship infrastructure

Types of Cyber Warfare¹

- 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

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

Types of Cyber Warfare¹

- Special – achieve special effects such as harming a state’s nuclear weapons production, taking down a website.
- Active defense – techniques designed to limit an active attacker’s abilities.
 - “Hacking back” is an example of active defense.
 - **What are other examples?**
- Libicki does not include cyberexploitation under the heading of cyberwarfare.

1. Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Detering Cyberattacks.

Norms of Deception¹

- Laws of armed conflict frown on making military operators look like civilians.
- But, deception is sine qua non of cyberwarfare.
- **Should norms frown on making military systems look like civilian ones?**

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

Proportionality Norms¹

- 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.
- **The issue of proportionality needs to be investigated for cyberspace.**
 - How do we set up this issue for discussion?

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

Military Necessity & Collateral Damage¹

- Although desirable to avoid gratuitous harm, hard to predict which civilian systems affected.
- A state that anticipates that it will participate in a cyber conflict has an obligation not to co-mingle civilian and military systems more than business logic would dictate.
 - Do you agree?
 - How should we approach it?

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

Law of Armed Conflict (LOAC)

- Authors of Tallinn Manual on cyber conflict argue that LOAC apply to cyberspace
- 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
 - Severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumption of legitimacy.
 - Terms defined on subsequent pages.

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.
- *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.

Schmitt Test for Use-of-Force (cont)

- *Measurability*: States are more likely to view a cyber operation as a use of force if the consequences are easily identifiable and objectively quantifiable.
- *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.³⁵

Neutrality Norms¹

- 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?

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

Cyber Network Exploitation (CNE) Norms¹

- 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.

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

US Laws and Cyber Actions

- Title 10 of the US Code outlines the role of US armed forces
- Title 50 of the US Code concerns covert action
- Privateer – privately owned ship authorized for use in war by issuance of a Letter of Marque
 - Can capture enemy vessel and sell it in admiralty court
 - US Constitution recognizes Letters of Marque (Art. 1)
 - Could the US use this power to fight hackers/terrorists?

Reversibility Norm¹

- 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?

1. Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.

Hack-Back Defense¹

- What is hack-back?
 - The victim uses attacker-like tools, techniques and procedures (TTP) to penetrate & control attacker.
 - Is it legal in the US?
- An attacker may defend against a hack-back by using a proxy.
- Is hack-back legal under US law?

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

Avoiding Cyber Conflict²

- 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

2. **On Cyber Peace**, Les Bloom and John Savage, Issue Brief, Atlantic Council, August 2011

Fund Innovative Research²

- 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

2. **On Cyber Peace**, Les Bloom and John Savage, Issue Brief, Atlantic Council, August 2011

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

US Defense Science Board³

- 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

3. Task Force Report: Resilient Military Systems and the Advanced Cyber Threat, U.S. Department of Defense, Defense Science Board, January 2013.

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.