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 attacks** or **cyber-physical attacks** designed to cause serious long-lasting damage to an adversary.

• **Attacks and exploitations** differ in intent but 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.
  – Why is this observation important?
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 ~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, if patching done.
  - How to handle zero-days? Bug bounties, criminalization?
- Pure cyber attacks can be serious or expensive.
  - Memories of > 30,000 Saudi Aramco computers wiped in 8/12. Restoring them took 10-15 days.
- Cyber-physical attacks likely to be more serious.
  - Stuxnet was a cyber-physical attack comparable to kinetic
  - Android app* to control of an airplane described (4/10/13)


† [http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/](http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/)
Attribution of Cyber-Attacks

- Attribution is difficult and may be deniable.
  - But some orgs good at identifying adversaries
- Persistent cyber-attacks can be complex to plan & execute — See Appendix B, Mandiant report*
- It is difficult to limit collateral damage.
- Cyber-attacks likely 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
• Sow distrust in field reports
• Influencing outcome of an election
• Changing medical records of leaders
• Opening adversary’s censorship infrastructure
Types of Cyber Warfare*

- **Strategic** – designed to affect the will and capabilities of an 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*

• **Special** – achieve special effects, e.g. harming nuclear weapons production, embarrassing a state by taking down an important 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.

* 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.
- Should norms frown on making military cyber systems look like civilian ones?

*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.
  – A cyber weapon is often a self-replicating worm.

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

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

- 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?

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

• It is a branch of international law;
• Governs relations between States during armed conflicts;
• Also applies to fighting within the State;
• Is intended to reduce as much as possible the suffering, loss and damage caused by war;
• Places obligations on persons in the States involved, primarily members of the armed forces;
• Is not designed to impede military efficiency

Law of Armed Conflict in Cyberspace

• 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.
  – These terms are defined on subsequent pages.

* https://www.nap.edu/read/12997/chapter/12#155
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.
Neutrality Norms*

• Geographical distribution of servers and cloud computing complicate sovereignty issues.
• In normal war neutrals who allow belligerents to pass their territory 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.

• Hard to distinguish between espionage and attack.

• If attack against a system is off-limits, so is spying.

* Pulling Punches in Cyberspace, M. Libicki, Procs., 2010NAS Workshop on Deterring Cyberattacks.
US Laws and Cyber Actions

- Title 10 of US Code defines 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?
Libicki’s Reversibility Norm*

• Every attack not intended to break something must have 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 every attack should have 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 defend against a hack-back by using a proxy.

• Is hack-back legal under US law?

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

• In 2013* US & Russia agree to Cybewar-Hotline.


• On Cyber Peace, Bloom & Savage, Issue Brief, Atlantic Council, August 2011
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)
  – Modify program for un-trusted cloud so that Cloud returns transcript of computation that customer can quickly check for correctness

• Secure Computation (SC)
  – Encrypt data before sending to cloud
  – Replace standard operations with ones that combine encrypted data and yield encryptions of standard ops.
  – Results are then decrypted at customer site.

• CI is now efficient, SC less so but improving
US Defense Science Board*

• 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

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.