CSCI 1800 Cybersecurity and International Relations

Is Cyberwar A Real Possibility?

John E. Savage
Brown University
Outline

• Three articles:
  – Think Again: Cyberwar. Don’t fear the digital bogeyman. Virtual conflict is still more hype than reality. By Thomas Rid, Foreign Policy, March/April, 2012
  – Cyberwar is Already Upon Us, By John Arquilla, Foreign Policy, March/April, 2012
Thomas Rid: Think Again Cyberwar

- Is cyberwar coming?
- Is a digital Pearl Harbor only a matter of time?
- Are cyberattacks becoming easier?
- Can cyberweapons create massive collateral damage?
- In cyberspace does offense dominate defense?
- Do we need a cyberarms treaty?
- Is the West falling behind Russia and China?

1. Think Again: Cyberwar. Don’t fear the digital bogeyman. Virtual conflict is still more hype than reality, by Thomas Rid, Foreign Policy, Feb. 27, 2012.
Is Cyberwar Already Upon Us?

• Cyberwar predictions:
  – 1993 “Cyberwar is coming!” Arquilla & Ronfeldt
  – 2006 “is a domain in which the Air Force flies and fights” AF Secretary Michael Wynne
  – 2012 “just as critical to military operations as air, sea, and space” William J. Lynn III, Deputy Secretary of Defense
  – Lots of books and papers
Is Cyberwar Already Upon Us? No Way

• “Still more hype than hazard.”
• An act of war “has to be potentially violent, it has to be purposeful, and it has to be political.”
• No cyber attack, including Stuxnet, meets criteria.
• Doubts 1982 Soviet pipeline explosion happened.
• 2007 Estonia attack - three weeks, blocked max of 58 sites, but not violent, no one took credit.
• No known cyber attack led to loss of life!
Is Digital Pearl Harbor Likely? No!

- 2014 Former DoD Sec Panetta warns cyber attack could “devastate our critical infrastructure and paralyze our nation.” – Symantec Govt. Conf.
- 2010 Clarke book, Cyber War, predicts calamities
- 2011 at URI, Gen. Alexander expresses worry about destructive attacks
  – Not good example. Resulted from poor maintenance
- Difficult to conjure up good scenarios!  
  – Do you agree?
Are Cyber Attacks Becoming Easier?

• Although malware volume growing, the kind that has very large impact is hard to produce.

• Stuxnet cleverly attacked Natanz centrifuges.
  – It randomly degraded centrifuges, circumvented safety procedures, and misled operators.

• Complexity of Stuxnet strongly suggests that high-impact cyber weapons take a lot of time and intelligence to craft.

• Cyber attacks becoming harder, not easier!
Can Cyber Weapons Produce Massive Collateral Damage?

• Stuxnet is a worm and it propagated around the world.

• However, it was designed to attack a specific facility and did no damage except at Natanz.

• This suggests that high-impact weapons will be narrowly targeted and, thus, not result in massive collateral damage.
Does Offense Dominate Defense?

• Many believe cyber gives advantage to attacker
  – Attacker chooses time and mode of attack to acquire control

• Offense is at a disadvantage because:
  – High cost of developing powerful weapon
  – Generic weapons have limited effectiveness
  – Weapon may only be useable once

• Political threat exists if replication possible
Let’s Examine Rid’s Assertions

• Reasons why offense is at a disadvantage:
  – High cost of developing powerful weapon
    • Why are powerful weapons costly?
  – Generic weapons have limited effectiveness
    • Do monocultures make it easier to develop weapons?
  – Weapon may only be useable once
    • Doesn’t Mandiant report that ATP1 stayed in computers for months and years?

• How reliable is his analysis?
Is a Cyber Arms Control Treaty Needed?

• Cyberspace is now a domain for competition on development of cyber weapons.

• Shouldn’t try to forge cyber arms treaty because:
  – Difficult to distinguish between crime and politics
  – Verification is impossible given dual use of weapons
  – Aggressors see no political benefit to attribution

• Having a few states agree on arms limitations is as unrealistic as trying to outlaw espionage.
Is West Falling Behind Russia & China?

• While Russia and China are aggressive, their skills are almost certainly overrated.
• For military grade ability, US & Israel dominate
• Russia and China concerned more about state security than genuine cybersecurity.
  – West has more valuable intellectual property
  – Free speech, protected in West, not in East
  – Reflected in Russia/China UN code of conduct.
• Russia and China lead in defining cybersecurity as fight against subversive behavior.
Summary of Rid’s Article

• Is cyberwar coming? No!
• Is digital Pearl Harbor only a matter of time? No
• Are cyberattacks becoming easier? No
• Can cyberweapons create massive collateral damage? Not likely
• In cyber does offense dominate defense? No
• Do we need a cyberarms treaty? No
• Is the West falling behind Russia and China? Only if cybersecurity defined as preventing subversion.
Arquilla: Cyberwar is Already Upon Us²

• Cyberwar is here to stay
  – Most info on cyberwar says it would be devastating
  – Georgian 2008 attack greatly eased Russian invasion

• Not unlike use of air power in Spanish civil war
  – Military techniques are being tested, which is ominous.

2. Cyberwar is Already Upon Us, By John Arquilla, Foreign Policy, March/April, 2012
Entrusting Too Much To Cyberweapons

• Bemused by argument that cyberwar is a way to covertly achieve advantage without first defeating conventional land, sea & air forces.
  – Bombing is not definitive nor will bits be.
  – Nonetheless, can impose high costs on nations

• More concerned that small-scale cyberwar actions will be scaled up.
  – Yes, weapons expensive but once created can overcome defenses. Advantage to attackers.
Defending Against Cyberweapons

• Given potential for damage to net centric military, we must obtain a better understanding of this new technology.
Nakashima: US Accelerating Cyberweapon Research

- “The Pentagon is accelerating new generation of cyberweapons capable of disrupting enemy military networks even when those networks are not connected to the Internet.”
- “U.S. officials say that existing cyberweaponry has the potential to disable components of a weapon system although not likely to destroy the system.”

2015 DoD Law of War Manual*

- Section XVI on cyber operations, page 994
- Cyber operations defined. Examples:
  - Disrupt, deny, degrade, or destroy information
  - Advance force preparation
    - E.g. reconnaissance, seizure of supporting positions, and pre-implantation of capabilities and weapons
- What are the implications of “implanting cyber access tools or malicious code”?
  - Could this result in “armed conflict”?

Lect22 4/19/2017
Application of LOAC to Cyber Ops

- Obvious if effects are equivalent to kinetic ops
- New challenges due to variety of cyber op effects
  - Cyber ops as forcible means & methods of warfare
  - Cyber ops as non-forcible means & methods
  - Others equivalent to seizure of property
- General humanitarian guiding principle
  - Must avoid suffering, injury or destruction unnecessary to achieve military objective
Jus ad Bellum (The Right to Go To War)

• Criteria to consult to decide if war is justified
• Some uses of force are not permissible under UN Charter
• Cyber effects equivalent to use of force:
  – Cause nuclear power plant meltdown
  – Open a dam above a city causing death & destruction
  – Disable air traffic control causing deaths.
  – Cripple a military’s logistics system
UN Charter on Use of Force

• UN Article 2(4): “[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”
International Law Applies in Cyberspace

• Peacetime intelligence & counterintelligence OK
  – However, cyber intrusion may be seen as hostile
  – UN Article 51, right of self defense, may be triggered

• US asserts right to respond with kinetic to cyber
International Law Applies in Cyberspace

• A state’s right to necessary and proportionate self-defense in response to armed attack through cyberspace applies whether the attack is attributed to a State or a non-State actor.

• In US, generally the President decides whether to invoke the right of self-defense.
Cyber Ops & Law of Neutrality

- Belligerent States are bound to respect the sovereign rights of neutral States.
  - But cyber ops in one state may affect another
- They must not erect a facility in a neutral state to communicate solely with belligerents
  - However, publicly available facilities are exempted
Cyber Ops and Jus in Bello

• Concerns just conduct of war.
• Cyber use of force must comport with
  – Requirements of distinction and proportionality
• Distinction: Must distinguish between civilian and military targets.
• Proportionality: Loss of life, injury & damages to civilian objects must not be out of proportion to the military advantage to be gained.
Cyber Ops That Are Not Attacks

- Operations that are reversible or have only temporary effects.
- Some examples:
  - defacing a government webpage;
  - a minor, brief disruption of internet services;
  - briefly disrupting, disabling, or interfering with communications; and
  - disseminating propaganda.
Other Considerations

• Sometimes less harm caused by cyber ops
• Incidental damage may be minimized

• Improper use of signs during cyber ops
  – Using non-hostile comms for hostile purposes
  – Fabricating message from enemy head of state to troops signaling a cease-fire
  – But not prohibited to disguise network traffic as enemy traffic
  – Non-military can participate in cyber conflict
Review

• Three articles:
  – Think Again: Cyberwar. Don’t fear the digital bogeyman. Virtual conflict is still more hype than reality. By Thomas Rid, Foreign Policy, March/April, 2012
  – Cyberwar is Already Upon Us, By John Arquilla, Foreign Policy, March/April, 2012