Some Practical and Legal Challenges in Addressing Cyber Conflict

Professor/Lecturer Phil Mann (Phil)
Lecturer, Old Dominion University

Caveat: I am solely responsible for the content.
Why such challenges?

• Cyber conflict as a study is new, perhaps 35 years old.

• The study of cyber conflict lies at the intersection of technology, security, law and policy, so it requires some degree of both technical and legal/policy knowledge to be effective. It can be maddeningly ambiguous too.

• The digital world has no boundaries, no walls, no tanks, no guns....
The challenge of understanding the architecture of cyber conflict

• Behind any real or potential "cyber conflict" in a generic sense in which a government is involved, there may be elements of:
  • Cybersecurity as a defensive posture;
  • Criminal and national security investigations;
  • Criminal and national security intelligence collection;
  • Diplomatic and foreign relations;
  • Offensive operations; and
  • National strategy.

• Coordination of multiple agencies so affected, both civilian and military, may be daunting.
## Essential Characteristics of Different Cyber-Actions -- One Approach

<table>
<thead>
<tr>
<th>Type of Cyber-Action</th>
<th>Involves only non-state actors</th>
<th>Must be violation of criminal law, committed by means of a computer system</th>
<th>Objective must be to undermine the function of a computer network</th>
<th>Must have a political or national security purpose</th>
<th>Effects must be equivalent to an “armed attack,” or activity must occur in the context of armed conflict</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-Attack</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Cyber-Crime</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber-Warfare</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>
Some Observations about Relationship among Cyber-Actions

• Do all cyber-crimes constitute cyber-attacks? No.
• Do some cyber-crimes also constitute cyber-attacks? Yes
• Do all cyber-attacks also constitute cyber-warfare? No
• Do some cyber-attacks also constitute cyber-warfare? Yes
• Do all acts of cyber-warfare constitute cyber-attacks? Yes
Investigative/Intelligence challenges of cyber conflict

• Making informed decisions about any possible conflict or incident requires investigation – the who, what, when, where and why.

• In the cyber realm, any of the 5Ws can be especially challenging.

• Examples...attribution...the who?
Investigative/Intelligence Challenges: Realities of Cyberwar/Cyber Conflict: **The Who**

- Internet as ecosystem composed of "incredibly wide mix of players...." Who are *they*?
- And what about proxy and quasi-state actors? Who takes responsibility? Who controls them? Friend or foe or something else?
  - Cyber Blackwater/Government Outsourcing
  - Patriotic Hackers
  - Non-state actors (Think privateers, War of 1812; Anonymous; Terrorists)
Investigative/Intelligence Challenges: Realities of Cyberwar: The What

• While cyberwar operates with "digital precision...the effects of the actual attacks may be staggering imprecise." Singer and Cole, The Reality of Cyberwar, Politico.com, 7/9/2015
  • Kinetic effect can range wildly.
  • Russian attacks on Ukraine’s power grid.
Investigative/Intelligence Challenges: Why would a foreign government hack?

Intelligence and information collection (by military/civilian agencies)?
Covert action (not simply collect, but alter or destroy data)?
Armed conflict (cause a meltdown on a nuclear-powered ship)?
Prepare the battlefield (access a targeted system, but no more)?
Hold-at-risk (signal to the enemy that you can and have accessed a valuable data)?
Or "simply" to gain trade secrets?

But how can the victim-nation reliably know the true intent?
Legal challenges of cyber conflict

- Technology outpaces law and policy.
  - Laws commonly react to and frame developments in society.
  - In contrast, technologies and the language of technology often lead developments, especially in a digital world.
    - U.S. wiretap laws in the Omnibus Crime Control Act of 1968
    - International laws and customs face the same limitations.
**Legal Challenges: The "Laws of War," Jus Ad Bellum and Jus in Bello**

- Laws of war impose limitations

1) under what circumstances may military force – warfare – be lawfully used:
   - Is there legal justification to even enter into warfare and use force... is it just, as in “Jus Ad Bellum?”

2) if military force is justified, how may such warfare be conducted:
   - What humanitarian considerations limit how warfare/military force may be carried out, as in “the Jus in Bello?”
**Legal Challenges:** How do *fundamental* rules of war and International Humanitarian Law (IHL) apply in cyberspace?

- **Principle of military necessity** (an appropriate target is one that will confer a military advantage)
- **Requirement to distinguish military forces from civilian populations**  
- **Prohibition on targeting civilians** and civilian objects
- **Principle of proportionality of response**  
- **Imperative to minimize collateral damage**
- **Ban on perfidy** (In the context of war, perfidy is a form of deception in which one side promises to act in good faith (such as by raising a flag of truce) with the intention of breaking that promise once the enemy is exposed (such as by coming out of cover to attack the enemy coming to take the "surrendering" prisoners into custody)).
- **Principle of neutrality** (International law has long recognized that States may remain neutrals in an international war, but that means that these neutral States may not support in any meaningful manner any side, or allies, etc.)
**Legal Challenges**: What fully addresses international law applicable to cyber operations or cyberwarfare?

- **Tallinn Manual**
  - NATO Cyber Defense Centre of Excellence (CCD CoE)
  - Proposal for a „Law of Cyber War“
  - Cyber warfare ≈ other military operations
  - Response by military activities (rule 5.13)
  - Act must be attributable to a state (rule 6.6)
    - UN Charter Art 51
    - Attribution problem

- **Tallinn 2.0**
  - sovereignty, jurisdiction, intervention
  - International participation
Legal Challenges: Sample Tallinn 2.0 Rules

• Rule 20 – **Countermeasures** (general principle)
  • A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international obligation that is owed by another State.

• Rule 21 – **Purpose of countermeasures**
  • Countermeasures, whether cyber in nature or not, may only be taken to induce a responsible State to comply with legal obligations it owes to an injured State.
    • Designed to bring about a return to lawful relations between the States concerned, not retaliation or punishment; countermeasures are generally thought of as temporary measures.

• Rule 23 – **Proportionality of countermeasures**
  • Countermeasures, whether cyber in nature or not, must be proportionate to the injury to which they respond.

• Rule 24 – **States entitled to take countermeasures**
  • Only an injured State may engage in countermeasures, whether cyber in nature or not.
Questions? More material follows
Now suppose as a nation, we formulate a response: What is right and appropriate?

• We can try to *prevent cyberhacking and related cyberconflict* through enhanced *cybersecurity* measures. But what if such efforts fail? Options:
  • **Criminal investigative response**: Publicly prosecute the wrongdoers!
    • Seek justice? Embarrass the responsible nation or entity?
  • **Diplomatic and economic pressures/responses**?
  • **Covert actions**?
  • **Offensive cyber operations**?
Cyber Ops run the gamut: They may refer to a range of activities aimed at foreign computer systems from:

- intelligence collection
- counterintelligence
- covert actions conducted abroad
- to cyberwarfare (executed by DoD)
Cyberspace as a U.S. operational domain: What entities carry this out and how?

• **Title 10** of the United States Code governs the **form, functions, duties and responsibilities of the U.S. Armed Forces in its traditional military activities** executed through Secretary of Defense to combatant commanders. Think cyberwar.

• DOD is scrupulous about honoring laws, limits and customs of war.

• Any operation carried out by President/Commander in Chief consistent with accepted norms of war.
Cyberspace may be defined as "a global domain within the information environment consisting of interdependent networks of information technology... including the Internet, telecommunications networks, computer systems."

Cyber Operations are those that involve "the employment of cyberspace capabilities where the primary purpose is to achieve objectives or effects in or through cyberspace." Consider these examples of objectives:

Examples:
- Ops that disrupt, deny or degrade information resident in computer networks and the computers or networks themselves
- Ops that implant cyber access tools or malicious code
- Ops that acquire foreign intelligence unrelated to specific military objectives such as gaining info about an adversary's intent, capabilities
A U.S. perspective on responding to hostile or malicious cyber operations...force

• Under Article 51 of the U.N. Charter, a State's inherent right of self-defense may be triggered by cyber ops that amount to an armed attack (or imminent threat thereof). The U.S. may respond to hostile acts in cyberspace, but its response must be reported immediately to the U.N. Security Council.
  • U.S. will respond against any illegal use of force; this potentially gives the right to take necessary and proportionate actions in self-defense.
  • And the U.S. response in self-defense need not be a cyber action, as long as it's necessary and proportionate.
  • If cyber ops against the U.S. do not constitute a use of force, the U.S. may take necessary and appropriate actions that do not constitute the use of force. E.g. economic embargo; diplomatic protest.
  • Decisions about whether to invoke a State's (e.g. U.S.) right of self-defense must be made at the national level (e.g. the President) as they involve rights and responsibilities under international law.
• Title 50 of the United States Code governs how the United States conducts war and ensures the national security, including the use of covert actions.

• Title 50's 43 chapters address intelligence operations, espionage, military equipment and assets, emergency powers, and nuclear security, among other issues.

  • For example, consider the Foreign Intelligence Surveillance Act (FISA), Title 50, USC 1801 forward...
What are covert activities?

• Executive Order 12333 and National Security Act (Title 50) define "covert action" as distinct from clandestine intelligence collection, as an operation undertaken by USG primarily designed "to influence political, economic or military conditions abroad, where it is intended that the role of the USG will not be apparent or publicly acknowledged." Key word is influence.

• Covert activities do not include traditional 1) counterintelligence activities; 2) traditional military activities conducted under Title 10; 3) diplomacy; 4) law enforcement, and 5) pure intelligence collection.

• Traditionally conducted by CIA, though CIA may be assisted by military and other USG agencies.
Title 50 requirements for **covert action:**

• Title 50, USC Section 413b requires *the President*, through the National Security Council, to provide *written findings* that the covert operation:
  • is necessary to promote identifiable foreign policy objectives *and*
  • is important to U.S. security *and*
  • doesn't violate the Constitution or federal law.

• There are requirements for Congressional reporting......

• **Covert actions cannot take place inside the U.S.!!!**
What if it's not a covert action, but rather a **traditional** military activity in **cyberspace**?

Go to Department of Defense and Title 10 authorities, which are subject to oversight by the Armed Services Committees of Congress.

*Just because an operation must be conducted in secret doesn't make it a covert operation.* Think special ops, military deception ops or clandestine ops to prepare environment for future military action.

*Traditional doesn't mean the technology is traditional.*
• When no specific rule applies, the principles of the law of war form the general guide for conduct during war (Jus in Bello).
  • Certain cyber ops may have no clear *kinetic* (involving application of lethal force in motion) parallel in terms of their capabilities and the effects they create.
  • Sometimes they do. Consider bombing a dam that floods a civilian population; *the insertion of a malicious code might do the same thing.*
Applying Jus in Bello – Operations that Constitute Cyber Attacks

- If a cyber operation constitutes an attack, then the law of war rules on conducting attacks may apply to cyber operations.
  - For example, a cyber-attack that would destroy enemy computer systems could not be directed against ostensibly civilian infrastructure (e.g. no attacks against computer systems supporting ODU or NYSE unless they are legitimate military objectives...)
  - And proportionality rules apply too. Consider incidental damages to computer systems that are not military objectives. What are the potential effects?
    - A brief disruption of internet services would not, for example, require a proportionality analysis.