A Survey and Examination of the Adequacy of the Laws Related to Cyber Warfare

A paper arguing that the current rules of war can address the emerging issues raised by cyber warfare

Presented by:
Dondi West, M.Sc., J.D.
Associate, Booz Allen Hamilton

Def Con 18
July 30th – August 1st 2010
Las Vegas, Nevada

Disclaimers

- The views expressed in this presentation and its supporting materials are those of the author alone and do not necessarily reflect the official policy or position of Booz Allen Hamilton, or any entity of the US Government.

- This talk is for general information purposes and is not intended to be and should not be taken as legal or consulting advice on any particular matter.

Agenda

- Introduction to CNO and the Actors Involved
- Survey of the Laws with the Largest Impact on Cyber Warfare
- Popular Issues Intensifying Cyber Warfare Debate
- Five Reasons Why the U.S. Shouldn't Enter into Int'l Treaties for Cyber Warfare
- Conclusion, Question and Answers

Introduction

- President Obama's 60-Day Study
- 2008 Cyber Attack against Georgia Infrastructure and Key Government Websites
- Cyber Spies Penetrate US Electrical Grid (2009)
- July 4th Cyber Attacks Against U.S.

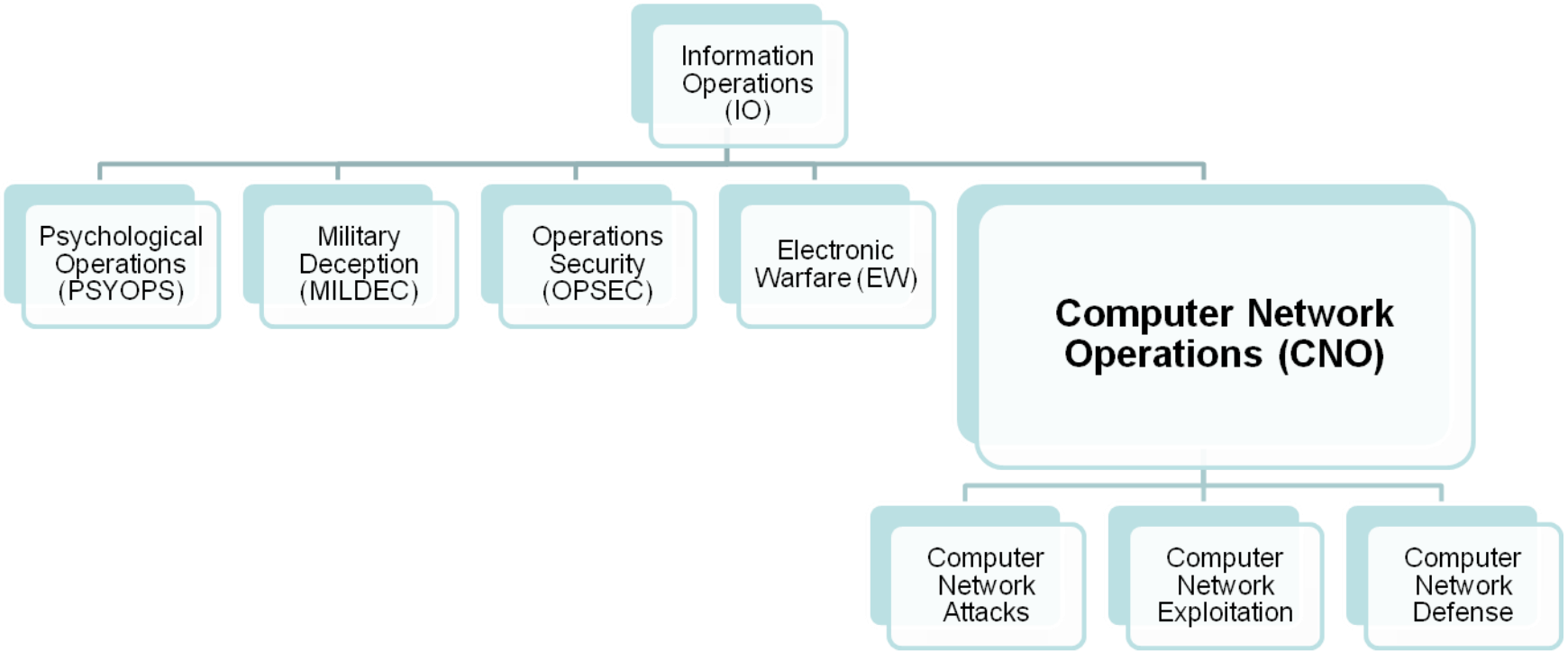
<u>Results of 60 Day Study</u>

- Many Near-Term & Mid-Term Action Plans
- No Mandate for Examining Laws of Cyber Warfare in Results of 60-Day Study
- Intense Debate: International Treaty for Cyber Warfare

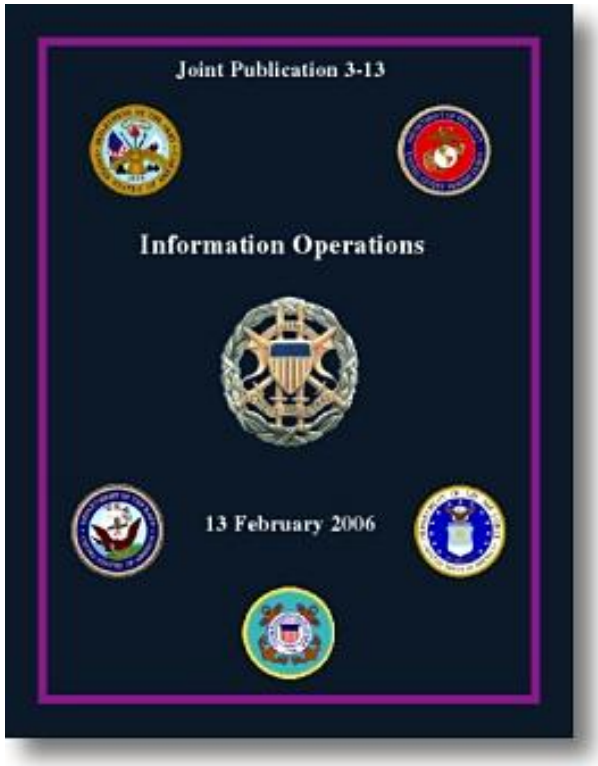
I. Introduction to Computer Network Operations and the Actors Involved

Introduction to CNO

Joint Pub 3-13 Categorizes Cyber Acts Under the Domain of **Computer Network Operations** (CNO)



Computer Network Operations



- **Computer Network Defense (“CND”)**
  - Includes actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks
- **Computer Network Exploitation (“CNE”)**
  - Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks
- **Computer Network Attack (“CNA”)**
  - Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves

- The term “Cyber” is used in a overly broad manner
- It is necessary to understand Cyber within the context of which of the three CNO domains are being referenced

The Actors Involved

- Nation State vs. Nation State
- Nation State vs. non-State Actor
  - Post 9/11:UNSCR 1368

- This study is not concerned with international cyber crimes
- This study is not concerned with Private Hacker vs. Private Hacker
- Attribution: Huge Issue, But Outside Scope of Study

II. A Brief Overview of Cyber Warfare's Current Legal Framework

The two principle questions facing military operations in cyberspace are:

1. Which interstate activities in cyberspace constitute a threat or use of force under international law, and
2. When such a threat or use of force does constitute an armed attack under international law, how does that law of armed conflict apply to the lawful exercise of the inherent right of self defense in cyberspace.*

Two regimes: (1) Pre-Hostilities Law; and (2) Post-Hostilities Law

** Thomas C. Wingfield & James B. Michael, An Introduction to Legal Aspects of Operations in Cyberspace 10 (Naval Postgraduate School) (explaining that two important legal issues related to cyber warfare are (1) when does a CNA constitute a threat or use of force, and (2) how do the laws of armed conflict govern cyber warfare) (2004); see also Jeffrey Carr, Inside Cyber Warfare 31-43 (Mike Loukides ed., O'Reilly Media 2010) (2009).*

Pre-Hostilities Law (Jus ad Bellum)

- UN Charter Article 2(4)
  - All 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 any other manner inconsistent with the Purposes of the United Nations
  - UNSC has the exclusive power to determine when an act is a use of force and respond to such acts.

- Article 51: Right to Self Defense
  - *Nothing in the present Charter shall impair the inherent right of individual or collective self defense…*

- There is a general prohibition against ALL uses of force, except those:
  - Sanctioned by the UN Security Council; OR
  - Done in Self-Defense

Post-Hostilities Law (Jus in Bello)

- Once two nations are in armed conflict with each other, the law of war applies.
- The Law of War must apply in ALL military operations. Cyber operations NOT exempt.
- Only Lawful Military Targets may be attacked.
- When deciding if a target can be attacked, a combatant commander must consider:
  - Distinction
  - Balancing Military Necessity With Humanity
  - Proportionality

Distinction

1) Must be formal distinction between combatant and non-combatants AND
2) Duty to conduct warfare in manners that minimize harms to civilians

- **Article 50:** defines who are civilians and civilian populations
- **Article 51:** describes protections to be given to civilian populations
- **Article 52:** regulation of targeting civilian objects
- **Article 57:** outlines specific steps commanders must take in order to verify what isn't a civilian object in nature

Distinction: Cyber Implications

- Interconnective nature of internet causes networks to have duel use
- Civilian ISP provide online networks to civilians and support military objectives of communication
- Commanders must take reasonable steps to limit attacks on part of a network used by the enemy combatant

Example: Releasing a comp virus in a network essential to civilian function such as a banking or electrical power will likely violate the principle of distinction.

Military Necessity and Humanity

Caveats:

A. Necessity: Attack on target must further legit military objectives or grant a definite military advantage.

B. Humanity: Attack shouldn't cause unnecessary suffering or unwarranted injury for a military purpose.

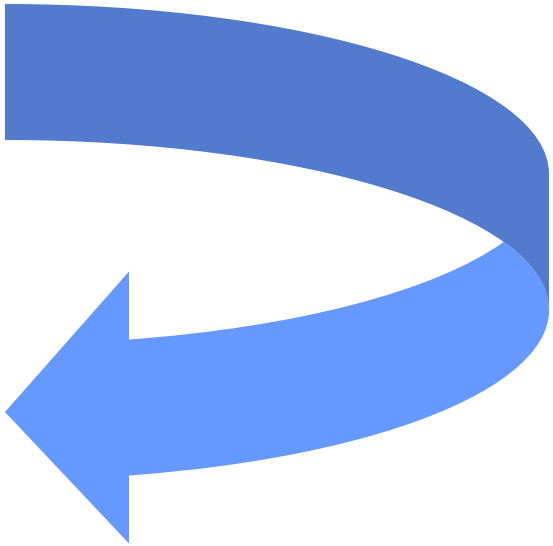
Cyber ex:

- Attack on enemy computer system that controls enemy's power supply (SCADA)
- Necessity here is easy…
- Humanity…. NOT SO EASY
- What if that power also supplies a civilian hospital?

Proportionality

1. Deontology: “ends justify the means”
2. Business Language: Essentially a ROI Analysis
3. Tool for balancing military necessity and humanity
4. Attacker has responsibility to take reasonable steps to determine what collateral damage to contemplated attack can cause

* Determine if benefits from winning military objectives outweigh its negative collateral effects like extensive power loss to civilian populations



III. Popular Issues Intensifying Cyber Warfare Debate

The “Use of Force?” Debate

- Schmitt/Wingfield Multifactor Tests
- The Security Council has the sole authority and discretion to ratify any use of force; to include a very mild cyber attack
- Article 51 of the UN Charter provides for the right of countries to engage in military action in self defense, including collective self-defense
  - Should the Security Counsel Adopt a Multifactor Tests?
  - All Uses of Force are Presumed to be Forbidden
  - Criticisms of Multifactor Tests

The “Use of Force?” Debate

- The Rule (In Dondi’s Opinion): *A nation conducting any CNA, prior to hostilities, is legally doing so only in the case of reasonable self-defense; if self-defense is not involved, then the nation actor is conducting CNA with the risk of being sanctioned by the UN Council*
  - This may imply that the UN Council needs to implement means of monitoring all state-sponsored acts of CNA and become more aggressive in holding countries accountable for cyber acts, which is a challenge in and of itself, but it does not imply that the international laws of war are inadequate

The “Cyber Arms Race” Analogy

- “A ‘dead heat’ is a race, campaign or other contest that is so close that it is impossible to predict the winner. That’s what it looks like when it comes to the continuing race for cyber warfare supremacy, and experts agree this will be the case for the foreseeable future. With images of the Cold War and its associated arms race, as cyber warfare, cyber espionage, cyber attacks and cyber terrorism continues to evolve the top three leaders (US, Russia and China) are jockeying for position.” —*Defense Tech*

- Nuclear Weapons -vs- Cyber Weapons

- The Cyber threat is real, but shouldn’t be compared to Nuclear Weapons

- Nuclear Treaties → Cyber Treaties

The Cyber Threat DebateThe "Cyber Arms Race" Analogy

- *On June 8, 2010, Booz Allen Executive Vice President Mike McConnell and his debate partner, Harvard law professor Jonathan Zittrain, jointly debated two opponents on the topic of cyber threat titled "The Cyber War Threat Has Been Grossly Exaggerated," and McConnell and Zittrain faced off against privacy advocate Marc Rotenberg and security technologist Bruce Schneier, who argued in favor of the measure -- that the threat has been exaggerated.*

- *At the close of the fast paced and entertaining discussion, the McConnell/Zittrain arguments had swayed 71% of the audience to their position, vs. 23% for the opponents and only 6% undecided.*

- **Dondi's Opinion: <u>Cyber is the new Fire.</u>** Cybersecurity awareness must become engrained in our society like fire safety.
  - It is hard to exaggerate the threat or dangers of fire.
- Dondi's "Fire-Marshal Bill" Test: The threat is real, but when it comes to cyber security, we should only throw the flag in the event of Gross Exaggeration.

IV. Arguments Against Creating a Distinct Body of and International Treaty for Cyber Warfare Law

Fields of Law are Seldom Demarcated by Technology

- Sommer Argument
  - The Laws of Spears, Bows, Arrows and Shields
  - The Treaty Against Imitating Paranormal Activity During Warfare
  - The Law of Equestrian Warfare (Horse Law)
  - The Law of the Semi-Automatic Rifle
  - The Hague Rules of Aerial Warfare
  - The treaty Banning the Use of Environmental Modification Techniques in Warfare
  - Protocol Banning Weapons whose Fragments Cannot be Detected by X-ray
  - Protocol Banning the use of Blinding Lasers
- The current rules of war, prior to, and during hostility, encompass cyber warfare

Undue Limitations on a Primarily Non-Lethal Strategic Deterrence

- Because cyber warfare is primarily non-lethal, and due to its deterrence capability, it may be the greater of two evils when it is compared to traditional kinetic weaponry such as missiles

- In light of the UN Charter's guiding principle of preserving human life, proponents of the creation of a cyber warfare treaty should consider the fact that such a treaty may have the effect of limiting a primarily non-lethal weapon, and possibly shift the weaponry trend back to the use of kinetic weapons

Our Real Adversaries are Unlikely to Comply with a Cyber Treaty

- Creating an international law will, therefore, have the actual effect of crippling our warfighting ability, while our real adversaries continue to run rogue

- If we were to enter into a cyber warfare treaty, we would essentially be volunteering to fight war “with one hand behind our back,” while those we are likely to fight against will do so with no rule of law in mind—let alone a rule governing cyber warfare

The rate of technology will outpace the ability for an international cyber regime to produce responsive policy, while the flexibility allotted by the UN Charter are able to absorb technological advances.

Conclusion

- The laws of war will be tested by cyber warfare in two situations: first, prior to the commencement of an armed conflict; second, when an armed conflict is ongoing. In each of these situations, the current laws of war can address the emerging issues raised by cyber warfare.

- Although several hot-button issues related to cyber warfare are often discussed and fuel the cyber warfare debate, they may not be issues at all. A careful analysis shows that the current UN Charter and Laws of War should continue to govern cyber warfare.

- Creating an international treaty or law for cyber warfare would do more harm than good and seriously cripple our ability to conduct war.

Question and Answers

Contact Information:
Email: dondiw@gmail.com
Twitter: @dondiwest
BLOG: www.cyberwarandlaw.com