Cyber Warfare v. Cyber Stability

Jody R. Westby, Esq.

Cyber Power: The Quest Towards a Common Ground

October 11, 2012

STATUS OF INTERNET

- 2.3 billion people online and 250 countries & territories connected
- Systems deployed without proper security controls
- Security best practices & standards not implemented
- Cybercrime laws are inconsistent; substantive & procedural; many countries do not have cybercrime laws
- Response requires swift coordination, certainty on legal authority for actions – Lacking framework– takes months
- Many countries do not have a CERT or security professionals
- 24/7 Points of Contact Networks: only 50+ countries since 1997
- Lack of trained law enforcement personnel for investigation, cooperation, and search & seizure assistance
- Judges and prosecutors are not trained in cyber considerations
- Leaves open opportunities for cyber conflict

GEO-CYBER STABILITY

- Geo-Cyber Stability – The Ability of All Countries to Utilize the Internet for Both National Security Purposes and Economic, Political, and Social Benefit While Refraining From Activities That Could Cause Unnecessary Suffering & Destruction
- Depends on Legal Framework to Assure Agreed Upon Level of Geo-Cyber Stability Through Mutual Cooperation & International Law
- Means Country's Critical Infrastructure Shall Not Be Disrupted In Manner Inconsistent With the Laws of Armed Conflict & Other Applicable Treaties and Conventions

LAW OF ARMED CONFLICT

- Regulates Conduct of Armed Hostilities
- Applies to Conduct of Military Operations & Related Activities in Armed Conflict
- Armed Conflict (Necessity, Distinction, Proportionality)
- Prevent Unnecessary Suffering & Destruction in War
- Protects Civilians, Prisoners, Wounded, Sick, Shipwrecked
- Military Must Plan & Execute Operations Within Law of Armed Conflict

BASIC LEGAL FRAMEWORK

National Laws

- Cybercrime Laws (Substantive & Procedural & Assistance)
- Armed Conflict
- Jurisdictional Issues (extradition, dual criminality)
- International Cooperation (search/seizure, investigation, ISPs, 24/7)

International Laws

- Council of Europe Convention on Cybercrime
- UN Charter
- NATO Treaty
- Geneva Conventions & Protocol on Protection of Victims
- Hague Conventions
- Convention on Prohibition or Restrictions on Weapons

LAW OF ARMED CONFLICT: How

Military Necessity – **Combat forces can engage in only those acts necessary to accomplish legitimate military objective**. Means can target facilities, equipment, forces that **would lead to enemy's partial or complete submission.** Examples of illegal: bio-chem weapons, expanding hollow bullets

Military Distinction – **Must distinguish between lawful & unlawful targets, such as civilians, civilian property, wounded**. **Must separate military from civilian** to maximum extent possible. Indiscriminate attack strikes both military & civilians or civilian targets

Military Proportionality -- **prohibits force in excess of that needed to accomplish military objective.** Proportionality **compares military advantage to the harm inflicted.** Requires balancing between direct military advantage anticipated and expected incidental civilian injury or damage.

LAW OF ARMED CONFLICT: Who

Lawful Combatant – **Person authorized by governmental authority to engage in hostilities.** May be an irregular force. Must be commanded by person responsible for subordinates, have distinctive emblems recognizable at distance, such as uniform, carry arms openly, and conduct operations according to Law of Armed Conflict. Have immunity for lawful acts of war.

Noncombatant – **Not authorized by governmental authority to engage in hostilities.** Does not engage in them. Examples: civilians accompanying military, military personnel such as chaplains, medics. They may not be object of direct attack, but may be killed incident to direct attack.

Unlawful Combatant – **Individuals who directly participate in hostilities without authorization by governmental authority or under international law.** Examples: civilians who attack forces, pirates, bandits. May be targeted and killed, tried as war criminal.

Undetermined Combatant – Geneva Convention applies until determined

LAW OF ARMED CONFLICT: What

Military Targets – Targets that by their nature, location, purpose, or use make effective contribution to an **enemy's military capability and whose total or partial destruction or neutralization at the time of attack** enhance legitimate military objectives.

Protected Targets – Some **targets protected, such as hospitals, transportation of wounded or sick, religious or cultural sites, safety zones** of Geneva Convention. But if objects used for military purposes they may be attacked.

LEGAL FRAMEWORK: UN CHARTER

Art. 2(4): Members refrain from threat or use of force against **territorial integrity and political independence**

Art. 41: Security Council may decide what measures **not involving the use of armed force** are to be employed; complete or partial disruption of communications ok

Art 42: If Security Council considers actions pursuant to Art 41 inadequate, it may take **action by air, sea, or land forces**

Art 51: Nothing impairs inherent right to self-defense if armed attack occurs

Art 99: Secretary-General may bring to the attention of the Security Council **any matter which in his opinion may threaten the maintenance of peace and security**

LEGAL FRAMEWORK: NATO TREATY

Art. 3: Parties separately & jointly maintain and develop individual and collective capacity to resist **armed attack**

Art. 4: Parties will consult when **territorial integrity, political independence, or security** of any of the Parties is threatened

Art 5: Parties agree **armed attack** against one or more of them shall be considered attack against all

Art 6(1): Armed attack means

- On **territory** of any of Parties in Europe or North America
- On **territories or on islands** of any of Parties
- On the **forces, vessels, or aircraft** of any of the Parties

Art 12: After 10 years in force, Parties shall, if any of them requests, **consult together for the purposes of reviewing the Treaty, having regard for the factors then affecting peace and security**

LEGAL FRAMEWORK: HAGUE CONVENTIONS

Conventions V & VIII:

- Sets forth rights and duties of neutral countries re war on **land, sea, and air**
- Country may not move troops or convoys across **territory** of neutral nation or commit any act of hostility in **territorial waters** of neutral country

LEGAL QUESTIONS

- What Constitutes an Act of Cyber Warfare?
- Can Critical Infrastructure Be Targeted?
- If Infrastructure Supports Targets Protected by Geneva Convention, Can These Be Targeted?
- Are Infrastructure Attacks Necessary to Achieve Military Objectives?
- How are Military and Civilian Targets Distinguished?
- Is Damage Proportional to Military Objectives?
- How Are Cyber Soldiers Distinguished?
- How Is It Determined If Third Parties Are Acting for Nation State?
- What is Excessive Force In Cyberspace?
- What Cooperation & Assistance Do Governments Have to Provide?
- What Permission From Other Countries Is Required?
- Can Governments Take Over Private Sector Network?

CYBER STABILITY: WHERE TO BEGIN

- Need International Laws That Govern Cyber Conflict—Assure Minimum Stability
- Armed Conflict Laws Intended to Prevent Unnecessary Suffering & Destruction
- Harm and Damage from Cyber War Can Be Widespread & Not Proportional
- Impossible Not to Involve Communication Systems of Other Countries
- Should Protect Critical Infrastructure Like Hospitals, Civilians, Sick, Wounded Because All of Life is Dependent Upon Them, Even Medical Treatment
- Use of Botherders or Rogue Actors Are Not Within Definition of Legal Combatant
- Need NATO Treaty or International Agreement to Ensure Collective Defense as Deterrent
- Need International Agreement to Assist & Cooperate on Cyber Investigations
- Countries Should Have Separate Laws to Govern Cybercrimes, Attacks on Critical Infrastructure & Attacks That are for Purpose of Terrorism

4 PROPOSED PRINCIPLES CYBER CONFLICT

1. A certain amount of critical infrastructure should be protected to prevent unnecessary destruction, harm, and suffering and ensure minimum essential communications

   - For example, Hospitals & medical, assisted living, financial, supply chains, transportation, news, educational, religious, first responders, law enforcement
   - Harm and damage that would flow from destruction or incapacitation of infra systems in unnecessary and would cause extreme suffering and hardship Geneva Conventions
   - Right to choose methods not unlimited; distinguish between civilian and military; protection of sick, infirm, expectant mothers; may propose neutralized zones
   - Children under 15 orphaned or separated should have maintenance, religion, and education facilitated
   - Destruction of real or personal property belonging individually or collectively to private persons, country, or public authorities is prohibited
   - Civilians enjoy protections against dangers from military operations; shall not be objects of attack or subjected to acts designed to spread terror or indiscriminate attacks
   - Attacks against objects indispensible to survival (food, water, supplies) and attacks against dangerous prohibited
   - Hague Conventions ban on weapons having excessively injurious or indiscriminate effects

4 PROPOSED PRINCIPLES CYBER CONFLICT

2. The use of botnets and other irregular cyber forces should be outlawed
    - Combatants are indistinguishable from other attacker; no distinctive emblem; not distinguishable from distance
3. Countries must respect the neutrality of other countries and shall not transmit any kind of attack through their critical infrastructure
    - Hague restrictions on transport of troops or supplies across neutral territories or waters
4. Countries must assist one another in their investigation of cybercriminal activities
    - All cyber attacks look the same at the outset; investigation helps identify
    - Countries that want to be connected should have an obligation to assist; countries who refuse could be viewed as aiding and abetting the criminals or attacking country by refusing to assist. Only through assistance, can countries can remain neutral

ACTIONS TO TAKE

CYBERCRIME

Develop Harmonized Laws

- CoE Cybercrime Convention
- International Toolkit for Cybercrime Legislation

Harmonized Nat'l Strategies for CIP

- ITU Best Practices for Nat'l Approach
- ITU CIIP Self-Assessment Toolkit

Multilateral Agreement to Assist Cyber Investigations & Govt-to-Govt Coop

Est. Multi-Disciplinary Response Ctrs

Complete Global 24/7 POCs

Training Programs

Multilateral Exercises

Collaborative R&D

Standards Development

CYBER CONFLICT

Hague Convention

- Permission to Launch Attacks Through Networks of Another Country

Geneva Convention (IV & Protocol I)

- Civilian Critical Infra Protected Target
- Cyber Combatants Prohibited

UN Charter

- Territorial Integrity Includes Critical Infra
- Cyber Attack can be Armed Attack
- Amend Self Defense Provisions
- Security Council Action Can Include Cyber

NATO Treaty

- Cyber Attack is Armed Attack; Territorial
- Collective Defense for Cyber

A STEP FORWARD

- All governments should recognize that international law guarantees individuals the free flow of information and ideas; these apply to cyberspace. Restrictions should only be as necessary and accompanied by a process for legal review.

- All countries should work together to develop a common code of cyber conduct and harmonized global legal framework, including procedural provisions regarding assistance and cooperation that respects privacy and human rights. All governments, service providers, and users should support international law enforcement efforts against cyber criminals.

- All users, service providers, and governments should work to ensure that cyberspace is not used in any way that would result in the exploitation of users, particularly the young and defenseless, through violence or degradation.

A STEP FORWARD

- Governments, organizations, and the private sector, including individuals, should implement and maintain comprehensive security programs based upon internationally accepted best practices and standards and utilizing privacy and security technologies.
- Software and hardware developers should strive to develop secure technologies that promote resiliency and resist vulnerabilities.
- Governments should actively participate in efforts to promote global cyber security and cyber peace and to avoid the use of cyberspace for conflict.

CONCLUSION

A legal framework applicable to cyber conflict that assures a minimum level of geo-cyber stability must be developed, lest the Wild Wild Web become the 21st century tool of destruction and impede on the rule of law regarding armed conflict, human rights, and friendly relations among nation states.

THANK YOU!

Jody R. Westby

westby@globalcyberrisk.com

202.255.2700