Legal Aspects of Cyberspace Operations

Black hat Abu Dhabi 2012

Agenda

- **Cyberspace Operations**
  - **Computer Network Security & Defense**
  - **Computer Network Exploitation**
  - **Computer Network Attack**
  - **Active Response**

Disclaimer - aka the fine print

- **Joint Ethics Regulation**
- **Views are those of the speaker**
- **I'm here in personal capacity**
- **Don't represent view of government**
- **Disclaimer required at beginning of presentation.**
- **All material - unclassified**

Cyberspace Operations
(Computer Network Operations)
Where Law
And
Technology Meet

Cyberspace Law & Policy

- **Sources of Law**
  - **Customary International Law**
  - **UN Charter**
- **Law of Sovereign Nation**
  - **Domestic Law**

Sources of Law

- **How long does it take to create customary/international law?**

Sources of Law

- **Hours after the September 11, 2001 terrorist attacks President Bush announced that, in bringing to justice those responsible, "we will make no distinction between the terrorists who committed these acts and those who harbor them."**

Sources of Law

- **Hours after the September 11, 2001 terrorist attacks President Bush announced that, in bringing to justice those responsible, "we will make no distinction between the terrorists who committed these acts and those who harbor them."**
- **On September 12, 2001, one day after the initial proclamation of what has come to be known as the Bush Doctrine, the members of the United Nations (U.N.) General Assembly and Security Council passed resolutions reinforcing the doctrine.**

Sources of Law

- **Article 38 of the Statute of the International Court of Justice (ICJ) defines custom as “evidence of a general practice accepted as law.”**

Sources of Law

- **Article 38 of the Statute of the International Court of Justice (ICJ) defines custom as "evidence of a general practice accepted as law."**
- **Legal writings maintain that customary international law consists of two elements:**

Sources of Law

- **Article 38 of the Statute of the International Court of Justice (ICJ) defines custom as "evidence of a general practice accepted as law."**
- **Legal writings maintain that customary international law consists of two elements:**
  - **(1) *usage*, states' practice, and,**

Sources of Law

- **Article 38 of the Statute of the International Court of Justice (ICJ) defines custom as "evidence of a general practice accepted as law."**
- **Legal writings maintain that customary international law consists of two elements:**
  - **(1) *usage*, states' practice, and,**
  - **(2) *opinio juris*, a sense of legal obligation.**

Sources of Law

- **Article 38 of the Statute of the International Court of Justice (ICJ) defines custom as "evidence of a general practice accepted as law."**
- **Traditional writings maintain that customary international law consists of two elements:**
  - **(1) *usage*, states' practice, and,**
  - **(2) *opinio juris*, a sense of legal obligation.**
- **Courts traditionally have ascertained custom by engaging in a detailed historical analysis of many centuries of state practice, recognizing a customary international law when it reflects both a state's uniform practice over a long period of time and that state's conscious acceptance of the principle as law.**

Sources of Law

- **New theory of "instant" customary law-**
  - **States can advance a new customary international law, either in concert with other states or unilaterally, simply by evincing a new *opinio juris*, if other states do not object, and in fact follow suit, they will share the same *opinio juris*, thus forming a new rule of customary international law.**

Cyberspace Operations

Cyberwar

&

Law of Armed Conflict

Personal Analysis & Opinion

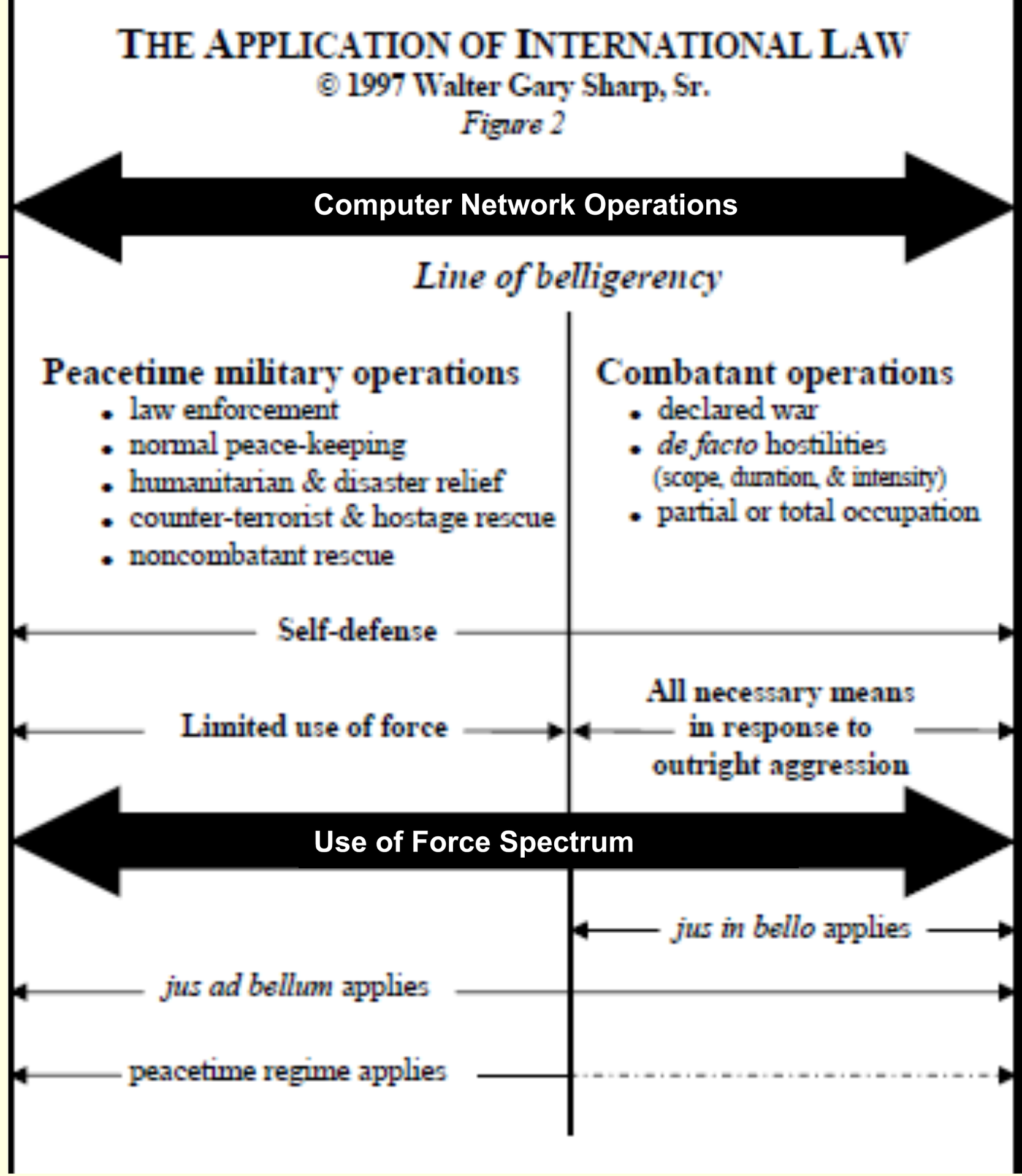
Not US Government Position

The Law of Armed Conflict

- **Computer Network Attack = Act of War ?**
- **Obsolete concept not mentioned in the UN Charter and seldom heard in modern diplomatic discourse.**
- **An act of war is a violation of another nation's rights under international law that is so egregious that the victim would be justified in declaring war.**
- **Declarations of war have fallen into disuse**

Law of Armed Conflict

Developed to govern a regime for peacetime and conflict spectrum



Department of Defense Cyberspace Policy Report

A Report to Congress
Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934

November 2011

'TALLINN MANUAL'
ON
THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE

Prepared by the International Group of Experts
At the Invitation of
The NATO Cooperative Cyber Defence Centre of Excellence

DRAFT

CURRENT AS OF
21 AUGUST 2012

FORTHCOMING, CAMBRIDGE UNIVERSITY PRESS

INQUIRIES: Professor Michael Schmitt
schmitt@aya.yale.edu

National Security

U.S. official says cyberattacks can trigger self-defense rule

By Ellen Nakashima, Published: September 18

Cyberattacks can amount to armed attacks triggering the right of self-defense and are subject to international laws of war, the State Department's top lawyer said Tuesday.

Spelling out the U.S. government's position on the rules governing cyberwarfare, Harold Koh, the department's legal adviser, said a cyber-operation that results in death, injury or significant destruction would probably be seen as a use of force in violation of international law.

25 Comments
Weigh In | Corrections?

(Read Harold Koh's remarks here.)

In the United States' view, any illegal use of force potentially triggers the right of national self-defense, Koh said.

The Post Most: World

Most Popular

1. China's increasing military spending unnerves neighbors
2. Plan for hunting terrorists signals U.S. intends to keep adding names to kill lists
3. Email: State Department told White House militants claimed responsibility for Libya attack

The Law of Armed Conflict

- **Developed to govern a regime for peacetime and conflict spectrum**
- **United Nations Article 2 (4) "refrain in their international relations from the threat or use of force**
  - **2 exemptions –**
    - **security council authorizes use of force**
    - **self-defense**
- **Article 51 of the Charter provides:**
- **Nothing in the present Chapter shall impair the inherent right of individual or collective self defense if an armed attack occurs**

The Law of Armed Conflict

- **U.S. believes in an expansive interpretation of the UN Charter contending that the customary law right of self-defense (including anticipatory self-defense) is an inherent right of a sovereign State that was not "negotiated" away under the Charter.**
- **United States has not made a distinction between "use of force" and an "armed attack"**
  - ***See* William H. Taft, *Self-Defense and the Oil Platform Decision*, 29 Yale J. Int'l. 295, 300 (2004)**

The Law of Armed Conflict

- **Nondestructive insertion of a cyber capability into the computer system of another nation**
  - **use of force ?**
  - **an armed attack ?**
- **Such activities—without an accompanying intent for imminent action—would not be uses of force, so long as the cyber capability lies dormant**
  - **Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, Strategic Studies Quarterly (Spring 2011)**

The Law of Armed Conflict

- **Article 51, UN Charter governs relations between nation-states, not individuals.**
- **The DoD general counsel opines that when "individuals carry out malicious [cyber] acts for private purposes, the aggrieved state does not generally have the right to use force in self-defense." To do so ordinarily requires some indicia of effective state control of the cyber actors to impute state responsibility**
  - **Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, Strategic Studies Quarterly (Spring 2011)**

The Law of Armed Conflict

- **In testifying before the Senate Committee considering his nomination to head the new Pentagon Cyber Command, Lieutenant General Keith Alexander explained that "[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force.“ He went on to suggest, however, that "[i]f the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response.”**
  - **Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int’l L. 421**

The Law of Armed Conflict

- Combatants v noncombatants
- Military necessity
- Proportionality
- Superfluous injury
- Indiscriminate weapons
- Neutrality

Cyberwar & Law of Armed Conflict

Department of Defense Cyberspace Policy Report

A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934

November 2011

Department of Defense Cyberspace Policy Report

A Report to Congress
Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934

November 2011

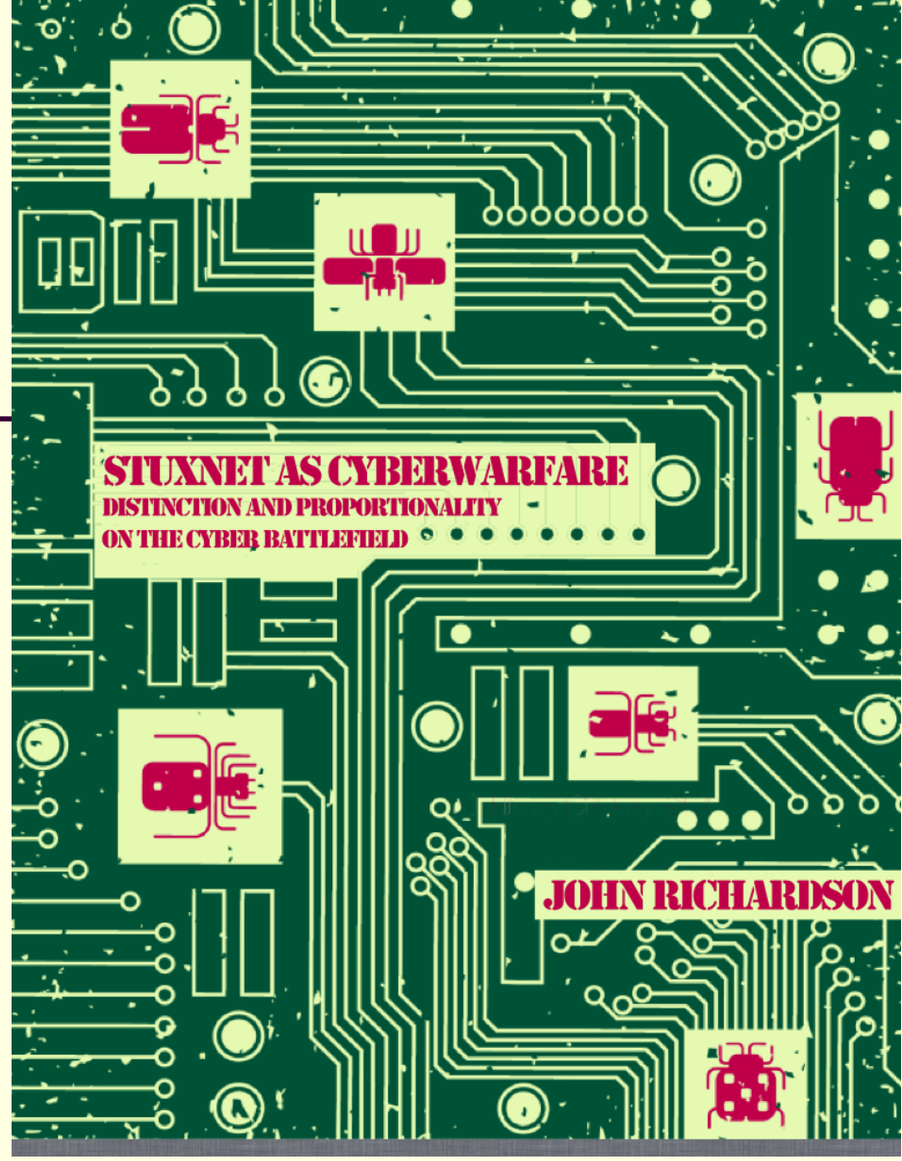
- **This report answers 13 specific questions from Congress.**
  - **http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf**

Department of Defense Cyberspace Policy Report

- **1. All states possess an inherent right to self-defense**
- **2. Reserves right to respond using all necessary means to defend our Nation . . . response options may include using cyber and/or kinetic capabilities**
- **4. International Strategy provides clear statement that US reserves right to use all necessary means - diplomatic, informational, military, and economic —to defend our Nation, Allies, partners, interests in cyberspace.**
- **5. Department seeks to prevent dangerous escalatory situations by the law of armed conflict.**
- **6. DoD has rules of engagement for the operation and defense of its networks**
- **7 Espionage ... long history .... practiced in both directions. United States Government collects foreign intelligence via cyberspace, and does so in compliance with all applicable laws, policies, and procedures.**
- **11. No international consensus regarding definition of "cyber weapon." LOAC provides strong basis to apply to cyberspace governing responsible state behavior.**
- **12. "act of war" and "threat or use of force," UN Charter and LOAC, apply to sea, air, land, and space, also apply to the cyberspace.**

Law of Armed Conflict Computer Network Attack - Anticipatory Self-Defense

Law of Armed Conflict
Computer Network Attack
Anticipatory Self-Defense



- **Issues – a few**
  - **Imminent Threat**
  - **Necessity**
  - **Proportional**
  - **Targeting**
  - **Use of Force**
  - **The Nuclear Age and WMD**
  - **El-Shifa Pharmaceutical Industries Company v United States, 378 F.3d 1346 (Fed. Cir. Aug 11, 2004)**

Personal Analysis & Opinion
Not US Government Position

The Law of Armed Conflict

- **LOAC requires commanders do everything feasible to ensure the target is a proper military objective.**
- **International courts have used the "reasonable commander" standard.**
- **Reasonably well informed person; in the circumstances of the actual commander; making reasonable use of the information available to him or her; and, concludes the target met the legal standards.**
- **As to degree of certainty, Schmitt offers a "clear and compelling standard" which is higher than the preponderance of evidence standard used in certain civil and administrative proceedings and lower than criminal law's beyond a reasonable doubt criterion.**
  - **Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwar*, Strategic Studies Quarterly (Spring 2011)**

The Law of Armed Conflict

- **Lieutenant General Keith Alexander explained that "[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force.“**
  - **Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int’l L. 421**

Debate Club

Should There Be an International Treaty on Cyberwarfare?

The Flame computer virus is the latest digital malware program uncovered in the escalating practice of large-scale cyberattack. Twenty times larger than its predecessor Stuxnet, the Flame virus infected computer systems throughout the Middle East. Analysts believe the Flame virus was designed for espionage purposes, some arguing that it then doesn't qualify as "cyberwarfare" (though Kapersky Lab, the Russian cybersecurity firm that uncovered the virus, said it does). However, the motive of 2010's Stuxnet was undoubtedly malicious. The virus infected Iranian nuclear enrichment facilities—which Iran insists are for peaceful purposes, but many believe are being used to develop nuclear arms—and derailed the operations of thousands of centrifuges at multiple Iranian plants. The *New York Times* recently reported that the United States, with the help of Israel, was behind Stuxnet in a mission code-named "Olympic Games." Government sources cited in the article refused to admit responsibility for the Flame virus, however Kaspersky Lab has linked Flame to Stuxnet.

The ambiguities of cyberwarfare worry international law experts, diplomats, and military commanders alike. What qualifies as an act of war versus espionage? Does the law of "proportionality"—that collateral damage to civilians in battle must not be disproportionate to the military target attacked—apply to cyberwar, especially since the line between civilian and military computer systems is not so clear? Should a cyberattack by a lone hacker be treated differently than that engineered by a national government? Thus some legal and cybersecurity experts have suggested that an international treaty, like those created to address the terms of conventional war, should be drafted to clarify the rules of cyberwarfare, a few even proposing an all-out ban on the practice. Others insist that such a treaty would be difficult to even draft, and impossible to enforce. Should there be an international treaty on cyberwarfare? Here is the Debate Club's take:

The Arguments

#1 31 Pts — 36 / 5

NO — A treaty would prevent countries from using this nonviolent weapon, leading to more human casualties

LAWRENCE L. MUIR JR., Computer Crime Prosecutor | Comment (1)

#2 8 Pts — 10 / 2

NO — Cyberespionage capabilities are evolving too fast for an unenforceable piece of paper to control them

JON LINDSAY, Research Fellow at the University of California Institute on Global Conflict and Cooperation at UC-San Diego. | Comment

#3 5 Pts — 8 / 3

NO — Even the most damaging cyberattack to date--Stuxnet--may not have been cyberwarfare

SEAN LAWSON, Assistant Professor at the University of Utah | Comment

#4 3 Pts — 3 / 0

NO — Restrictions on cyberweapons uneforceable, and could even harm cybersecurity

MARTIN LIBICKI, Author of 'Cyberdeterrence and Cyberwar' | Comment (1)

#5 0 Pts — 2 / 2

NO — A cybersecurity treaty would be unworkable

JAMES LEWIS, Director of the Technology and Public Policy Program at the Center for Strategic and International Studies | Comment

#6 -1 Pts — 7 / 8

YES — A treaty wouldn't completely stop cyberattacks, but it is a step in the right direction

BRUCE SCHNEIER, Security Technologist and Author | Comment (1)

#6 -1 Pts — 1 / 2

NO — World must first find common ground on how and when to seek what regulation of cyberwar is possible

HERBERT LIN, Chief Scientist of the Computer Science and Telecommunications Board of the National Research Council. | Comment

Active Defense - Hacking Back

- Self-Defense
- Beacons
- Dis-information

Computer Network Exploitation

- **Espionage**
  - **The practice of using spies to collect information about what another government or company is doing or plans to do.**
    - **Black's Law Dictionary 585 (9th ed. 2009)**

Computer Network Exploitation

- **Roger D. Scott, *Territorial Intrusive Intelligence Collection and International Law*, 46 A.F. L. Rev. 217 (1999)**
  - **Issue – under operational law is surreptitious spying in another nation's territory illegal?**

- **Facts –**
  - **No sabotage or other destructive acts**
  - **simply the collection of information**
  - **through various surreptitious, intrusive means**
  - **inside a foreign nation's territory**
  - **without that nation's knowledge or consent.**

Computer Network Exploitation

- **Roger D. Scott, *Territorial Intrusive Intelligence Collection and International Law*, 46 A.F. L. Rev. 217 (1999)**
  - **Traditional doctrinal view – spying in another's territory during peacetime is an unlawful intervention.**
    - **Lack of respect for –**
      - **Territorial boundaries of another sovereign**
        - **National airspace**
        - **Internal waters**
        - **Territorial seas.**

Computer Network Exploitation

- **Roger D. Scott, *Territorial Intrusive Intelligence Collection and International Law*, 46 A.F. L. Rev. 217 (1999)**
  - **Espionage may give rise to the use of force as well as a response under domestic criminal law.**
  - **Espionage by ships, submarines, or aircraft raise issues of national self-defense**
    - **Shoot down of U-2s over China and former Soviet Union**
    - **North Korean attack upon the U.S.S. Pueblo**
    - **Swedish government's use of depth-charges against Soviet submarines in Sweden's territorial sea**

Computer Network Exploitation

- **The lack of strong international legal sanctions for peacetime espionage may also constitute an implicit application of the international law doctrine called "*tu quoque*" (roughly, a nation has no standing to complain about a practice in which it itself engages). Whatever the reasons, the international legal system generally imposes no sanctions upon nations for acts of espionage except for the political costs of public denunciation, which don't seem very onerous.**

Computer Network Exploitation

- **Computer Network Exploitation**
  - **Typically no presence inside another's territory**
  - **Highly unlikely that the notions of "electronic presence" or "virtual presence" will ever find their way into the law of war concept of spying**
    - **Not physically behind enemy lines**
    - **No issue of acting under false pretenses by abusing protected civilian status or by wearing the enemy's uniform.**

Computer Network Security & Defense

- **Common Law**
  - **Trespass to Chattel**
  - **Statutory Law**

Computer Network Security & Defense

- Common Law Doctrine-Trespass to Chattel
- Cause of action for trespass
- Recover actual damages
- Suffered due to impairment of or loss of use of the property
- May use reasonable force to protect possession against even harmless interference
- The law favors prevention over post-trespass recovery, as it is permissible to use reasonable force to retain possession of a chattel but not to recover it after possession has been lost
- *Intel v. Hamidi,* 71 P.3d 296 (Cal. Sp. Ct. June 30, 2003

Computer Network Security & Defense

- **Right to exclude people from one's personal property is not unlimited.**
- **Self defense of personal property one must prove that he was in a place he had a right to be, that he acted without fault and that he used reasonable force which he reasonably believed was necessary to immediately prevent or terminate the other person's trespass or interference with property lawfully in his possession**
  - ***Moore v. State*, 634 N.E.2d 825 (Ind. App. 1994) *and* *Pointer v.* State, 585 N.E. 2d 33, 36 (Ind. App. 1992)**

Computer Network Security & Defense

- Privacy and Civil Liberties
- Log-on banners and user agreements
- Workplace policies and rules of behavior
- Computer training

Computer Network Security & Defense

- **Consent**
  - **Where there is a legitimate expectation of privacy, consent provides an exception to the warrant and probable cause requirement.**
  - **A computer log-on banner, workplace policy, or user agreement may constitute user consent to a search. *See United States v. Monroe*, 52 M.J. 326, 330 (C.A.A.F. 1999) (log-on banner stating "users logging on to this system consent to monitoring).**
  - **In the context of public employment, employee consent is valid only if it is limited to consent to reasonable searches. Thus, the underlying search still must be reasonable.**

Computer Network Security & Defense

- **Consent**
  - **Memorandum for Fred F. Fielding, Counsel to the President, subject: *Re: Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch* (January 9, 2009)**
  - **Memorandum Opinion for and Associate Deputy Attorney General, *Legality of Intrusion Detection System to Protect Unclassified Computer Networks in the Executive Branch* (August 14, 2009)**

Computer Network Security & Defense

- **Wiretap Statute: Rights or Property Exception**
- **18 U.S.C. § 2511(2)(a)(i)**
  - **A provider "may intercept or disclose communications on its own machines "in the normal course of employment while engaged in any activity which is a necessary incident to . . . the protection of the rights or property of the provider of that service."**
  - **Generally speaking, the rights or property exception allows tailored monitoring necessary to protect computer system from harm. *See U.S. v McLaren*, 957 F. Supp 215, 219 (M.D. Fla. 1997).**

Computer Network Security & Defense

Event Will Determine Response and Legal Authority

- Multiple disciplines
- Network Ops- CERTs/ NOSCs
- Intelligence
- Counterintelligence
- Law enforcement
- Government

- Computer Security Events
- Incidents
- Intrusions
- Attacks

The End