Legal Aspects of Cyberspace Operations

Black hat USA 2012

Agenda

- Cyberspace Operations
  - Computer Network Security & Defense
  - Computer Network Exploitation
  - Computer Network Terrorism
  - Computer Network Attack
  - Lawful Active Response - DoJ

Disclaimer

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 Law & Policy

Sources of Law

- Constitution
- § Statute
- International Law (Customary Law)

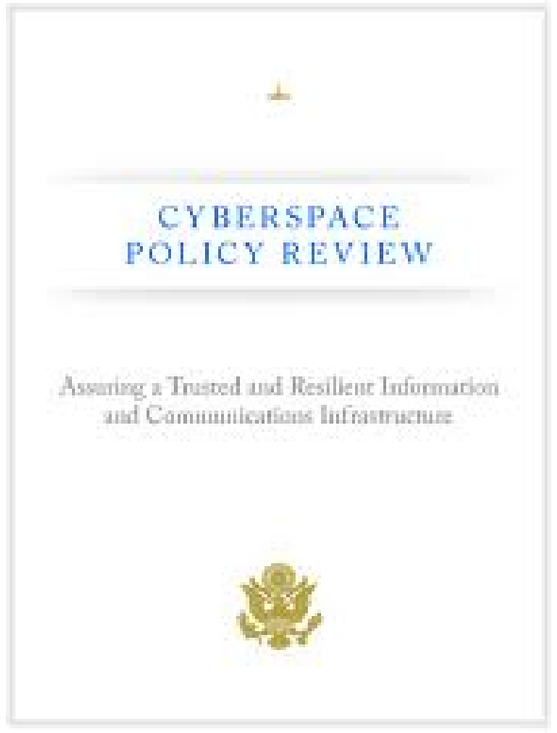
Sources of Policy

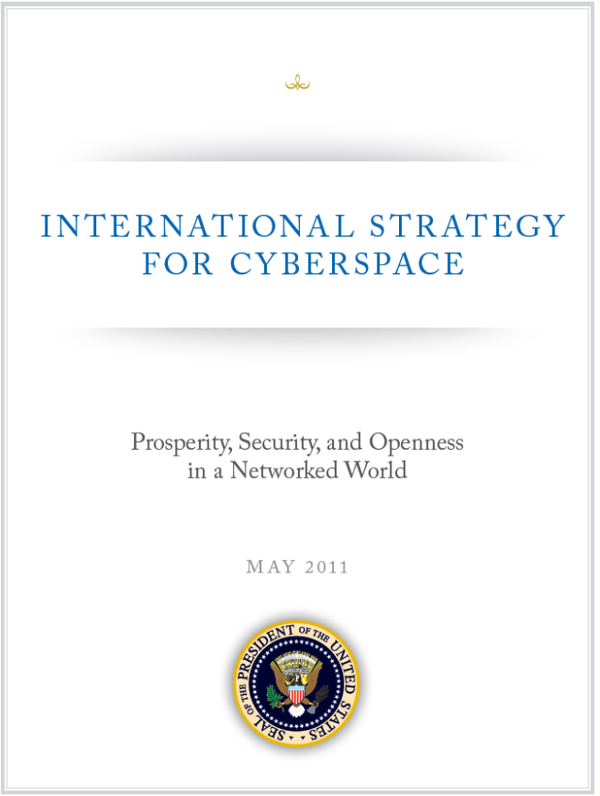
- Executive Order
- Presidential Directives
- Memoranda and Regulations

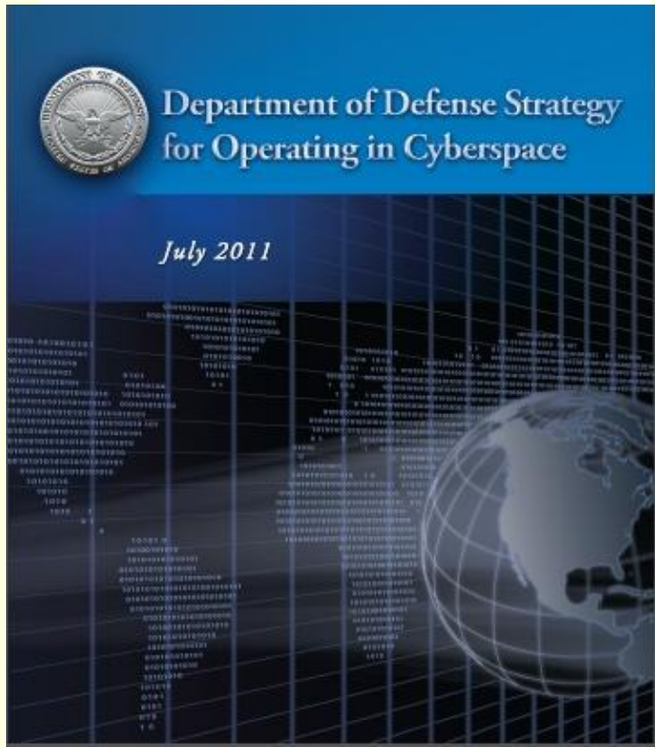
The National Security Policy Process: The National Security Council and Interagency System

The National Security Policy Process: The National Security Council and Interagency System
http://www.ndu.edu/icaf/outreach/publications/nspp/docs/icaf-nsc-policy-process-report-10-2010.pdf

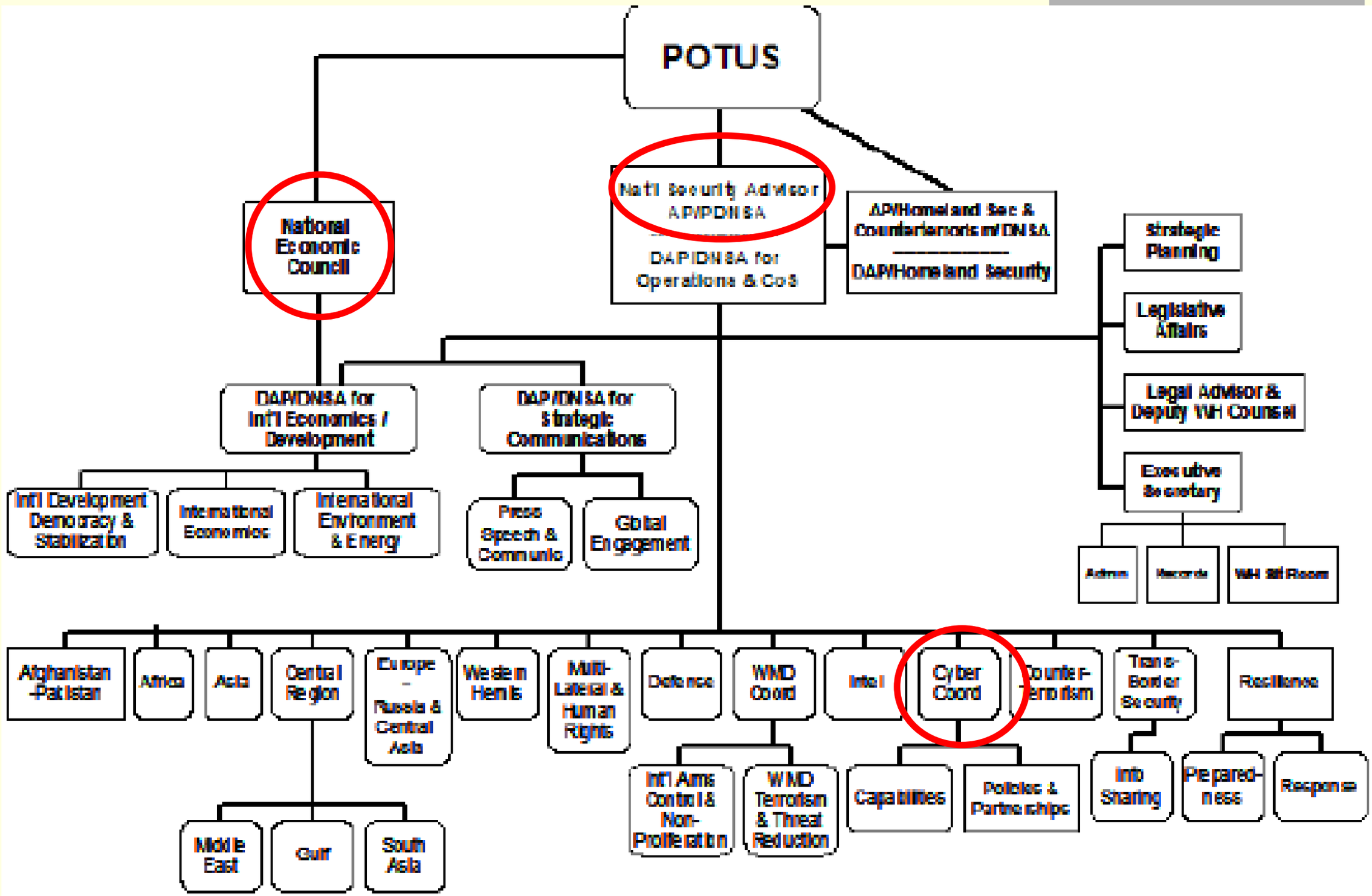
Cybersecurity Policy – top down







The National Security Policy Process: The National Security Council and Interagency System



Cyberspace Operations

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 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.**

What is Cyber-Terrorism?

- What would an act of cyber-terrorism look like?
- Do we know?
- Will we find out?

Developing a Definition of Cyber-terrorism

- **By adapting the definition of domestic terrorism that was created in 18 U.S.C. 2331 we can derive a working definition of "cyber-terrorism."**
- **In conventional terrorism cases, the difference between a homicide or an assault and terrorism is the motive or purpose of the attack.**
- **Similarly, what distinguishes cyber-terrorism acts from normal intrusion cases is largely the purpose for the attack. While this is theoretically what sets terrorism apart from other violent crime, you'll see that many of the federal statutes often don't explicitly refer to motive.**

Terrorism

- When is a cyberattack considered cyberterrorism
- Two views for defining the term cyberterrorism:
  - **Effects-based**. Cyberterrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals other than terrorists.
  - **Intent-based**. Cyberterrorism exists when unlawful, politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage

The Law of Armed Conflict

- **Is a computer network attack an 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**

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

- **In interpreting self-defense under Article 51, cyber strategists should keep in mind that the 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

- **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**

Legal Issues - Active Response

Hack Back – Legally!!

- ***United States v John Doe, et al.,*** **No. 3:11 CV 561 (VLB), Dt. Conn, June 16, 2011**
- **Coreflood**
- **Civil Complaint**
- **Execution of Criminal Seizure Warrants**
- **TROs**
- **Most comprehensive enforcement action by US authorities to disable an international botnet**

Hack Back

- ***United States v John Doe, et al.,*** **No. 3:11 CV 561 (VLB), Dt. Conn, June 16, 2011**
- **Civil Complaint against 13 "Doe" defendants**
- **Wire fraud**
- **Bank fraud**
- **Illegal interception of electronic communications**
- **Search Warrants throughout country**
- **29 Domain Names**

Hack Back

- *United States v John Doe, et al.*, No. 3:11 CV 561 (VLB), Dt. Conn, June 16, 2011
  - TRO
    - Authorizes government to respond to signals sent from infected computers in the United States
    - Stops Coreflood software from running
    - Prevents further harm to hundreds of thousands of unsuspecting users of infected computers in US
- "These actions to mitigate the threat posed by the Coreflood botnet are the first of their kind in the United States and reflect our commitment to being creative and proactive in making the Internet more secure."
  - Shawn Henry, Executive Assistant Director of the FBI's Criminal, Cyber, Response and Services Branch.

Hack Back

- ***United States v John Doe, et al.*, No. 3:11 CV 561 (VLB), Dt. Conn, June 16, 2011**
- **TRO**
- **"[T]here are special needs, including to protect the public and to perform community caretaking functions, that are beyond the normal need for law enforcement and make the warrant and probable-cause requirement of the Fourth Amendment impracticable"**
- **"the requested TRO is both minimally intrusive and reasonable under the Fourth Amendment."**

Hack Back

- ***United States v John Doe, et al.*, No. 3:11 CV 561 (VLB), Dt. Conn, June 16, 2011**
- **The Coreflood botnet**
- **Operated for nearly a decade**
- **Infected more than two million computers worldwide**
- **Steals usernames, passwords, other private personal and financial information for a variety of criminal purposes, including stealing funds from the compromised accounts.**
- **One example described in court filings, through the illegal monitoring of Internet communications between the user and the user's bank, Coreflood was used to take over an online banking session and caused the fraudulent transfer of funds to a foreign account**

Hack Back

- ***United States v John Doe, et al.*, No. 3:11 CV 561 (VLB), Dt. Conn, June 16, 2011**
- **The Coreflood botnet**
- **Five C & C servers seized**
- **29 domain names used to communicate with the C & C servers**
- **If C & C servers do not respond, the existing Coreflood malware continues to run on the victim's computer, collecting personal and financial information. TRO authorizes government to respond to requests from infected computers in the United States with a command that temporarily stops the malware from running on the infected computer.**

Hack Back

- ***United States v John Doe, et al.*, No. 3:11 CV 561 (VLB), Dt. Conn, June 16, 2011**
- **The Coreflood botnet**
- **Government's action limits defendants ability to control botnet**
- **Allows computer security providers time to update virus signatures and malicious software removal tools so victims have reliable tool available to removes latest version of malware**
- **Identified owners of infected computers will also be told how to "opt out" from the TRO, if for some reason they want to keep Coreflood running on their computers. At no time will law enforcement authorities access any information that may be stored on an infected computer.**