Strategy Research Project

CRIME OR WAR: CYBERSPACE LAW AND ITS IMPLICATIONS FOR INTELLIGENCE

BY

COLONEL BRYAN D. DeCoster
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
11-02-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

Crime or War: Cyberspace Law and its Implications for Intelligence

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Bryan D. DeCoster

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Deborah L. Hanagan
Department of National Security and Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Cyberspace is a relatively new dimension in national security that could eventually rival the land, sea, air, and space environments in importance. Since cyberspace is relatively new, existing international law does not directly distinguish between crimes and acts of war for activities in cyberspace. However, making the distinction between crime and war using existing law is essential in determining which of the multiple stakeholders takes the lead in preventing or responding to computer network attacks on United States government or private networks. This paper analyzes six basic sources of cyberspace threats in terms of existing law to determine which threats and their resulting cyberspace activities are matters for law enforcement as opposed to acts of war to be pursued by the Department of Defense. Additionally, the paper describes the implications for intelligence collection and analysis and proposes several imperatives for the intelligence community that result from the legal status and constraints existent in international law interpretations on use of force and armed attacks that can generally be applied to the cyberspace environment.

15. SUBJECT TERMS

Computer Network Attack, International Law, Intelligence Analysis

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	38	

USAWC STRATEGY RESEARCH PROJECT

CRIME OR WAR:
CYBERSPACE LAW AND ITS IMPLICATIONS FOR INTELLIGENCE

by

Colonel Bryan D. DeCoster
United States Army

Colonel Deborah Hanagan
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Bryan D. DeCoster

TITLE: Crime or War: Cyberspace Law and its Implications for Intelligence

FORMAT: Strategy Research Project

DATE: 11 February 2011 WORD COUNT: 6,356 PAGES: 38

KEY TERMS: Computer Network Attack, International Law, Intelligence Analysis

CLASSIFICATION: Unclassified

Cyberspace is a relatively new dimension in national security that could eventually rival the land, sea, air, and space environments in importance. Since cyberspace is relatively new, existing international law does not directly distinguish between crimes and acts of war for activities in cyberspace. However, making the distinction between crime and war using existing law is essential in determining which of the multiple stakeholders takes the lead in preventing or responding to computer network attacks on United States government or private networks. This paper analyzes six basic sources of cyberspace threats in terms of existing law to determine which threats and their resulting cyberspace activities are matters for law enforcement as opposed to acts of war to be pursued by the Department of Defense. Additionally, the paper describes the implications for intelligence collection and analysis and proposes several imperatives for the intelligence community that result from the legal status and constraints existent in international law interpretations on use of force and armed attacks that can generally be applied to the cyberspace environment.

CRIME OR WAR: CYBERSPACE LAW AND ITS IMPLICATIONS FOR INTELLIGENCE

> Our Nation's growing dependence on cyber and information-related technologies, coupled with an increasing threat of malicious cyber-attacks and loss of privacy, has given rise to the need for greater security of our digital networks and infrastructures. In the Information Age, the very technologies that empower us to create and build also empower those who would disrupt and destroy.[1]
>
> —President Barack Obama

This statement by President Obama highlights current national security concerns with cyberspace, which is "a global domain…consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[2] In 2003, President Bush published "The National Strategy to Secure Cyberspace" and, in 2009, President Obama directed a 60-day review of cyber-security strategy which resulted in a policy review document.[3] Both documents recognized that cyberspace was a new domain in national security with complex legal issues and network vulnerabilities, especially in the nation's critical infrastructure.[4] Since cyberspace is relatively new, existing international law does not directly distinguish between crimes and acts of war for activities in cyberspace. However, making the distinction between crime and war is essential in determining which of the multiple stakeholders takes the lead in preventing or responding to computer intrusions on United States (US) government or private networks.

Part of the challenge in making legal distinctions is defining the evolving terminology related to cyberspace. This paper uses the definitions accepted in joint doctrine with some minor modifications. Computer intrusions are "incident[s] of unauthorized access to data or an automated information system"[5] or networks by state

and non-state actors. Computer intrusions take two forms: computer network exploitation and computer network attack. Computer network exploitation (CNE) is "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[6] Computer network attacks (CNA) are "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[7] While CNE and CNA tools are similar, CNE is usually done with the intent for espionage, while CNA is done for profit, sabotage, or other harm.[8]

According to General Keith Alexander, commander of US Cyber Command (USCYBERCOM), "[t]here is a real probability, that in the future, this country will get hit with a destructive [cyber] attack, and we need to be ready for it."[9] Imagine the following scenario as an example of such an attack. It is 2012 and the United States has just fallen victim to a cyber-worm designed to precisely target the supervisory control and data acquisition (SCADA) systems of nuclear power facilities and cause physical harm by shutting down reactor cooling systems. The worm infected 20 nuclear facilities, with two of the facilities experiencing temporary cooling system failures, resulting in 15 deaths and 80 injuries before the damage could be contained. Attribution has been elusive, with the worms being traced back to computers in the United States, India, and Pakistan, but intelligence officials suspect Iran of being behind the worm as retaliation for a 2010 CNA against Iranian nuclear facility centrifuges.

A post-attack intelligence review by the Office of the Director of National Intelligence (ODNI) revealed several data points that were never shared nor connected.

The Central Intelligence Agency (CIA) estimated Iran had intent but insufficient capability for CNA. The National Security Agency (NSA) conducted network analysis that showed contacts between Iranian intelligence officials and a Russian hacker web-site also associated with terrorist and criminal groups. The Department of State (DoS) had a human intelligence (HUMINT) report of a highly skilled Russian hacker traveling to Iran two weeks prior to the attack. At this point in time, USCYBERCOM and the federal government remain unclear on how to respond since attribution and the legal status of the attack, whether it was a criminal act or an act of war, remain unclear.

This paper examines the law concerning cyberspace and analyzes six basic sources of cyberspace threats in order to propose which threats and their resulting computer intrusions are criminal as opposed to acts of war. It then describes the implications for intelligence collection and analysis that result from this legal and threat environment in order to propose several imperatives for the intelligence community that could help prevent scenarios like the one described above.

Existing Law and Stakeholders Regarding Cyberspace Activities

There are differing opinions on the applicability of current international law to cyberspace. Some scholars and lawyers argue that there are “no common, codified, legal standards regarding cyber aggression” and “current international law is not well suited for cyber-attacks.”[10] Others argue “that a considerable body of international law applies to the use of force by states in cyberspace.”[11] One has only to apply the general international laws on the use of force by analogy to determine whether a computer intrusion is “simply a crime committed by a non-state actor or an unlawful use of force by a state under international law.”[12] Advocates of the need for new international laws to directly address computer intrusions argue that applying law by analogy to cyberspace

is currently necessary but flawed for several reasons, to include: translation problems; exclusion of non-state actors; and applicability of cyberspace to multiple overlapping legal regimes.[13] This paper uses the law by analogy argument since it appears to be the most generally accepted method despite its limitations.

So what international law is applicable by analogy? What constitutes an act of war in cyberspace? Making a legal distinction between crime and war is complicated due to the lack of accepted international definitions for key terms of aggression such as: act of war, armed conflict, use of force, and armed attack. International laws and treaties, to include the United Nations (UN) Charter, do not clearly define these terms of aggression.[14] In general, an act of war is any use of force occurring in the course of armed conflict. However, to apply this to cyberspace requires further examination of what international law states about the use of force, armed attack, and armed conflict.

Article 2(4) of the UN Charter prohibits the "use of force" against another state.[15] For the purposes of this paper, use of force is defined as "a state activity that threatens the territorial integrity or political independence of another state."[16] Customary international law prohibits a state from using force for retaliatory or punitive actions but allows using force in self-defense to deter future aggression. Article 51 of the UN Charter recognizes this right of a state to self-defense against an "armed attack."[17] For the purposes of this paper, armed attack is defined as "a use of force that rises to a certain scope, duration, and intensity threshold."[18] UN General Assembly Resolution 3314 provides examples of aggression that constitute armed attack, but they are traditional lethal examples as opposed to the non-traditional activities of cyberspace.[19] According to Common Article 2 of the four Geneva Conventions of 1949, armed conflict

exists upon: formal declaration of war; occupation of a state; or any other armed conflict between states even if war was not formally declared.[20]

To summarize and apply these terms, short of a formal declaration of war or occupation, armed conflict exists when one state conducts a use of force against another state which is of a scope, duration, and intensity that qualifies it as an armed attack.[21] Essentially, a use of force that meets the threshold of an armed attack qualifies as armed conflict and, under Article 51, triggers the right to self-defense.[22] Using law by analogy, a computer intrusion by one state on another state's computer network may qualify as a use of force if it threatens the territorial integrity or political independence of the state. If a state determines that another state's computer intrusion meets the threshold of an armed attack, the intrusion could also be considered armed conflict and an act of war.

The key distinction is the scope, duration, and intensity threshold for an armed attack. There is a requirement for legal analysis on a case by case basis to determine which computer intrusions meet the threshold for an armed attack.[23] Essentially, lawyers must study state practice and international precedent to make legal determinations, applying existing law by analogy. In order to determine whether a state's computer intrusion is an act of war, there is a requirement for a legal interpretation that concludes "an activity not traditionally considered an armed attack [computer intrusion] is used in such a way that it becomes tantamount in effect to an armed attack."[24] There are several proposed frameworks that lawyers can use to determine when a computer intrusion equates to armed attack, to include: the Schmitt framework, which applies seven factors beyond scope, duration, and intensity; and the Libicki framework, which

categorizes armed attacks into groupings which are universally, multilaterally, or unilaterally accepted within the international community.[25]

Regardless of the framework applied, it seems to be generally accepted through law by analogy that a CNA conducted by a state which causes physical damage to another state's assets would meet the threshold for unlawful armed attack unless conducted in self-defense or as part of a UN-sanctioned operation.[26] CNA used in self-defense under UN Charter Article 51, or as part of a UN-sanctioned operation, is legal as long as the principles of the Law of Armed Conflict are followed.[27] However, even if in self-defense, a CNA conducted by a state with the intent to cause physical damage to "works or installations containing dangerous forces, namely dams, dikes and nuclear electrical generating stations," would appear to be an unlawful armed attack under the 1977 Geneva Protocol I, Article 56.[28] For example, the CNA on US nuclear power plants described in the opening scenario would be considered an unlawful armed attack if it could be attributed to a state.

At this point, it is important to note two additional limitations in international law. First, CNE would not generally meet the standard of a use of force or an armed attack. In 1960, the UN Security Council concluded that a U-2 reconnaissance flight by the United States over Soviet territory was not a use of force under UN Charter Article 2(4). Using this precedent by analogy, the "virtual penetration of a state's cyberspace" for reconnaissance (i.e. CNE) also does not constitute a use of force under UN Charter Article 2(4).[29] While CNE and espionage do not violate international law, they could be prosecuted as criminal activity if the domestic law of the state in which it occurs outlaws such activity.[30] Second, international law and treaties, to include the UN Charter, apply

to state-on-state conduct and exclude non-state actors. Therefore, in order to make a legal determination that a CNA qualifies as an armed attack, it must be attributed to a state. As was evident in the example scenario, attribution for computer intrusions is extremely difficult; even if attributed to an individual, proving that individual was acting in an official capacity for a state is doubly difficult.[31]

As noted above, CNE and the computer intrusions of non-state actors, to include CNA, could constitute crimes rather than acts of war, unless a UN resolution or other international convention were to specifically sanction military operations against non-state actors conducting CNA. CNE and the computer intrusions of non-state actors are customarily left to domestic law enforcement agencies or to states for resolution. A state's response against a non-state actor is a "law enforcement issue that must, at least at present, be principally addressed through cooperative bilateral and multilateral extradition and mutual legal assistance treaties."[32]

Domestically, the Computer Fraud and Abuse Act (CFAA) is the principal US law addressing Internet-related computer crime.[33] The CFAA prohibits unauthorized access to a protected computer or gaining and using information in a manner exceeding authorized access. Robert Morris, a Cornell University computer science student, was the first person convicted under this act in 1990 when he released a virus that affected hundreds of educational and military computers during the early stages of the Internet.[34] Additionally, the United States has indicted criminals for using, maintaining, and selling botnets, which are networks of robotic internet devices that control other computers without the user's knowledge.[35] The use of botnets can be prosecuted as civil trespass but the plaintiff must establish damages as well as trespass in cyberspace.[36] There are

also copyright laws protecting companies from cyber-theft. The Digital Millennium Copyright Act protects companies that encrypt trade secrets from hackers who would try to circumvent the company's encryption or digital locks.[37]

These US laws apply to both US and foreign citizens, but prosecution of foreign citizens is more difficult because it requires recognition of the law and the right to extradition by another state. Prosecution of cyber-crimes that cross state borders, enforcement of national criminal judgments, and extradition of cyberspace criminals are complicated since "there is no international treaty for enforcement of judgments or any Convention providing for extraterritorial Internet enforcement."[38] Some nations have weak governments, security forces, and/or law enforcement agencies and would have difficulty capturing and extraditing criminals.

Most nations have different laws and some nations have no laws regarding cyberspace activities. For example, France made it a crime for an internet service provider (ISP) to "give access to or possess Nazi memorabilia" while China required Yahoo to "filter materials critical of the Communist party regime as a condition of access to Chinese markets."[39] Both of these national rulings are at odds with US rulings on First Amendment rights and cause conflicts in Internet governance since many of the ISPs are American-based. An Israeli citizen who hacked into the Rome Lab, a US military research and development laboratory, multiple times in 1994 was not prosecuted because there were no Israeli laws recognizing this as a crime.[40] In 2000, a Filipino hacker was not prosecuted for his "I Love You" virus, which infected over 60 million computers worldwide, again because there were no laws against this cyberspace activity in the Philippines.[41]

There has been some recent international progress in trying to address these difficulties in accountability for cyber-crimes. Thirty-three countries, including the United States, have signed the Council of Europe's Convention on Cybercrime (CoECC) published in November 2001.[42] The Convention "seeks to better combat cybercrime by harmonizing national laws, improving investigative abilities, and boosting international cooperation."[43] Critics of the Convention point out, however, that it will be ineffective as long as the signatories do not include nations where criminals and terrorists operate freely.[44] The UN Secretariat has also recently established a Working Group on Internet Governance (WGIG) to study and make proposals for Global Internet Governance.[45]

A final complicating factor in this examination of when cyberspace activities qualify as crime versus war relates to the key stakeholders involved. There are many stakeholders with varied and often competing interests and authorities. This further complicates the environment and makes the formulation of consistent, unified responses against cyberspace activities challenging.

Internationally, key stakeholders include: multilateral cooperative organizations like the UN, CoECC, North Atlantic Treaty Organization (NATO), and International Criminal Police Organization (INTERPOL); non-governmental organizations (NGO); states; and non-state actors. Through its Security Council and General Assembly resolutions, the UN may sanction a state or non-state actor for a CNA that constitutes an armed attack or authorize military actions against state and non-state actors conducting CNA. NATO also has the authority to determine when a CNA on one of its member states constitutes an armed attack. For example, in 2007 NATO determined a CNA against Estonia did not trigger Chapter 5 thresholds requiring a NATO response

against an attack on a NATO member.[46] INTERPOL and the CoECC are focused on cooperation against cyber-crime. Some NGOs are very focused on privacy rights and argue against cyber-security measures that improve attribution methods on the Internet. State actors have varied interests; some want to advance cooperation against computer intrusions and cyber-crime, while others tend to exploit difficulties in attribution by employing covert non-state actors to perform their CNE and CNA. Non-state actors can act individually or in support of states when conducting computer intrusions.

Domestically, key stakeholders include: agencies of the Executive Branch such as the National Security Council (NSC), the Department of Defense (DoD), the Department of Homeland Security (DHS), the Secret Service, the Department of Justice (DoJ), the Federal Bureau of Investigation (FBI), the Federal Trade Commission, DoS, ODNI, CIA, NSA, and USCYBERCOM; members of Congress; NGOs and lobbyists; private companies; and governments and courts from federal to local level. The NSC advises the president on policy decisions, while Congress, state, and local governments pass laws related to cyberspace activities. Courts make rulings on law regarding cyberspace activities at all levels. NGOs and lobbyists have varied interests from advocating privacy rights to increased federal regulation of cyber-security. Private companies own 85% of the nation's infrastructure, including the digital infrastructure, and are therefore invested in their own cyber-security.[47]

Based on law and policy, acts of war in cyberspace involve DoD, ODNI, CIA, NSA, USCYBERCOM and potentially DHS, while cyber-crimes involve DHS, Secret Service, DoJ, FBI, and the Federal Trade Commission.[48] DHS is responsible for focusing on protection of government agency and private information systems to include

reducing and consolidating external access points, deploying passive network sensors, and defining public and private partnerships. DHS is also the focal point for efforts to protect the nation's computer-reliant critical infrastructure.[49] DoD is responsible for protecting military information systems to include monitoring, increasing security of classified networks, and deploying intrusion prevention systems. ODNI is responsible for monitoring intelligence community information systems and other intelligence-related activities, including the development of a government wide cyberspace counterintelligence (CI) plan.[50]

Sources of Threats and Their Status Under Law

Having examined the law on cyberspace and key stakeholders, this paper will now describe the basic threats in cyberspace and their general status under the law. There are six basic sources of threats: foreign nations, criminal groups, hackers, hacktivists, disgruntled insiders, and terrorists.[51]

Foreign nations would appear to have the most robust cyberspace means and capabilities at this time. It is estimated that "over 120 countries already have or are developing computer attack capabilities."[52] Most of these countries are focused on CNE or using cyberspace tools as part of their intelligence and espionage activities.[53] According to the ODNI, the majority of computer intrusions originate in Russia and China, and both nations have large efforts focused on CNE and CNA.[54]

The CNE activities of foreign nations fall into the criminal category under existing law and are more common than CNA. CNA by foreign nations is generally accepted as the most dangerous threat to US computer networks.[55] As previously discussed, CNA could rise to the level of an armed attack based on scope, duration, and intensity.

Essentially, a CNA that causes physical damage could equate to an armed attack. The primary difficulty, however, is attributing that armed attack back to a foreign nation.

There are several historical examples of CNA believed to have been launched by foreign nations. In 1999, the Indonesian government was generally blamed for what might have been the first reported state-on-state CNA when non-governmental computers in Ireland were attacked, bringing down the East Timor virtual country domain and internet service to over 3000 customers.[56] In April and May of 2007, Estonia was the target of the "first-ever coordinated cyber-attack against an entire country."[57] Estonia's digital infrastructure suffered extensive distributed denial of service (DDOS) and botnet attacks that adversely effected its banking and government operations and denied basic access to ISPs.[58] In August 2008, the country of Georgia experienced extensive CNA used in conjunction with military attacks. As Russian troops were moving into South Ossetia, Georgia's digital infrastructure and government web sites experienced DDOS attacks, web defacement, and disinformation and propaganda attacks intended to paralyze the government response.[59] In June 2010, several countries discovered the first precision CNA intended to cause physical harm to infrastructure in the form of a cyber-worm known as "Stuxnet." This cyber-worm targeted, infiltrated, and took control of specific SCADA software "used to run chemical plants and factories as well as electric power plants and transmission systems worldwide."[60] The worm was estimated to have infected at least 45,000 industrial control systems worldwide and may have been specifically designed to target centrifuges at the Bushehr Iranian nuclear facility.[61]

Debate continues in each case over whether there was sufficient physical damage and/or attribution to qualify the CNA as armed attacks by a foreign nation.[62] Attribution of a CNA to a foreign government is complicated because it is difficult to trace the connection between an individual hacker and a government. Furthermore, some nations may attempt to use an IP address that attributes the CNA to another nation or individual (i.e., they engage in false flag operations).[63]

Criminal groups, by the nature of their intent, fall into the category of cyber-crime. These groups conduct computer intrusions for profit, and cyber-crime will continue to expand as long as it remains lucrative.[64] Criminal groups target personally identifiable information (PII) on individuals and proprietary information from private companies in order to gain unauthorized access to credit and bank accounts, run scams, or sell information to the highest bidder. In some cases, these groups seize SCADA controls for extortion, forcing the private company to pay a fee to regain control of important functions.[65] Criminal groups also market and sell the tools for crime like botnets, spiders, and zombie computers.[66]

Hackers comprise a wide category of individuals who often conduct CNE and CNA for thrills or bragging rights.[67] In the past, hackers required exceptional skill, but the proliferation of attack scripts and protocols from the Internet available for download on hacker websites has made hacking easier. In general, “attack tools have become more sophisticated and easier to use.”[68] Hackers generally fall into the category of cyber-crime and are increasingly co-opted and paid for by criminal groups for their services. Hackers can also be co-opted by foreign intelligence services to perform CNE or CNA when a nation wants to prevent attribution. It is feasible that a hacker could

conduct a CNA that rises to the level of an armed attack, but he would have to be pursued on a criminal basis unless attribution to a foreign nation could be proved. This would be the case from the opening scenario if the CNA were attributed to the Russian hacker and not the Iranian government.

There are hundreds of hackers conducting computer intrusions each day. The previously cited example of Robert Morris is a typical example of a hacker. In February 1998, two California teenagers and an Israeli teenager conducted CNA on DoD computers in intrusions known as "Solar Sunrise."[69] In 2003, a hacker used the "Slammer" worm to corrupt the safety monitoring systems of a nuclear power plant in Ohio for five hours via a backdoor through the Internet.[70] Another hacker's worm, known as "MS Blast" or "Blaster," was reportedly linked to the major power outage that hit the northeast United States in August 2003, where it "crippled key detection systems and delayed response during a critical time."[71] While these computer intrusions by hackers took significant money, time, and other resources to fix, none rose to the level of an armed attack.

Hacktivists are individuals or groups who conduct politically motivated computer intrusions. They normally use DDOS attacks or modify publicly accessible web pages or e-mail servers to send a political message.[72] Hacktivists fall into the criminal category. Russian hacktivists, incensed by Estonia's plan to move a Russian soldier monument, were involved in the CNA on Estonia in 2007. In the case of Estonia, the energized hacktivists made attribution for the attacks even more difficult than usual, possibly providing an effective smokescreen for Russian government operatives.[73]

Disgruntled insiders can work from within an organization to conduct computer intrusions. Their existing access and knowledge of the computer network makes it easier to cause damage to or steal data from the system.[74] Insiders are often involved in criminal activity for profit, whether directly through embezzlement or indirectly by passing information to criminal groups. For example, in 2001, two accountants working for Cisco Systems used their access to company computer systems to "illegally issue almost $8 million in Cisco stock to themselves."[75] Insiders, even if recruited by a foreign intelligence service to conduct espionage, fall into the criminal category.

Like hacktivists, terrorists are also individuals or groups who conduct politically motivated computer intrusions. The main difference, however, is the terrorist intent for violence. US law defines terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents."[76] As previously discussed, since international laws, treaties, and conventions generally only recognize states, terrorists normally fall into the criminal category unless a specific UN resolution has sanctioned military operations against a terrorist group.

Cyber-terrorism is "the use of computers as weapons, or as targets" by terrorists.[77] Terrorists use the Internet extensively, but to this point "not for offensive actions."[78] Most computer intrusions by terrorists fall in the realm of CNE intended to gather information for potential future lethal attacks. To date, there has been no published linkage of a CNA to a terrorist group.[79] In general, it would be very difficult to label a CNA as cyber-terrorism because of the difficulty in determining attribution and intent.[80]

General Alexander does not see terrorist groups as a major CNA threat currently, but that could change.[81] Nations on the DoS list of states that sponsor terrorism generated less than 1% of all reported computer intrusions in 2002.[82] Al Qaeda has used the Internet extensively to network its strategic communications to other terrorist groups and recruit disciples. Furthermore, Al Qaeda computers captured in Afghanistan had extensive data on dam controls and methods to potentially cause catastrophic failure of infrastructure control systems, showing planning and intent for future terrorist attacks.[83] Although terrorist groups might not have extensive CNA capabilities currently, they could obtain the required expertise in several ways: sending true believers to cyberspace schooling; trying to convert hackers to their cause; or paying criminal groups or hackers to execute their attacks by proxy.[84] By coordinating a proxy CNA with a physical terrorist attack, terrorist groups could feasibly degrade a state's ability to respond.[85]

Implications for the Intelligence Community

Leaders, policymakers, and other stakeholders have many complex decisions to make regarding cyberspace. This section will highlight two that evolve from the preceding analysis of cyber law and sources of threats. First, they must decide what level of risk is acceptable in cyber-security based on the threat. Second, they must determine how to respond to CNE and CNA. A key role of the intelligence community is to facilitate these decisions. Having examined existing law, the sources of threats, and their status under law, what are the implications for the intelligence community in fulfilling this role? This paper proposes five imperatives that evolve from the previous

analysis and which are important for the intelligence community to internalize in order to support these key decisions.

The first imperative is that legal advisors must be embedded in intelligence organizations undertaking computer network operations. As previously stated, computer intrusions often fall into a gray area between crime and war requiring a case by case legal analysis using law by analogy. Intelligence organizations conducting cyberspace activities need lawyers for several purposes.

First, the lawyers can assist with legal determinations on which computer intrusions meet the threshold for an armed attack. These computer intrusions will generally fall under the purview of DoD or the CIA who make recommendations to the president and then execute appropriate foreign intelligence collection, covert action, or military responses. Computer intrusions that do not meet the armed attack threshold may be passed to the DoJ, DHS, or other domestic stakeholders for action if they qualify as crimes or relate to domestic terrorism or security concerns.

Second, legal expertise on intelligence law is necessary to ensure intelligence agencies are operating legally within their established authorities. For example, DoD intelligence agencies have limitations on the collection, retention, and dissemination of information on US persons as established by US Code Title 50 Chapter 36, Executive Order 12333, and DoD Directive 5240.1-R. Agencies with domestic intelligence authorities have corresponding restrictions on foreign intelligence collection, retention, and dissemination. There are additional limitations on authorities and collection methods existing in various other domestic intelligence laws and policies such as: the

Foreign Intelligence Surveillance Act, Electronic Communication Privacy Act, the Patriot Act, Stored Communication Act, and Economic Espionage Act.[86]

Third, any organization that will conduct CNA will require legal expertise on the Laws of Armed Conflict (LOAC) to understand how the principles of military necessity, unnecessary suffering, proportionality and discrimination of military targets from civilian sites apply in cyberspace.[87] In the opening scenario, USCYBERCOM would require a legal determination of an armed attack based on attribution and intent in order to respond. The appropriate response would be tested against the LOAC.

The second imperative is that intelligence must clearly quantify threat capabilities, intent, and vulnerabilities to facilitate the decisions of key stakeholders. One of the mission objectives of the US National Intelligence Strategy (NIS) is to "enhance cybersecurity."[88] The NIS further emphasizes that one of the ways the intelligence community does this is "by expanding our knowledge of the capabilities, intentions, and cyber vulnerabilities of our adversaries."[89]

As stated above, stakeholders must decide what level of risk is acceptable in cyber-security based on the threat. In order to do this, they must understand the threat's capabilities and intent. The United States has a diverse set of networks that vary from separate and secure classified DoD networks to Internet-based, privately-owned, critical infrastructure networks. Understanding the threat's cyberspace capabilities against the various networks in the United States and their intent for using those capabilities helps guide stakeholders' decisions on what security measures to take for networks as well as the amount of federal regulation required for the nation's critical infrastructure. The United States may be able to partner with nations or groups that possess cyberspace

capabilities but no harmful intent in order to establish international norms and standards for cyber-security. Limited resources and security measures are necessary to defend against threats with harmful intent but no cyberspace capabilities. In this case, the United States can focus its intelligence to ensure the threat does not partner with another to gain cyberspace capabilities to match its intent. For example, in the opening scenario the United States should have focused its intelligence collection on any attempts by Iran to gain CNA capabilities. A threat that possesses both intent and capability requires the highest security measures, federal regulation, and priority intelligence monitoring.

In deciding how to respond to a computer intrusion, intelligence can provide decision makers with a better understanding of the threat's intent and vulnerability. Understanding the threat's intent (i.e. CNE versus CNA) makes a difference in the US response. If the United States decides to respond in kind, understanding the adversary's cyberspace vulnerability becomes important. A comprehensive CNA on US infrastructure would require extensive planning and preparation.[90] This amount of preparation, surveillance, and testing is vulnerable to detection if intelligence is sufficiently focused and persistent in determining capabilities and intent.

As previously stated, determining attribution is very difficult. However, attribution is precisely what decision makers need from intelligence for both prevention and response. The NIS emphasizes that the intelligence community further enhances cyber-security "by increasing our ability to detect and attribute adversary cyber activities."[91] Decision makers need attribution for suspicious computer intrusions and CNE to proactively determine the true nature of the threat, defend networks, and prevent

potential escalation to CNA. Decision makers also need attribution for CNA to determine the status of the threat and attack under law and the appropriate response. In the opening scenario, USCYBERCOM could have made a recommendation on the appropriate response if attribution of the CNA was clear.

This problem of attribution contributes to the third intelligence imperative, which is that network analysis is important in order to determine the true source of the threat. While certain members of the intelligence community have made great progress in using network analysis methods, progress is sporadic across the community as a whole.[92] The intelligence community, whether associated with military or law enforcement organizations, should be investing in data mining and link analysis technologies and training. Data mining is generally used to determine anomalies while link analysis finds commonalities.[93] These network analysis technologies can exploit large amounts of data and have proven to be powerful tools in determining affiliations and linkages while also highlighting the absence of linkages. For example, scientists at the Massachusetts Institute of Technology conducted an experiment in which they were able "to use network analysis to determine the sexual orientation of Facebook users even though these users had not disclosed their preferences publicly."[94]

Hackers conducting computer intrusions have social networks that can be charted and analyzed to effectively determine their linkages. The linkages could turn up associations with other hackers, hactivists, and insiders, or in some cases criminal groups, terrorists, or foreign government agents directing the activity. For example, in the opening scenario, NSA successfully employed network analysis to determine Iranian government and Russian hacker associations. An absence of key linkages is

also important because it can indicate an individual is less of a threat and not directed by criminal groups, terrorists, or a foreign nation.

Intelligence analysts can focus on key indicators that can be tracked through network analysis. As previously noted, terrorist groups are making extensive use of the Internet for strategic communications and recruiting but appear to have limited CNA expertise. There are a limited number of hackers with high-level expertise. Monitoring the social networks and movement of these individuals can indicate when a foreign nation, terrorist or criminal group is recruiting a hacker for training, preparation, or an actual attack.[95] For example, in the opening scenario, the HUMINT report on the Russian hacker's travels should have triggered further intelligence collection to confirm the hacker's activities in Iran. Studies have shown that terrorist and criminal groups share technology and expertise for reasons more related to profit and gaining operational capability than ideological similarities.[96] Analysts can monitor hacker and terrorist chat rooms and web sites to determine linkages between the two and their potential sharing of technology and expertise.[97]

The fourth intelligence imperative is that an all-source approach is necessary. This is directly tied into the problem of attribution and network analysis. Because cyberspace resides in the signals intelligence (SIGINT) discipline, it would be very easy to look at this solely as a SIGINT problem. However, telephony and computers do not have all the answers. Individuals with expertise in computer intrusions also generally have expertise conducting those intrusions in a way that electronically attributes the intrusions to another individual's computer using botnets. Thus, it would be very easy to make a false attribution using single-source SIGINT. Bringing other intelligence

disciplines into the analysis should help capture such inconsistencies, as well as possibly show linkages not seen through SIGINT. In fact, the NIS specifically emphasizes the need to integrate CI with cyberspace to protect critical infrastructure.[98] All intelligence disciplines can be used for collection on both foreign and domestic threats. The collection must be done by the intelligence agencies with the correct foreign or domestic collection authorities under legal advice as discussed in the first intelligence imperative.

An all-source approach complicates the technology aspect of network analysis because HUMINT, imagery intelligence (IMINT), and CI come in various information formats that differ significantly from SIGINT. Data mining and link analysis technologies generally have limitations in handling non-structured formats that combine different types of information, like text and video. However, there have been significant advances in tagging these formats for data mining, and the intelligence community needs to continue to develop this capability in order to provide more comprehensive network analysis. In the opening scenario, better tagging of HUMINT may have allowed for its integration with SIGINT during network analysis to connect the dots on the Russian hacker-Iran connection.

The fifth imperative is that intelligence sharing must be improved both within the intelligence community and with key stakeholders. Having just highlighted the importance of a comprehensive all-source intelligence approach, it is crucial to share intelligence between the multiple stakeholders involved in order to improve detection and attribution. Additionally, intelligence sharing is especially important to get domestic and foreign intelligence into the hands of those intelligence agencies and stakeholders

with the correct legal authorities for response as noted in the first imperative. The opening scenario highlighted problems with information sharing since the CIA's assessment of Iran as having intent with no capability was not informed by the SIGINT from NSA and HUMINT from DoS. The NIS recognizes this imperative with enterprise objectives to "strengthen partnerships" and "improve information integration and sharing."[99] According to the Comprehensive National Cybersecurity Initiative (CNCI), ODNI has responsibility to "connect current cyber centers to enhance cyber situational awareness and lead to greater integration and understanding of the cyber threat."[100]

Activities like the Cyber Storm series of exercises conducted by DHS have improved intelligence sharing with 13 countries, 11 states, and seven cabinet-level federal agencies which participated in the latest Cyber Storm III exercise.[101] However, there is still room for improvement. The exercise report from the Cyber Storm III exercise specifically cited that "exchanging and sharing classified information among organizations proved to be a challenge."[102]

Conclusion

The issues of cyberspace law are complex and unlikely to be resolved any time soon. Although efforts like the CoECC and UN WGIG represent progress in international cooperation on the development of cyberspace standards and norms, most of this progress is in the area of defining cyber-crime rather than cyber-war. Given US interests in protecting privacy rights, the issues related to attribution will also endure. However, stakeholders require timely and accurate intelligence in order to make decisions on the legal status of a computer intrusion and its source as well as the appropriate response, whether criminal prosecution or military action.

The five intelligence imperatives proposed in this paper are not panaceas but would greatly reduce the risk of the opening scenario ever happening in the United States. Applying these intelligence imperatives facilitates decisions and mitigates risk. Comprehensive network analysis and using an all-source intelligence analytical approach would assist with quantifying threat capabilities and intentions, thereby facilitating detection, prevention, attribution, and decision making. Increased intelligence sharing supports the all-source approach, facilitates collaboration between law enforcement and the military, and provides a common operating picture to all stakeholders. Finally, embedding experienced legal advisors into intelligence organizations involved in cyberspace activities will facilitate quicker determinations of legal status and appropriate responses by the agencies with the proper legal authorities.

Endnotes

[1] Barack Obama, *National Cybersecurity Awareness Month*, Proclamation by the President of the United States (Washington, DC: The White House, October 1, 2009), 1.

[2] U.S. Deputy Secretary of Defense Gordon England, "The Definition of Cyberspace," memorandum for Secretaries of the Military Departments, Washington, DC, May 12, 2008, 1; Melissa Hathaway, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: U.S. Executive Office of the President, 2009), 1; U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Department of Defense, April 12, 2001, as amended through September 30, 2010), 118. This paper uses the joint definition of cyberspace cited in these three sources. However, there are at least 15 different definitions of cyberspace discussed in Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 26-28.

[3] George Bush, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), 1; Barack Obama, *Remarks by the President on Securing the Nation's Cyber Infrastructure* (Washington, DC: The White House, May 29, 2009), 1.

[4] Bush, *National Strategy to Secure Cyberspace*, 2; Hathaway, *Cyberspace Policy Review*, 1; Dennis C. Blair, *The National Intelligence Strategy* (Washington, DC: Office of the Director of National Intelligence, August 2009), 9; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York, NY: Harper Collins Publishers, 2010), 145-146; Lolita C. Baldor, "General Suggests 'Secure Zone' to Counter

Cyber Threats," *Fayetteville Observer*, September 24, 2010. According to Clarke and Knake, "of the eighteen civilian infrastructure sectors identified as critical by the Department of Homeland Security, all have grown reliant on the Internet to carry out their basic functions, and all are vulnerable to cyber-attacks by nation-state actors." These sources also agree that the majority of national infrastructure is privately owned and operated. Baldor cites that 85% of national infrastructure is owned and operated by private companies. Private ownership makes it subject to less federal regulation and control than government networks that fall under the Federal Information Security Management Act. According to the *National Intelligence Strategy*, "the architecture of the Nation's digital infrastructure, based largely upon the Internet, is neither secure nor resilient." Military cyber-exercises like Eligible Receiver and homeland security cyber-exercises like Cyber Storm have specifically identified multiple vulnerabilities in critical infrastructure networks. For more on these exercises and network vulnerabilities see Bradley K. Ashley, *Anatomy of Cyberterrorism: Is America Vulnerable?* (Maxwell Air Force Base, AL: U.S. Air War College, 2003), 25-26; Scott Beidleman, *Defining and Deterring Cyber War,* Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, 2009), 3; Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Falls Church, VA: Aegis Research Corporation, 2000), 22; and U.S. Department of Homeland Security, National Cyber Security Division, *Cyber Storm Exercise Report* (Washington, DC: U.S. Department of Homeland Security, National Cyber Security Division, September 12, 2006), 1-20.

[5] U.S. Joint Chiefs of Staff, Joint Publication 1-02, 93.

[6] Ibid. A simpler, but less comprehensive definition, used by Martin Libicki, is when "states steal data from other states," but I would add non-state actors as potential thieves as well. See Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 14.

[7] Ibid. Again, a simpler, less comprehensive definition, used by Martin Libicki, is "deliberate disruption or corruption by one state of a system of interest to another state," but I would also add non-state actors as potential attackers as well. See Libicki, *Cyberdeterrence and Cyberwar*, 23.

[8] Clay Wilson, *Information Operations and Cyberwar: Capabilities and Related Policy Issues* (Washington, DC: Library of Congress, Congressional Research Service, September 14, 2006), 5.

[9] Thom Shanker, "Cyberwar Chief Calls for Secure Computer Network," *New York Times*, September 23, 2010.

[10] Beidleman, *Defining and Deterring Cyber War*, 2 and 15-16.

[11] Wingfield, *Law of Information Conflict*, 5.

[12] Ibid., xvi.

[13] Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis & Clark Law Review* 11, no. 4 (Winter 2007): 1023-24; Jeffrey T. G. Kelsey, "Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare," *Michigan Law Review* 106, no. 7 (May 2008): 1430; Paul A. Matus, *Strategic Impact*

of Cyber Warfare Rules for the United States, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, 2010), 14-15.

[14] Wingfield, *Law of Information Conflict*, 73.

[15] Ibid., 39; United Nations, "Charter of the United Nations," http://www.un.org/en/documents/charter/index.shtml (accessed December 7, 2010). "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 in any other manner inconsistent with the Purposes of the United Nations."

[16] Wingfield, *Law of Information Conflict,* 123.

[17] Ibid., 39-40; United Nations, "Charter of the United Nations." "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."

[18] Wingfield, *Law of Information Conflict,* 123.

[19] Ibid., 111; Bruno Simma, *The Charter of the United Nations: A Commentary* (Oxford, UK: Oxford University Press, 1994), 670; United Nations, "United Nations General Assembly Resolution 3314," http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX) (accessed December 7, 2010). Some examples include: invasion, bombardment and cross-border shooting; blockade; attack on the land, sea, or air forces or on the civilian marine and air fleets; breach of stationing agreements; placing territory at another state's disposal; and participation in the use of force by militarily organized unofficial groups.

[20] International Committee of the Red Cross, "The Geneva Conventions of August 12, 1949," http://www.icrc.org/ihl.nsf/INTRO/365?OpenDocument (accessed December 7, 2010). The exact wording is: "Armed conflict exists upon: declaration of war; occurrence of any other armed conflict between two or more contracting parties even if state of war is not recognized by one of them; and in all cases of partial or total occupation even if met with no armed resistance."

[21] Walter G. Sharp, Sr., *Cyber Space and the Use of Force* (Falls Church, VA: Aegis Research Corporation, 1999), 69.

[22] Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition," *The Air Force Law Review,* vol. 64 (2009): 71.

[23] Sharp, *Cyber Space and Use of Force,* 69. According to Sharp, "what constitutes a use of force of a scope, duration, and intensity that constitutes an armed attack and triggers the law of armed conflict is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances."

[24] Wingfield, *Law of Information Conflict*, 113.

[25] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework* (Colorado Springs, CO: Institute of Information Technology Application, 1999), 18-19; Libicki, *Cyberdeterrence and Cyberwar*, 179-180. A good example of applying the Schmitt framework to the 2007 CNA against Estonia is in Thomas C. Wingfield,

"International Law and Information Operations," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 527-533.

[26] Wingfield, *Law of Information Conflict*, 100-101; Matus, *Strategic Impact of Cyber Warfare Rules,* 12; Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008-09): 60; Arie J. Schapp, "Cyber Warfare Operations: Development and Use Under International Law," *The Air Force Law Review,* no. 64 (2009): 147.

[27] Matus, *Strategic Impact of Cyber Warfare Rules,* 31.

[28] Wingfield, *Law of Information Conflict*, 290; International Committee of the Red Cross, "Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977" http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 (accessed December 7, 2010). Under this protocol, "works or installations containing dangerous forces, namely dams, dikes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."

[29] Matus, *Strategic Impact of Cyber Warfare Rules*, 10; Wingfield, *Law of Information Conflict,* 352-354.

[30] Todd, "Armed Attack in Cyberspace," 94. According to Todd, "while a criminal offense in virtually every nation state, espionage is not a violation of the law of war and was first recognized in the Lieber Code in 1863."

[31] Attribution for cyberspace intrusions is historically very difficult. You can often attribute the attacks to certain computers based on their internet protocol (IP) addresses but these computers are often infected by robot networks directing the intrusions from other remote computers. This makes clear attribution to a responsible individual difficult. If you get that far, then proving the individual was operating in an official capacity as a representative of a foreign nation is an additional level of difficulty. The problems in attribution make deterrence by punishment challenging although deterrence through denial remains possible. For more information on the difficulty with attribution see Ashley, *Anatomy of Cyber Terrorism*, 25-26; and Beidleman, *Defining and Deterring Cyber War*, 3. For a detailed discussion of the difficulty with attribution and its effect on deterrence, see Libicki, *Cyberdetterence and Cyberwar*.

[32] Wingfield, *Law of Information Conflict*, 8. According to Wingfield, "[even though] a non-state actor can cause identical damage to a state's information infrastructure as can a state actor, a hostile, transnational activity in cyberspace committed by a non-state actor remains a law enforcement issue. The issue of state and non-state sponsorship, however, may be very factually complicated by a number of circumstances such as the activities of state-owned commercial enterprises and surrogate-actors, as well as the anonymity afforded by technology. Nevertheless, the legal analysis remains rather straightforward. Determining when state-owned commercial enterprises, for example, are acting as a commercial enterprise or at the direction of a state is a determination surrounding facts such as who controls the enterprise, who directed the activity, and the nature of the activity. It is not an issue of law. Consequently, from a legal perspective, all hostile transnational activities in cyberspace are either non-state-sponsored and

thus a crime addressed by national and peacetime treaty law, or they are state-sponsored and thus a use of force governed by the law of conflict management and the law of armed conflict. The complete refusal or unwillingness of a state, however, to cooperate in the suppression or prevention of an acknowledged non-state-sponsored hostile, transnational activity in cyberspace that originates in its sovereign territory constitutes state-sponsorship of a use of force ipso facto, thereby invoking the law of conflict management which may authorize a use of force in self-defense against such a state or the non-state actors in that state. In the absence of any state-sponsorship of terrorist or criminal activities, a use of force by a state against those non-state actors in the sovereign territory of another state without that state's consent may rise to the level to be an unlawful use of force against that territorial state."

[33] Stuart Biegel, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge, MA: The MIT Press, 2001), 236; Michael L. Rustad, *Internet Law in a Nutshell* (St. Paul, MN: Thomson Reuters, 2009), 247; Robert W. Taylor et al., *Digital Crime and Digital Terrorism* (Upper Saddle River, NJ: Pearson Prentice Hall, 2006), 254-255.

[34] Rustad, *Internet Law in a Nutshell*, 247-249.

[35] Ibid., 246-247. For a more detailed discussion of botnets and how they are used, see Clay Wilson, "Cyber Crime," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 420-422.

[36] Rustad, *Internet Law in a Nutshell*, 155-157.

[37] Ibid., 53; Taylor, *Digital Crime and Digital Terrorism*, 255.

[38] Rustad, *Internet Law in a Nutshell*, 43 and 66.

[39] Ibid., 58-60. France's prosecution of Yahoo! for hosting Nazi web sites is also noted in James A. Lewis, "Overcoming Obstacles to Cooperation: The Council of Europe Convention on Cybercrime," in *Cyber Security: Turning National Solutions into International Cooperation,* (Washington, DC: The CSIS Press, 2003), 96.

[40] Beidleman, *Defining and Deterring Cyber War*, 3.

[41] Beidleman, *Defining and Deterring Cyber War*, 3; Kristin Archick, *Cybercrime: The Council of Europe Convention* (Washington, DC: Library of Congress, Congressional Research Service, September 28, 2006), 1; Michael Vatis, "International Cyber-Security Cooperation: Informal Bilateral Models," in *Cyber Security: Turning National Solutions into International Cooperation,* ed. James A. Lewis (Washington, DC: The CSIS Press, 2003), 7.

[42] Clay Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Washington, DC: Library of Congress, Congressional Research Service, April 1, 2005), 33; Archick, *Cybercrime,* 1; Rustad, *Internet Law in a Nutshell*, 256-257.

[43] Archick, *Cybercrime*, 1; Henrik Kaspersen, "A Gate Must Either Be Open or Be Shut: The Council of Europe Cybercrime Convention Model," in *Cyber Security: Turning National Solutions into International Cooperation,* ed. James A. Lewis (Washington, DC: The CSIS Press, 2003), 16-18. Kaspersen describes the Convention's aims a little differently than Archick by stating five

aims: harmonization of criminal law; harmonization of criminal procedural law concerning criminal investigations in public and private computer systems and networks; facilitate mutual legal assistance; codify international public law; and provide for an international legal framework.

[44] Pottengal Mukundan, "Laying the Foundations for a Cyber-Secure World," in *Cyber Security: Turning National Solutions into International Cooperation,* ed. James A. Lewis (Washington, DC: The CSIS Press, 2003), 34.

[45] Rustad, *Internet Law in a Nutshell*, 45.

[46] Rebecca Grant, *Victory in Cyberspace* (Arlington, VA: Air Force Association, 2007), 8.

[47] Baldor, "General Suggests 'Secure Zone.'"

[48] Clarke and Knake, *Cyber War*, 267.

[49] Bush, *National Strategy to Secure Cyberspace*, 2; U.S. Government Accountability Office, *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats*, statement for the record to the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate (Washington, DC: U.S. Government Accountability Office, November 17, 2009), 12.

[50] U.S. Government Accountability Office, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, report to Congressional requesters (Washington, DC: U.S. Government Accountability Office, March 2010), 17.

[51] This categorization into six basic sources of threats was developed by the Federal Bureau of Investigation and cited in GAO, *Cybersecurity: Continued Efforts Needed*, 4.

[52] Beidleman, *Defining and Detering Cyber War*, 18; Clarke and Knake, *Cyber War*, 144; U.S. General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," http://www.fas.org/irp/gao/aim96084.htm (accessed December 7, 2010). Clarke and Knake provide a more conservative estimate of over twenty nations with some cyber war capability.

[53] GAO, *Cybersecurity: Continued Efforts Needed*, 4.

[54] U.S. Congress, Senate, Select Committee on Intelligence, 15th Annual World-Wide Threat Hearing, *Current and Projected National Security Threats to the United States,* 111th Cong., 1st sess., February 12, 2009, 8; Clarke and Knake, *Cyber War*, 144. Clarke and Knake estimate that the US has the most sophisticated cyber war capability followed closely by Russia, China, and France.

[55] Steven P. Bucci, *The Confluence of Cyber Crime and Terrorism* (Washington, DC: Heritage Foundation, June 12, 2009), 3; Daniel J. Busby, *Peacetime Use of Computer Network Attack,* Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, 2000), 1.

[56] Wingfield, *Law of Information Conflict*, 24.

[57] Cyber Security Strategy Committee, *Cyber Security Strategy* (Tallinn, Estonia: Ministry of Defence, 2008), 6.

[58] Grant, *Victory in Cyberspace*, 4-9; Clarke and Knake, *Cyber War*, 15-16; Taylor, *Digital Crime and Digital Terrorism*, 27-28. Grant provides a detailed explanation of the CNA on Estonia and its implications for the future. Taylor provides further background on the forms of distributed denial of service attacks.

[59] Korns and Kastenberg, "Georgia's Cyber Left Hook," 60; Clarke and Knake, *Cyber War*, 17-18.

[60] Mark Clayton, "Stuxnet Malware is 'Weapon' Out to Destroy…Iran's Bushehr Nuclear Plant?," *Christian Science Monitor*, September 21, 2010; John Markoff and David E. Sanger, "In a Computer Worm, a Possible Biblical Clue," *New York Times*, September 29, 2010. This particular SCADA software was produced by Siemens, a German-based company, and is widely used in international industry.

[61] Clayton, "Stuxnet Malware;" Thomas Erdbrink and Ellen Nakashima, "Iran Struggling to Contain 'Foreign-Made' Computer Worm, *Washington Post*, September 28, 2010; Associated Press, "Iran Accuses West of Computer Sabotage," *USA Today*, October 6, 2010.

[62] Beidleman, *Defining and Deterring Cyber War*, 5; Libicki, *Cyberdeterrence and Cyberwar*, 2; Bruce Caulkins, *Proactive Self-Defense in Cyberspace* (Arlington, VA: The Institute of Land Warfare, 2009), 8.

[63] Libicki, *Cyberdeterrence and Cyberwar*, 89.

[64] GAO, *Cybersecurity: Continued Efforts Needed*, 4; Bucci, *Confluence of Cyber Crime*, 5; Caulkins, *Proactive Self-Defense*, 7.

[65] William D. O'Neil, "Cyberspace and Infrastructure," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 127; Wilson, "Cyber Crime," 433. According to O'Neil, the CIA has warned of this potential for cyber extortion noting that "cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities." According to Wilson, in January 2008, the CIA stated "we have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands."

[66] Caulkins, *Proactive Self-Defense*, 8; Wilson, *Computer Attack and Cyberterrorism*, 20; Rustad, *Internet Law in a Nutshell*, 246. According to Rustad, "the U.S. Justice Department indicted a Brazilian cybercriminal, Leni de Abreu Neto, for participating in a conspiracy with a 19-year old man from the Netherlands, Nordin Nasiri, to use, maintain, lease and sell an illegal botnet."

[67] GAO, *Cybersecurity: Continued Efforts Needed*, 4.

[68] Ibid.

[69] Ashley, *Anatomy of Cyber Terrorism*, 26-28; Beidleman, *Defining and Deterring Cyber War*, 3; James Glave, "Analyzer Nabbed in Israel?," *Wired News*, March 16, 1998; Jaxon Van Derbeken, Jim Doyle, and Glen Martin, "Hacking Suspect Caught in Cloverdale," *San Francisco Chronicle*, February 27, 1998.

[70] Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Network," *Security Focus*, August 19, 2003, http://www.securityfocus.com/news/6767 (accessed December 7, 2010).

[71] Beidleman, *Defining and Deterring Cyber War*, 6; O'Neil, "Cyberspace and Infrastructure," 125; Wilson, *Computer Attack and Cyberterrorism*, 10-11; Robert Lemos, "MSBlast and the Northeast Power Outage," *CNet News*, February 16, 2005, http://news.cnet.com/8301-10784_3-5579309-7.html (accessed December 7, 2010); Dan Verton, "Blaster Worm Linked to Severity of Blackout," *Computerworld*, August 29, 2003, http://www.computerworld.com/printthis/2003/0,4814,84510,00.html (accessed December 7, 2010). There is some dispute over how significant the MSBlast or Blaster worm was in causing the blackout. According to Wilson, congestion caused by the Blaster worm delayed the exchange of critical power grid control data across the public telecommunications network, which could have hampered the operators' ability to prevent the cascading effect of the blackout. According to O'Neil, "investigation showed that neither al Qaeda nor Blaster was responsible."

[72] GAO, *Cybersecurity: Continued Efforts Needed*, 4; Taylor, *Digital Crime and Digital Terrorism*, 92.

[73] Libicki, *Cyberdeterrence and Cyberwar*, 62-63.

[74] GAO, *Cybersecurity: Continued Efforts Needed*, 4; Taylor, *Digital Crime and Digital Terrorism*, 7. Some experts reason that insiders pose the greatest threat because of their access and knowledge of where to look for information in the network. Studies cited in Taylor's book attribute 73% to 90% of economic computer crimes to insiders.

[75] Taylor, *Digital Crime and Digital Terrorism*, 60.

[76] Clay Wilson, *Computer Attack and Cyberterrorism*, 6. United States law (Title 22 USC, section 2656) has employed this definition of terrorism for statistical and analytical purposes since 1983. The DoD definition, from U.S. Joint Chiefs of Staff, Joint Publication 1-02, 468, is similarly worded: "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."

[77] Wilson, *Computer Attack and Cyberterrorism*, 7. There is considerable debate over what constitutes cyber-terrorism. In Irving Lachow, "Cyber Terrorism: Menace or Myth?," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 438, Lachow offers a more detailed definition of cyberterrorism as "a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples." An important distinction is that terrorism is defined by the nature of the act not by

the identity of the perpetrators. Use of the internet by terrorists for propaganda and recruiting should not be considered cyber-terrorism. Cyber-terrorism, consisting of an act of CNE or CNA by a terrorist group, must intend to result in the same effects as physical acts of terrorism such as violence against human targets or as Barry Collin of the Institute for Security and Intelligence puts it "hacking with a body count." For more on this debate and distinction see Taylor, *Digital Crime and Digital Terrorism*, 21-23.

[78] Bucci, *Confluence of Cyber Crime*, 4; Clarke and Knake, *Cyber War*, 135.

[79] John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," *Networks and Netwars: The Future of Terror, Crime and Militancy* (Santa Monica, CA: RAND Corporation, 2001), 1-28; Clarke and Knake, *Cyber War*, 135.

[80] Wilson, *Computer Attack and Cyberterrorism*, 6.

[81] Baldor, "General Suggests 'Secure Zone.'"

[82] Wilson, *Computer Attack and Cyberterrorism*, 19.

[83] Ashley, *Anatomy of Cyberterrorism*, 29; Beidleman, *Defining and Deterring Cyber War*, 6; Permanent Monitoring Panel of Information Security, *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar* (New York, NY: World Federation of Scientists, August 2003), 9; Kevin Poulsen, "FBI Issues Water Supply Cyberterror Warning," *Security Focus*, January 30, 2002, http://www.securityfocus.com/news/319 (accessed December 7, 2010); William Matthews, "Al Qaeda Cyber Alarm Sounded," *Computer Crime Research Center*, July 25, 2002, http://www.crime-research.org/news/2002/07/Mess2601.htm (accessed December 7, 2010); Taylor, *Digital Crime and Digital Terrorism*, 31.

[84] Bucci, *Confluence of Cyber Crime*, 5-6; Taylor, *Digital Crime and Digital Terrorism*, 31. Taylor cites a statement from an Islamic cleric associated with bin Laden who indicates "fundamentalist Islamic groups are assembling cadres of computer science students sympathetic to al Qaeda's cause."

[85] Ashley, *Anatomy of Cyber Terrorism*, 23; Taylor, *Digital Crime and Digital Terrorism*, 30-31. Taylor describes the combination of a CNA attack with a physical attack as an "adjunct attack" and discusses how it can be a force multiplier for the terrorist by enhancing the impact of the physical attack. For example, hacking into and disabling emergency response systems during a physical attack would hamper the response of rescue personnel.

[86] Rustad, *Internet Law in a Nutshell*, 258-268; Taylor, *Digital Crime and Digital Terrorism*, 237-239 and 249-255. Both of these sources provide more detailed discussions of these federal statutes and their implications and constraints for intelligence and law enforcement officials.

[87] Wingfield, *Law of Information Conflict*, 146 and 159.

[88] Blair, *National Intelligence Strategy*, 5 and 9. Specifically the NIS stated mission objective is "Enhance cybersecurity – understand, detect, and counter adversary cyber threats to enable protection of the Nation's information infrastructure."

[89] Ibid., 9.

[90] Some experts believe it would require 2-4 years of surveillance, testing, and preparation and maybe even 6-10 years for a truly comprehensive mass disruption of multiple infrastructure networks. See Wilson, *Computer Attack and Cyberterrorism*, 17.

[91] Blair, *National Intelligence Strategy*, 9.

[92] U.S. Department of Homeland Security, *Cyber Storm Exercise Report*, 6-8. According to this report, the sheer volume of information constrained the ability of organizations to do both situational awareness and the second order technical analysis of networks and individuals.

[93] James Jay Carafano, *The Future of Anti-Terrorism Technologies* (Washington, DC: Heritage Foundation, January 17, 2005), 5.

[94] Rustad, *Internet Law in a Nutshell*, 30-31.

[95] Kim Cragin et al., *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies* (Santa Monica, CA: RAND Corporation, 2007), xvi and 97.

[96] Ibid., xv and 94.

[97] Wilson, *Computer Attack and Cyberterrorism*, 26.

[98] Blair, *National Intelligence Strategy*, 9.

[99] Ibid., 5.

[100] GAO, *Cybersecurity: Progress Made*, 18.

[101] Shaun Waterman, "Cyber Storm III Aims to Protect Against Real Thing," *Washington Times*, September 28, 2010.

[102] U.S. Department of Homeland Security, *Cyber Storm Exercise Report*, 10.