Cyber Terrorism Technology and The Laws of Cyber Warfare

Shauna Guyton

Available at: https://works.bepress.com/shauna_guyton/1/
The United States is currently engaged in a game of cyber warfare that looks like the plot of a Steven Spielberg science-fiction film. More importantly, the United States is losing. The recent online infiltration of Google Inc. by Chinese hackers demonstrates yet again that the U.S. is not safe from state-sponsored cyber attack. A 2005 survey by the Federal Bureau of Investigation estimates that American businesses lose approximately $67.2 billion dollars per year due to computer crimes. The cost to U.S. business is slight in comparison to the more important threats to our national security. As of this time, there is no comprehensive legislation encompassing national cyber crime and state-sponsored cyber terrorist attacks.

I. BACKGROUND

In January of 2011, Google, Inc. announced that it had been the victim of a “sophisticated cyber attack originating from China.” The hackers targeted the e-mail accounts of human rights activists, Chinese journalists, and several senior U.S. officials. According to the U.S.-China Economic and Security Review Commission report, strategy experts for the Chinese are openly writing about taking advantage of the U.S. military’s “reliance on technologies and attacking key civilian targets.” The United States is not the only country under attack. A coordinated assault out of China, dubbed the Night Dragon series, targeted major oil and gas companies around the world. Furthermore, China is not the only offender. In 2001, the European Union accused the

---

3 Chris Arsenault, China and the US: Sizing up for Cyber War?, Al Jazeera (June 9, 2011, 8:53 AM).
United States of launching a cyber espionage campaign known as Echelon against the several EU businesses. This trend demonstrates that as technology advances, so too do the methods available to breach or manipulate that technology.

A. Defining Cyber Crime And Cyber Terrorism

Leading experts have yet to decide on a clear definition of cyber terrorism and cyber crime. The U.S. Department of Justice has three classifications for cyber crimes. The first involves those criminal acts in which the computer or computer network is the target. The second involves using the computer as a tool to commit a crime. The final classification is when the computer holds evidence of the crime but may not have been the primary means of committing that crime.

In contrast, cyber terrorism may be divided into two categories. The first applies in those situations where “technology is used to facilitate the activities of terrorists.” This type of crime is punishable under general criminal or terrorism laws. The second category is more difficult to punish or even identify. This applies to “the use of computer network tools to harm or shut down critical national infrastructures.” Cyber terrorism is conducted by both national and international organizations. An expert at the Federal Judicial Center, Mark Sherman, defines cyber terrorism as involving “politically motivated crimes designed to generate fear, such as

---

8 Id.
9 Id.
attacks that lead to death or bodily injury, explosions, severe economic loss, or attacks against critical infrastructures.”

B. The Technology Of Cyber Warfare

In order to address the dangers of cyber terrorism, it is important to understand the nature of the attacks. The United States Government Accountability Office has defined the techniques used to commit cyber crimes, one of which is phishing. Phishing is a scam that deceives people into disclosing their personal information through pop-up messages or spam messages. This was the method used by the Chinese hackers in the Google attacks. Consumer Reports Magazine estimates that over one million homes were affected by phishing in 2011 with a loss of approximately $650 million.

An even more dangerous threat comes from sniffer programs. These are designed to search data and capture passwords as the information flows through the Internet. In 2003 an attack out of China, dubbed Titan Rain, ran a continuous search for information inside secure U.S. networks. They employed a scanner system first to find exposed computers. Scanner programs are used to search for vulnerabilities in particular software or computer models. U.S. officials stated that Titan Rain was part of a large scale cyber espionage attack conducted over a

13 Id.
15 Id.
17 Id.
20 Sherman, Supra at 16.
long period of time. The hackers were able to access a range of information, including Army flight plan software, World Bank documents and access to NASA’s network.

Another popular hacking method involves a worm. This is a program that reproduces itself and copies across a computer network. In 2010, the computer worm, Stuxnet, infiltrated a nuclear plant in Iran and destroyed approximately one fifth of Iran’s nuclear centrifuges, delaying their ability to create nuclear weapons. These same hacking techniques can be used in small scale scams on local web users and attacks on government infrastructures.

C. The Law

The American government’s response to cyber crime has been gaining momentum. In February of 2011, Senator Joe Lieberman announced his latest cyber bill, The Cyber Security and Internet Freedom Act. This is one in a string of protective measures that has been born and then buried in the Senate. Last year, Senator Lieberman introduced the Protecting Cyberspace as a National Asset Act of 2010, which granted broad government powers over critical online infrastructures. Most notably, this bill included the controversial “kill-switch” that allows the government to shut down the Internet and deny Internet access. The Senate has been engaged in a controversial dance, balancing American civil liberties against the need for more protective measures.

A major flaw in U.S. cyber crime legislation is that it has no international significance. There is no clear definition of a proportional response. For instance, the Pentagon has offered

---

21 Id.  
22 Id.  
23 Id.  
the idea of “equivalence” whereby a cyber attack resulting in the type of “death, damage, destruction or high-level disruption” of a kind caused by a traditional military attack would be a candidate for military retaliation. In contrast, a U.S. military official has been quoted as saying “If you shut down our power grid, maybe we will put a missile down one of your smokestacks.” There is also no mechanism for promoting communication between countries or reporting cyber attacks. What is needed is a clear international treaty that universally defines cyber terrorism, outlines jurisdiction, and promotes coordination between nations. This treaty can build upon principles already accepted within the United Nations.

II. THE BUILDING BLOCKS FOR AN INTERNATIONAL CYBER CRIME AGREEMENT

At the annual general body meeting of the United Nations in September of 2011, President Nursultan Nazarbayev of Kazakhstan called for “an international legal framework of the global information space.” He suggested basing such a framework on the “nine elements of a global culture of cyber security.” This is in reference to a resolution adopted by the U.N. General Assembly is 2002. The resolution, entitled Creation of a Global Culture of Cyber Security, was meant as a guide for participating countries in developing a strategic plan to handle the growth of technology. Specifically, the resolution laid out nine goals: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Managements, and Reassessment. First, the participating country

---

29 Id.
31 Id.
should be “aware of what they can do to enhance security.”\textsuperscript{33} Second, it is the responsibility of the countries to create their own “policies, practices, measures and procedures”\textsuperscript{34} and ensure that these measures are appropriate. Third, participants should act “in a timely and cooperative manner to prevent, detect and respond” to breaches in cyber security.\textsuperscript{35} Fourth, each country must recognize that in a global community the actions of one will have an effect on other participant countries.\textsuperscript{36} Fifth, any regulations on cyber space must be consistent with the ideals of democracy in protecting freedom of thought and the free flow of information.\textsuperscript{37} Sixth, all participants should “conduct periodic risk assessment” to identify and risks or vulnerabilities.\textsuperscript{38} Seventh, security implementation should be an element in any planning or operation of all information systems.\textsuperscript{39} Eighth, participants should adopt “a comprehensive approach to security management”\textsuperscript{40} Finally, the participants should engage in reassessment of all security measures and modify them as necessary.\textsuperscript{41}

III. MEETING THE GOALS: AWARENESS, RESPONSIBILITY, RESPONSE, RISK ASSESSMENT, AND SECURITY DESIGN

The international community has already made great strides toward meeting the first set of goals. For instance, many countries are already using Computer Emergency Response Teams (CERT). These models were first deployed by the Carnegie Mellon University.\textsuperscript{42} The goal of CERT is to study vulnerabilities in computer networks and provide training to improve
security. There are currently rapid response CERT teams in more than forty seven countries. These teams are trained to manage and mitigate damage caused by cyber attacks in both the public and private sectors.

Many countries are also participating in cyber war games designed to improve security measures. On November 3, 2011, the United States and the European Union held their first joint cyber security exercise. These simulation drills, named Cyber Atlantic 2011, were conducted in Brussels, Belgium and included more than twenty EU country participants. These exercises were based on the findings of another joint effort, Cyber Europe 2010, in which cyber defenses were tested and vulnerabilities identified. Both exercises results from the “joint commitment to cyber security” established at the EU-US summit held in Lisbon is 2010.

The goal of the Cyber Atlantic 2011 exercise was to test the defense capabilities of each country against attacks on supervisory control and data acquisition systems (SCADA). The SCADA system was first deployed in 1960. The computer system is used to “monitor and control a plant or equipment” in major industries such as telecommunications or other large communication systems, oil and gas refining plants or civil alarm systems. It consists of a centralized computer system that interfaces and obtains information from remote terminals that

---

43 Id.
46 Id.
51 Id. at 4.
are placed in the industries plants.\textsuperscript{52} These industries are critical infrastructures and an attack on any one could create a national emergency. For example, the Department of National Communication Systems refers to a possible attack on SCADA by implanting a Trojan virus that allows a hacker to take control of a system.\textsuperscript{53} Essentially, the hacker is able to infiltrate and manipulate one of our critical infrastructures, such as an energy plant, by attacking the SCADA system that controls the equipment in that plant. The simulated exercises of Cyber Atlantic were aimed at protecting SCADA systems in electric utilities.\textsuperscript{54}

Following the EU-U.S. exercises, the United Nations organized and performed the first “cross-border cyber drill” in Southeast Asia in December of 2011 focusing on “mass web destruction, spam, and malware infection.”\textsuperscript{55} The drills were an attempt to improve responsiveness to future cyber attacks and assess the preparedness of participating countries Cambodia, Laos, Myanmar, and Vietnam.\textsuperscript{56} Each country’s CERT teams were tasked with identifying where the attack originated, implement solutions, and repair any damage to the computer systems.\textsuperscript{57} The test also aimed to improve communication between the participants. Datuk Mohd Noor Amin, Chairman of the International Multilateral Partnership Against Cyber Threats (IMPACT), stated that “[t]his cyber drill serves as the prototype for upcoming larger global exercises being designed for 2012.”\textsuperscript{58}

\textsuperscript{52} Id. 
\textsuperscript{53} Id. at 42. 
\textsuperscript{56} Id. 
\textsuperscript{57} Id. 
\textsuperscript{58} Id.
By participating in simulated drills, the international community is already addressed issues of risk assessment, response and security design. It also demonstrates the growing awareness of the need for more coordinated efforts to combat cyber terrorist tactics.

IV. MOVING FORWARD

There are several issues in establishing laws to govern cyber crime. One of the major problems is jurisdiction. The Web has global reach and access to the Internet is widespread. In the world of cyber crime there is no need for the offender to be in the same country as the victim. They do not even have to be in the same room. This poses a unique problem to enforcing cyber crime laws, especially for state-sponsored cyber attacks.

Three levels of jurisdiction were identified in the 2001 Convention on Cyber Crime. The first is prescriptive jurisdiction. This refers to whether the state has legislative power over the conduct. Second is adjudicative jurisdiction which asks whether the courts have jurisdiction to hear the particular dispute. The last jurisdiction is enforcement. This asks whether the state has the jurisdiction to enforce the law. In order to address cyber crime across international borders, countries must be willing to submit to the jurisdiction of a single court or body of law.

In order to achieve this end there must be communication among participating countries as well as a great deal of trust. Simply because an attack originates from one country does not mean that it is an attack from that government. As technology expert Bruce Schneier, told Al Jazeera, "[y]ou don't have nationality for cyber attacks, making retaliation hard." Any

---

60 Clough at 405-06.
61 Id.
62 Id.
63 Id.
64 Id.
65 Chris Arsenault, China and the US: Sizing up for Cyber War?, Al Jazeera (June 9, 2011, 8:53 AM).
international agreement would require countries to respond to attacks generated within their own borders or submit to an investigation by an independent tribunal.

In order to protect critical infrastructures within the United States, government and military organizations should lessen their reliance on computer networks. Sensitive data should be removed from computers. Chris Palmer, the technology director with the Electronic Frontier Foundation advocacy group, has stated that access to sensitive data and military documents "should be like Mission Impossible, requiring a physical presence".66

V. CONCLUSION

The United States and the international community are at a critical crossroads. Technological advances have made it possible to engage an enemy without leaving the living room. The Internet allows countries to plan and participate in cyber espionage and cyber terrorism on a level never before seen. Unfortunately, our security measures have not adapted as quickly as the changes in technology. In order to shield sensitive information and prevent acts of terrorism there must be a unilateral agreement between countries. This agreement must serve a dual purpose. Not only should it promote open communication and responsibility, the agreement must also protect the free flow of information to ensure that the civil liberties are not trampled in the race for personal and national security.

66 Id.