

JOURNAL OF LAW & CYBER WARFARE

FOREWORD

Cyber Warfare, What are the Rules?

By Daniel B. Garrie

ARTICLES

Cyber Attacks and the Laws of War

By Michael Gervais

If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare.

By Michael Preciado

They Did it For the Lulz: Future Policy Considerations in the Wake of Lulz Security and Other Hacker Groups' Attacks on Stored Private Customer Data

By Jesse Noa

A New Perspective on the Achievement of Psychological Effects from Cyber Warfare Payloads: The Analogy of Parasitic Manipulation of Host Behavior

By Dr. Mils Hills

Volume 1 | Winter 2012 | Issue 1

(c) 2012 – 2013. Journal of Law & Cyber Warfare.

All Rights Reserved.

www.jlcw.org

EDITORS

Daniel B. Garrie, Esq., Editor-in-Chief
Siddhartha Rao, Esq. Executive Editor

Associate Editors

Candice Lang, Esq., Editorial Fellow
Stephen Williams, Esq., Editor-at-Large

EDITORIAL BOARD

William Spernow	Jeff Bardin
Alex Carrillo	Dick Crowell
Uma Chandrashekhar	Gus Dimitrelos
Patrick Grey	George Hull
Thomas A. Johnson	Alan Roper
Jonathan E. Turner	Russell Walker
Judge David Harvey	Joseph E. Weiss
Michael Schmitt	

If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare

By Michael Preciado*

I. INTRODUCTION

This article will demonstrate four key points. First, that militaries around the world have implemented cyber warfare¹ as part their military doctrines.² Second, cyber warfare poses a serious threat to critical

* Michael Preciado is a 2013 J.D. Candidate of Chapman University School of Law. The author would like to gratefully acknowledge his wife, Mona Preciado, and his family for their support and encouragement throughout the writing process.

¹ See Brenner, *infra* note 266, at 401 (cyber warfare is the conduct of military operations by virtual means).

² See *infra* Part I-C (discussing the rise of cyber attacks in modern warfare); see also MCAFEE, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 5 (2011) (over 120 nations have or are currently developing cyber warfare capabilities).

infrastructure in the United States.³ Third, cyber warfare cannot be policed through international treaties.⁴ Fourth, for the foregoing reasons, the federal government needs to protect critical infrastructures in the United States from cyber warfare.⁵

Technology, although created for the advancement of mankind, is eventually turned into a weapon of war.⁶ The Internet is no exception.⁷

³ See *infra* Part II (discussing the dangers that cyber attacks pose to critical infrastructures in the United States); see also MCAFEE, IN THE DARK: CRUCIAL INDUSTRIES CONFRONT CYBER ATTACKS 6 (2011) (85% of critical infrastructures have reported being the victims of cyber intrusions). “Exploiting vulnerabilities in cyber infrastructure will be part of any future conflict. If opponents can access a system to steal information, they can also leave something behind that they can trigger in the even of a conflict or crisis. Porous information systems have allowed opponents to map our vulnerabilities and plan their attacks. Depriving Americans of electricity, communications, and financial services may not be enough to provide the margin of victory in a conflict, but it could damage our ability to respond and our will to resist. We should expect that exploiting vulnerabilities in cyber infrastructure will be part of any future conflict.” The 44th Presidency, *infra* note 131, at 13.

⁴ See *infra* Part III (discussing how international law, such as the United Nations Charter, will not provide an adequate legal framework to govern cyber warfare); C.f. Stuart S. Malawer, *Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance*, 58 VIRGINIA LAWYER 28, 30 (2010) (international law will provide hollow results and prove to be an illusion of safety).

⁵ See *infra* Part IV (concluding that the federal government can monitor critical infrastructure in the United States through a warrant type system that protects civil liberties).

⁶ AHMAD KAMAL, THE LAW OF CYBER-SPACE: AN INVITATION TO THE TABLE OF NEGOTIATIONS 76 (2005). “Industrialization led to attrition warfare by massive armies in World War I. Mechanization led to maneuver predominated by tanks in World War II. The information revolution implies the rise of a new mode of warfare in which neither mass nor mobility will decide outcomes; instead, the side that has greater technological knowledge will enjoy decisive advantages.” *Id.*

Throughout modern history, parties have learned how to take advantage of the Internet and how to exploit it.⁸ Initially, hackers used cyberspace to explore system networks.⁹ Criminals then learned how to use the Internet to commit personal identity theft.¹⁰ Similarly, terrorists learned how to use the Internet to disseminate propaganda.¹¹ In the end, militaries around the world have learned how to use cyberspace for intelligence gathering, covert operations, and warfare.¹²

As a result of nations resorting to cyber warfare, the militarized use of cyberspace poses serious dangers to the United States' critical infrastructure.¹³ Cyber attacks have been able to infiltrate nuclear power plants and affect the power grids.¹⁴ Cyber attacks can

⁷ See McAfee, VIRTUAL CRIMINOLOGY REPORT 2009, VIRTUALLY HERE: THE AGE OF CYBER WARFARE 3 (2009) (nations are building up their cyber attack capabilities in what has been described as a "Cyber Cold War").

⁸ See e.g., Krebs, *infra* note 61 (one of the first computer viruses, "The Brain," was created in 1986).

⁹ *Infra* Part I-C.

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ See *infra* Part II; see also U.S. Dep't of Homeland Sec., Presentation, National Cyber Exercise: Cyber Storm, New York City Metro ISSA Meeting 11 (June 21, 2006) (operation Cyber Storm was a simulated attack against critical infrastructures in the United States that demonstrated vulnerabilities in the electric grids, FAA computer systems, and commuter train systems); ANTHONY H. CORDESMAN & JUSTIN G. CORDESMAN, CYBER-THREATS, INFORMATION WARFARE, AND CRITICAL INFRASTRUCTURE PROTECTION 2 (2002) (cyber attacks threaten the United States, because information systems are becoming a major part of critical infrastructure and government). The threat of a cyber war has grown so much that some analyst predict a looming cyber "Pear Harbor." *Id.*

¹⁴ See Schneier, *infra* note 139 (discussing the Stuxnet virus that allegedly corrupted Iran's nuclear program).

theoretically crash the financial industry.¹⁵ Further, cyber attacks against government infrastructure have caused massive instability and confusion.¹⁶

In response to the potential dangers of cyber warfare, academics have proposed that the legality of cyber warfare could be governed by analogy.¹⁷ Theorists have suggested that legal analogies to the Nuclear Nonproliferation Treaty, the United Nations Charter, the Outer Space Treaty, or the Antarctic Treaty System provide adequate models to govern cyber warfare.¹⁸ Hypothetically, these analogies provide the principles to govern cyber warfare.¹⁹ In practice however, these analogies provide unworkable models to govern cyber warfare.²⁰ Practicing law by analogy would not adequately police cyber warfare because attributing responsibility for cyber attacks is improbable; nations will use cyber warfare as a means to force larger militaries into asymmetric warfare; and because cyber warfare can be used to attack critical infrastructure in order to thwart an enemy's military action.²¹ Accordingly, cyber warfare cannot be properly regulated through international means.²²

Because the dogs of cyber war cannot be shackled by international means, the United States needs

¹⁵ See McAfee, *supra* note 1, at 17 (only 14% of the population are completely confident the financial sector could withstand a major cyber attack).

¹⁶ See e.g., Brenner, *infra* note 266, at 396 (an orchestrated cyber attack could infiltrate ATMs throughout the nation, crippling the financial industry).

¹⁷ See *infra* Part III.

¹⁸ See Shackelford, *infra* note 152, at 216 (analogizing responses to cyber attacks in international law).

¹⁹ See *infra* Part III.

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

to protect the nation's critical infrastructure.²³ The federal government should institute active defense measures on critical infrastructure networks.²⁴ This will entail the monitoring of critical infrastructure networks for malicious code.²⁵ In order to ensure that civil liberties are protected, Congress should also pass legislation that allows Cyber Command²⁶ to monitor private networks upon judicial approval.²⁷

Part I will discuss the history of the Internet and the evolution of cyberspace into its ultimate utilization in cyber warfare. Part II will explain why cyber attacks pose threats to the United States' critical infrastructure. Part III will survey the international efforts proposed to regulate cyber warfare, why they are inadequate, and why subsequent legislation will prove ineffectual as a means to regulate cyber warfare. To conclude, Part IV will propose that the federal government needs to protect critical infrastructure in the United States.²⁸ This can be implemented through legislation that allows Cyber Command to monitor private networks upon judicial approval.²⁹

II. THE INTERNET AND THE RISE OF CYBER WARFARE

A. THE ORIGINS AND STRUCTURE OF THE INTERNET

The Internet was originally created for the Department of Defense ("DOD"), but later became widely incorporated within the general public.³⁰ The

²³ See *infra* Part IV.

²⁴ *Id.*

²⁵ *Id.*

²⁶ See *Cyber Command*, *infra* note 94.

²⁷ See *infra* Part IV.

²⁸ *Id.*

²⁹ *Id.*

³⁰ See e.g., Stephen Segaller, *Nerds 2.0.1: A Brief History of the Internet* (1998); Katie Hafner, *Where Wizards Stay Up Late: The Origins Of The Internet* (1998).

origin of the Internet can be dated to 1969 as an experimental project of the Advanced Research Project Agency (“ARPA”).³¹ The DOD funded the project for the purpose of building a communications network.³² Accordingly, ARPA developed the Advanced Research Project Agency Network (“ARPANET”).³³ a communications medium of dedicated telephone lines.³⁴ ARPANET provided a series of redundant communications between the DOD, defense contractors, and defense research universities.³⁵ Subsequently, ARPANET expanded to encompass corporations, universities, and the general public.³⁶ “The ARPANET came to be called the ‘DARPA Internet,’ and finally just the ‘Internet.’”³⁷

The structure of the Internet is comprised of a decentralized series of networks.³⁸ “No single entity—academic, corporate, governmental, or non-profit—

³¹ See Peter H. Salus, *The Net: A Brief History of Origins*, 38 JURIMETRICS J. 161, 161—167 (1998) (for a brief history of the Advanced Research Project Agency’s role in creating the Internet).

³² Donna Miles, *Bush Cites DOD Internet Development in Promoting U.S. Innovation*, AMERICAN FORCES PRESS SERVICE, Feb. 6, 2003 (the DOD funded the project to improve military communications).

³³ See *Am. Civil Liberties Union v. Reno*, 929 F. Supp. 824, 831 (E.D.Pa. 1996) (providing a succinct history of the Internet).

³⁴ See Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 135—36 (2005). “[N]ow internet communications travel through all available communication mediums: telephone lines, microwave relays, satellite uplinks and downlinks, fiber optic cables.” *Id.*

³⁵ See *e.g.*, FRED H. CATE, *PRIVACY IN THE INFORMATION AGE* 9—11 (1997); Salus, *supra* note 31, at 163 (the defense research universities included the University of California Los Angeles, Stanford, University of California Santa Barbara, and the University of Utah).

³⁶ Cate, *supra* note 35, at 9—10.

³⁷ *Reno*, 929 F. Supp. at 831.

³⁸ Cate, *supra* note 35, at 10.

administers the Internet.”³⁹ It was designed to be a decentralized series of communication links that could reroute a message instantaneously if one or more networks were damaged or unavailable.⁴⁰ For instance, an email sent from a user in Washington D.C. to a user in California may be diverted through several other networks and further subdivided to reach its final destination.⁴¹ The Internet is not a single streamlined entity, but rather a “giant network which interconnects

³⁹ *Reno*, 929 F. Supp. at 832.

⁴⁰ *Id.* at 831. “This redundant system of linked computers was designed to allow vital research and communications to continue even if portions of the network were damaged, say, in war.” *Id.*

⁴¹ *Id.* “A communication sent over this redundant series of linked computers could travel a number of routes to its destination. Thus, a message sent from a computer in Washington, D.C., to a computer in Palo Alto, California, might first be sent to a computer in Philadelphia, and then forwarded to a computer in Pittsburgh, and then to Chicago, Denver, and Salt Lake City, before finally reaching Palo Alto. If the message could not travel along that path (because of military attack, simple technical malfunction, or other reason), the message would automatically (without human intervention or even knowledge) be re-routed, perhaps, from Washington, D.C. to Richmond, and then to Atlanta, New Orleans, Dallas, Albuquerque, Los Angeles, and finally to Palo Alto. This type of transmission, and re-routing, would likely occur in a matter of seconds.” *Id.* “Messages between computers on the Internet do not necessarily travel entirely along the same path. The Internet uses ‘packet switching’ communication protocols that allow individual messages to be subdivided into smaller ‘packets’ that are then sent independently to the destination, and are then automatically reassembled by the receiving computer.” *Id.*; See also Antolin-Jenkins, *supra* note 34, at 137; George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT’L L. 1079, 1094–95 (2000).

innumerable smaller groups or linked computer networks. It is thus a network of networks.”⁴²

B. TYPES OF CYBER ATTACKS

In order to understand what cyber warfare is, it is important to understand what a cyber attack is. Cyber warriors have three types of cyber attacks within their arsenal: syntactic, semantic, and mixed.⁴³ The weapons vary in intensity, ranging from annoyance to

⁴² *Reno*, 929 F. Supp. at 830. Because the Internet is comprised of several networks, a user must connect to an Internet Service Provider (“ISP”) to access the Internet. See Antolin-Jenkins, *supra* note 34, at 136 (“By connecting to the ISP, the computer becomes part of the network, and it may be utilized in the process of sending messages.”). Although the Internet is comprised of several smaller networks, the majority of Internet traffic flows through large cable lines, known as dedicated “backbones.” See RICHARD A. CLARKE & ROBERT K. KNAKE, *CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT* 281 (2010) (Internet backbones are comprised of national fiber optic cables operated by large Tier 1 Internet Service Providers). Maintained by large telecommunications companies, these backbones, fiber optic cables, facilitate the transmission of large amounts of data simultaneously to various regions. See ELLEN S. COHEN, *BROADBAND INTERNET: ACCESS, REGULATION AND POLICY* 10 (2007) (AT&T, Verizon, Sprint-Nextel, Level3, and Quest are all Tier 1 service providers that own “backbone” cables). The backbones are then connected internationally to Network Access Points (“NAPs”). Antolin-Jenkins, *supra* note 34, at 136. The NAPs are the gateways through which international Internet traffic flows: “each individual entity, whether a government entity, a communications company, or a corporation with a large intranet, agrees to intercommunicate with one another through the NAPs.” *Id.*

⁴³ Some theorists have classified electromagnetic weapons as cyber weapons. See Natasha Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 305 (2008). An electromagnetic weapon is used to “overload computer circuitry with a blast of electromagnetic energy.” *Id.* Although electromagnetic weapons can affect computer-based systems, realistically they are kinetic weapons used to short circuit electrical systems. Accordingly, they are not included in this article’s definition of cyber weapons.

devastation,⁴⁴ but all pose serious threats to national security.⁴⁵

The first kind of cyber attack is the syntactic attack, a cyber attack comprised of malicious code.⁴⁶ Malicious code is computer language designed to affect a computer's operating system in order to modify it, retrieve information, or destroy it.⁴⁷ Examples include viruses, worms, Trojan horses, denial-of-service ("DOS") attacks, and distributed-denial-of-service

⁴⁴ See Jeffrey Carr, *Cyber Warfare: Mapping the Cyber Underworld* 1—12 (Mike Loukides, 1st ed. 2010).

⁴⁵ See e.g., John S. Fredland, *Building a Better Cybersecurity Act: Empowering the Executive Branch Against Cybersecurity Emergencies*, 206 MIL. L. REV. 1, 3 (2010) (DDOS attacks targeted several United States government and commercial websites: "The White House, Department of Homeland Security, Secret Service, National Security Agency, Federal Trade Commission, Department of the Treasury, Department of Defense, Department of State, New York Stock Exchange, NASDAQ Stock Market, Amazon, and Yahoo."); see also David Goldman, *Countries Brace for the Cold War*, CNN MONEY, Aug. 4, 2011, available at www.money.cnn.com/2011/08/03/technology/cyber_attack/index.htm.

⁴⁶ Antolin-Jenkins, *supra* note 34, at 139.

⁴⁷ See e.g., John Markoff, *New Version of Malicious Computer Program Is Released*, N.Y. TIMES, Feb. 23, 2009, available at <http://www.nytimes.com/2009/02/24/science/24computer.html> (the Conflicker worm infected over 12 million computers into a botnet, presumably to steal passwords from unsuspecting users); see also Tara Mthri, *In Fear of Cyberterrorism: An Analysis of the Congressional Response*, 2003 U. ILL. J.L. TECH. & POL'Y 297, 298—310 (2003) (discussing the legal response to malicious code used in terrorist activities).

("DDOS") attacks.⁴⁸ Above all, DOS and DDOS attacks are of the most concern.⁴⁹ DOS attacks temporarily or permanently incapacitate a website by overwhelming it with false data requests.⁵⁰ The network becomes so overworked that it crashes.⁵¹ DDOS attacks are similar to DOS attacks, but use thousands of botnet⁵² computers

⁴⁸ See Antolin-Jenkins, *supra* note 34, at 138—140 (discussing syntactic attacks). Viruses are activated when the user opens a file. They "corrupt and destroy files in the infected computer, making the computer inoperative." *Id.* at 139. "Worms replicate in the system without infecting the host computer." *Id.* "At a certain point, there is so much duplication of messages, the system as a whole suffers at the least, a slow-down, and at worst, a crash of host systems overwhelmed by the traffic, thereby denying legitimate traffic a means of transportation." *Id.* A Trojan horse is an executable code that upon being activated, will perform certain functions that it was created to do e.g., providing the sender of the code remote access to the infected computer. *Id.* In a denial-of-service attack, attackers attempt to cause computer networks to crash to prevent the public from accessing information. See *Understanding Denial-of-Service Attacks*, US-CERT: UNITED STATES COMPUTER EMERGENCY READINESS TEAM, available at <http://www.us-cert.gov/cas/tips/ST04-015.html>. A distributed denial-of-service attack is distributed because the attacker uses multiple computers to launch a denial-of-service attack. *Id.*

⁴⁹ See e.g., Jenifer A. Chandler, *Security in Cyberspace: Combating Distributed Denial of Service Attacks*, U. OTTAWA L. & TECH. J. 231, 237 (2003) (the Nachi DDOS attack disabled Air Canada check-in-systems, infected computers on the U.S. Navy intranet, and shut down CSX Corp., the third largest U.S. railroad operator).

⁵⁰ Wolfgang McGavran, *Intended Consequences: Regulating Cyber Attacks*, 12 TUL. J. TECH. & INTELL. PROP. 259, 262—63 (2009).

⁵¹ Chandler, *supra* note 49, at 236 (discussing the effects of DDOS attacks, which are similar to DOS attacks).

⁵² "An example of a mixed weapon is a 'bot network' or 'bot herd,' which is a group of 'bots.' Bots are remote-controlled or semi-autonomous computer programs that infect computers. The hacker who controls the bots may spy, copy and transmit sensitive data, and organize the bots in a swarm attack against targeted computers." Natasha Solce, *supra* note 43, at 305.

that exponentially cause websites to crash, or alternatively damage the websites' host hardware.⁵³

The second kind of cyber attack is the semantic attack.⁵⁴ Semantic attacks alter the information the computer has access to: a weapon of misinformation.⁵⁵ "The semantic attack targets the information, substituting inaccurate or misleading information."⁵⁶ In particular, the Logic Bomb is one of the most dangerous semantic attacks.⁵⁷ By implication their composition is that of a bomb: planted in a targeted area and ignited upon desire. Once ignited, Logic Bombs send false data to information systems that can cause them to malfunction.⁵⁸ The third type of cyber attack is the mixed attack.⁵⁹ These simply combine syntactic and semantic attacks.⁶⁰

⁵³ Wolfgang, *supra* note 50, at 262.

⁵⁴ Antolin-Jenkins, *supra* note 34, at 140.

⁵⁵ See e.g., MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 13 (2009) ("[i]t is possible to attack computers solely at the semantic level by feeding them false information, like lighting a match under a thermostat to chill a room or creating a fake news source.").

⁵⁶ Antolin-Jenkins, *supra* note 34, at 140.

⁵⁷ See generally, Mark R. Colombell, *The Legislative Response to the Evolution of Computer Viruses*, 8 RICH. J.L. & TECH. 18 (2002) at <http://www.jolt.richmond.edu/v8i3/article18.html> (Logic Bombs cause substantial damage before they are ever detected). "Examples include feeding false data to the seismic activity sensing arrays of nuclear plants, causing a shutdown of the plants and a shutoff of significant sources of electrical power, or providing false data to an air traffic control systems, simulating non-existent planes and flight paths, causing confusion and disruption." Antolin-Jenkins, *supra* note 34, at 140.

⁵⁸ Arie J. Shaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 137 (2009).

⁵⁹ Natasha Solce, *supra* note 43, at 304.

⁶⁰ Antolin-Jenkins, *supra* note 34, at 140.

C. THE RISE OF CYBER WARFARE: HACKERS,
CYBER CRIMINALS, CYBER TERRORISTS, AND
CYBER WARRIORS

Despite the wonders of the Internet, individuals have figured out how to manipulate it.⁶¹ Suitably, the actors behind cyber attacks have evolved throughout modern history, starting with hackers, cybercriminals, cyber terrorists, and finally to cyber warriors.⁶² Hackers⁶³ were the first to learn how to exploit system networks.⁶⁴ Then, organized crime realized how to monetize the Internet through fraud and personal identity theft.⁶⁵ Terrorists even used the Internet to further their goals.⁶⁶ Eventually, militaries around the world imbedded their operations in cyberspace: it became just another domain to conquer.⁶⁷

Hackers were the first to venture into the underworld of computer exploitation.⁶⁸ The definition of a hacker is an individual that uses computers to gain

⁶¹ See Brian Krebs, *A Short History of Computer Viruses and Attacks*, WASH. POST (Fed. 14, 2003), <http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26>.

⁶² Natasha Solce, *supra* note 43, at 297. “States, criminal organizations, terrorist organizations, and specific individuals are using the developed networks to transverse cyberspace and launch cyber attacks.” *Id.*

⁶³ See Deirdre Black, *The Computer Hacker- Electronic Vandal or Scout of the Networks?*, 4 J.L. & INF. SCI. 65 (1993) (discussing the characteristics of computer hackers).

⁶⁴ See ZULEY CLARK, JAMES CLAWSON & MARIA CORDELL, *A BRIEF HISTORY OF HACKING 1—2* (2003) (hacking became a modern trend in the 1980’s with the introduction of the personal computer).

⁶⁵ *Id.* at 2.

⁶⁶ See generally, Sarah Gordon & Richard Ford, *Cyberterrorism?*, Symantec Security Response White Paper 4 (2003) (cyberterrorism is terrorism conducted in cyberspace).

⁶⁷ See Aiden Lawes, *Cyber Crime: A 24/7 Global Battle*, ITP REPORT (Nov. 29, 2007) (120 nations have or are developing cyber warfare capabilities).

⁶⁸ See Cordell, *supra* note 64.

unauthorized access to data and modify or delete it.⁶⁹ Hackers were originally comprised of young adults curious about computer systems.⁷⁰ Primarily, hackers infiltrated networks to explore the mechanics of the systems.⁷¹ Subsequently, the trend shifted, as hackers became focused on personal gain, distributing pirated software, computer fraud, and spreading viruses.⁷² The case of Kevin Poulsen is illustrative.⁷³

In 1994, Poulsen plead guilty to hacking a radio station's phone system during a radio contest so that it would only let his phone calls through.⁷⁴ In short, Poulsen won two Porches, vacations trips, and \$20,000 cash.⁷⁵ Poulsen was sentenced to fifty-one months in prison for wire and computer fraud, among other

⁶⁹ See generally, BRUCE STERLING, *THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELECTRONIC FRONTIER* (1993); but see Bruce Schneier, *What is a Hacker?*, SCHNEIER ON SECURITY BLOG (Sep. 14, 2006), http://www.schneier.com/blog/archives/2006/09/what_is_a_hacke.html (portraying hackers as being adventurous in nature rather than criminal).

⁷⁰ See *Timeline: A 40-year History of Hacking*, CNN, Nov. 19, 2001, available at http://articles.cnn.com/2001-11-19/tech/hack.history.idg_1_phone-phreaks-chaos-computer-club-emmanuel-goldstein?_s=PM:TECH. "During heightened tensions in the Persian Gulf, hackers touch off a string of break-ins to unclassified Pentagon computers and steal software programs. Then-U.S. Deputy Defense Secretary John Hamre calls it 'the most organized and systematic attack' on U.S. military systems to date. An investigation points to two American teens. A 19-year-old Israeli hacker who calls himself 'The Analyzer' (aka Ehud Tenebaum) is eventually identified as their ringleader and arrested. Today Tenebaum is chief technology officer of a computer consulting firm." *Id.*

⁷¹ See Bruce Schneier, *supra* note 69.

⁷² See Cordell, *supra* note 64.

⁷³ See *Timeline*, *supra* note 70.

⁷⁴ *Id.*

⁷⁵ *Id.*

things.⁷⁶ The case of Kevin Mitnick is another example.⁷⁷ Over a two and half year period, Mitnick allegedly hacked into Motorola, Fujitsu, and Sun Microsystems, stole corporate secrets, broke into the national defense warning system, and stole 20,000 credit card numbers.⁷⁸ Mitnick was incarcerated in 1995 on a twenty-five-count indictment, including wire fraud.⁷⁹

Eventually, criminal organizations realized the potential of exploiting the Internet.⁸⁰ Cyber crime is generally defined as accessing any computer network with the intent to defraud or to obtain money by means of false representations.⁸¹ The main goal of any cybercriminal is to steal money or acquire information in

⁷⁶ *Id.*

⁷⁷ See John Christensen, *The Trials of Kevin Mitnick*, CNN, Mar. 18, 1999, available at <http://www.cnn.com/SPECIALS/1999/mitnick.background/>.

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 204—05 (2006). “No matter what its core product or service, nearly every business in today’s economy relies upon computers and computer networks to conduct its daily affairs. It is likely that many of a company’s assets—including its trade secrets are archived on these computer systems. If the company’s computer network is accessible to the Internet... those assets are subject to cyber-theft.” *Id.*

⁸¹ See *e.g.*, LA. REV. STAT. ANN. § 14:73.5 (2007).

Computer fraud is the accessing or causing to be accessed of any computer, computer system, computer network, or any part thereof with the intent to: (1) Defraud; or (2) Obtain money, property, or services by means of false or fraudulent conduct, practices, or representations, or through the fraudulent alteration, deletion, or insertion of programs or data.

exchange for money.⁸² In particular, The Russian Business Network (“RBN”) is a cybercrime syndicate that specializes in personal identity theft for resale.⁸³ The RBN sells website hosting services to various criminals.⁸⁴ They provide exploits to criminal customers, such as fake anti-spyware/anti-malware for the purposes of computer hijacking and identity theft.⁸⁵

⁸² See Natasha Solce, *supra* note 43, at 301; Wong Yang, *supra* note 80, at 204. Cyber criminals have also used cyber crime for other than monetary reasons. Press Release, United States Department of Justice, Orange County Man Who Admitted Hacking Into Personal Computers Sentenced to Six Years in Federal Prison for ‘Sextortion’ of Women and Teenage Girls (Sep. 1, 2011) (on file with the Department of Justice) (Luis Mijangos pleaded guilty to computer hacking for using malicious software to hack into teenage girls’ computers, access the victims’ webcams, and take indecent pictures of them. He would subsequently demand sexual favors from the teenage girls in exchange for not releasing the indecent photos. He was sentenced to seventy-two months in federal prison); *see also* Press Release, United States Department of Justice, Sixteen Individuals Arrested in The United States for Alleged Roles in Cyber Attacks (July. 19, 2011) (In 2010, WikiLeaks published large amounts of U.S. State Department cables on its website. In response, PayPal suspended WikiLeaks’ account so that it could no longer receive donations. In retribution for PayPal’s termination of WikiLeaks’ account, the hacker group Anonymous executed a DDOS attack against PayPal’s computer servers with the intent to damage their network).

⁸³ See *Extortion and Denial of Service (DDOS) Attacks, RUSSIAN BUSINESS NETWORK (RBN) BLOG* (last visited Oct. 23, 2011), <http://rbnexploit.com>. Businesses that take an active stance to combat the RBN have been targeted by DDOS attacks. *A Walk on the Dark Side: These Badhats May Have Bought Your Bank Account*, ECONOMIST, Aug. 30, 2007, available at <http://www.economist.com/node/9723768>. The RBN generates \$150 million in profit per year.

⁸⁴ Brian Krebs, *Shadowy Russian Firm Seen as Conduit for Cyber Crime*, WASH. POST, Oct. 13, 2007, available at <http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html>.

⁸⁵ See *e.g.*, David Bizeul, Russian Business Network Study 7 (2007).

Terrorist organizations have also learned how to exploit the Internet.⁸⁶ Cyber terrorism is defined as “the use of computers as weapons, or as targets, by politically motivated international, sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies.”⁸⁷ For example, al-Qaeda has been identified as using cyberspace in its jihad against the United States.⁸⁸ However, the extent of al-Qaeda’s use of cyberspace has been limited to a supporting role in its operations: using the Internet to communicate, collaborate, recruit, and fundraise for future attacks.⁸⁹ Incidentally, Anwar al-Awlaki used Facebook and YouTube to recruit jihadists and to preach for the destruction of the United States.⁹⁰

Terrorist groups have also built online libraries of training materials covering topics including: how sneak through customs, how to make a homemade

⁸⁶ See CARLOS A RODRIGUEZ, CYBERTERRORISM: A RISING THREAT IN THE WESTERN HEMISPHERE 7 (2006). Cyber terrorism is the act of weaponizing computer systems, by politically motivated individuals or groups, to “cause violence and fear in order to influence an audience, or cause a government to change its policies.” *Id.* The Aum Shinrikyo Cult of Japan stands for the proposition that a terror organization can penetrate the computer networks of a specific target. The Aum Shinriko Cult acquired access to Japanese companies and government agencies by selling them legitimate software “laden with backdoors.” Natasha Solce, *supra* note 43, at 300. The cult could have entered the companies systems unimpeded and installed computer viruses to launch a cyber attack. See TOM PARKER ET AL., CYBER ADVERSARY CHARACTERIZATION: AUDITING THE HACKER MIND 253 (2004).

⁸⁷ Natasha Solce, *supra* note 43, at 301.

⁸⁸ *Id.* at 299.

⁸⁹ *Id.*

⁹⁰ Loveday Morris, *The Anatomy of a Suicide Bomber*, NAT’L, Jan. 2, 2010, available at <http://www.thenational.ae/news/the-anatomy-of-a-suicide-bomber>.

bomb, and how to shoot at a U.S. soldier.⁹¹ Terrorists have also used the Internet to acquire donations to fund their operations.⁹² The extremist group Hizb al-Tahrir, for example, used multiple websites throughout Europe and Africa to acquire donations for their jihad.⁹³

As the actors behind cyber attacks evolved, it was only a matter of time before militaries got involved in cyberspace.⁹⁴ First, militaries implemented cyberspace in intelligence gathering.⁹⁵ Second, militaries used cyberspace in covert operations, and, eventually, cyber warfare became a modern part of warfare.⁹⁶

In its infancy, the Internet was used by militaries for intelligence gathering and espionage.⁹⁷ The most

⁹¹ See Steve Coll & Susan B. Glasser, *Terrorist Turn to the Web as Base of Operations*, WASH. POST, Aug. 7, 2005, available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html>.

⁹² See Gabriel Weimann, *www.terror.net: How Modern Terrorism Uses the Internet*, ASIAN TRIBUNE, Fed. 21, 2007, available at <http://www.asiantribune.com/node/4627>.

⁹³ *Id.*

⁹⁴ See e.g., *U.S. Cyber Command*, UNITED STATES STRATEGIC COMMAND (last visited Nov. 5, 2011) http://www.stratcom.mil/factsheets/cyber_command/ (Established in 2009, Cyber Command “is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks, and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries.”).

⁹⁵ C.f. James Andrew Lewis, *The Cyber War Has not Begun*, Center For Strategic international Studies 1—3 (2010) (cyberspace is widely used for espionage).

⁹⁶ See Jon Swaine, *Georgia: Russia 'conducting cyber war'*, THE TELEGRAPH (Aug. 11, 2008, 11:11 AM), <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> (Russia allegedly attacked Georgian government websites in a cyber war).

⁹⁷ See e.g., Nathan Thornburgh, *The Invasion of the Chinese Cyberspies*, TIME MAGAZINE (2005).

famous example of cyber espionage is allegedly attributable to China against the United States.⁹⁸ Classified as operation “Titan Rain,” it was a series of ongoing cyber attacks that occurred against United States computer systems beginning in 2003.⁹⁹ The intrusions allegedly harvested massive amounts of government secrets.¹⁰⁰ Equally illustrative is the cyber attack classified as “Moonlight Maze.”¹⁰¹ Russia, through cyber espionage, infiltrated DOD networks for over a year and stole information pertaining to the Department of Energy and NASA.¹⁰²

Militaries then realized the potential of cyberspace beyond espionage, and they implemented it in covert operations.¹⁰³ For instance, during the Cold War, CIA agents were able to hack into the industrial control systems of a Soviet gas pipeline.¹⁰⁴ The CIA installed a Logic Bomb in the pipeline’s operating system, which caused the software to go haywire.¹⁰⁵ The pipeline exploded, causing the biggest non-nuclear explosion in history.¹⁰⁶ Recently, Israel hacked into Syria’s air defense systems and disabled them in a covert

⁹⁸ *Id.*

⁹⁹ Shaap, *supra* note 58, at 141.

¹⁰⁰ See Nathan Thornburgh, *Inside the Chinese Hack Attacks*, TIME MAGAZINE, Aug. 25, 2005, available at <http://www.time.com/time/nation/article/0,8599,1098371,00.html>.

¹⁰¹ Shaap, *supra* note 58, at 141.

¹⁰² *Id.*

¹⁰³ *C.f.* John Markoff, *A Silent Attack, but Not a Subtle One*, N.Y. TIMES, Sep. 26, 2010 (The United States and Israeli Government allegedly used the Stuxnet virus to disrupt the Iranian nuclear program).

¹⁰⁴ See generally, Thomas C. Reed, *At the Abyss: An Insider’s History of the Cold War* (2004).

¹⁰⁵ Kim Zetter, *Future of Cyber Security: What Are the Rules of Engagement?*, WIRED MAGAZINE, July 28, 2009, http://www.wired.com/dualperspectives/article/news/2009/07/dp_sec_arity_ars0728.

¹⁰⁶ *Id.*

operation in 2007.¹⁰⁷ Israel then bombed suspected nuclear facilities in Syria.¹⁰⁸ The attacks were a complete success because Syria was unaware Israel had attacked.¹⁰⁹ The Israeli air force was able to fly over the Syrian airspace with impunity.¹¹⁰

Once governments began using cyber weapons for espionage and covert operations, using cyber weapons in conjunction with actual war naturally followed.¹¹¹ The 2008 conflict between Russian and Georgia is elucidatory.¹¹² The conflict broke out over South Ossetia, a demilitarized Georgian region on the

¹⁰⁷ See Sharon Weinberger, *How Israel Spoofed Syria's Air Defense System*, WIRED MAGAZINE, Oct. 4, 2007, <http://www.wired.com/dangerroom/2007/10/how-israel-spoof/>.

¹⁰⁸ See Kim Zetter, *Mossad Hacked Syrian Official's Computer Before Bombing Mysterious Facility*, WIRED MAGAZINE, NOV. 3, 2009, <http://www.wired.com/threatlevel/2009/11/mossad-hack/>.

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² See Eneken Tikk et al., *Cyber Attacks Against Georgia: Legal Lesson Identified 4* (2008); see also Jim Nichol, *CSR Report for Congress, Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interests 4* (2008) ("In the early 1990s, Georgia and its breakaway South Ossetia region had agreed to a Russian-mediated ceasefire that provided for Russian "peacekeepers" to be stationed in the region. Moscow extended citizenship and passports to most ethnic Ossetians. Simmering long-time tensions erupted on the evening of August 7, 2008, when South Ossetia and Georgia accused each other of launching intense artillery barrages against each other. Georgia claims that South Ossetian forces did not respond to a ceasefire appeal but intensified their shelling, "forcing" Georgia to send in troops. On August 8, Russia launched large-scale air attacks and dispatched troops to South Ossetia that engaged Georgian forces later in the day. By the morning of August 10, Russian troops had occupied the bulk of South Ossetia, reached its border with the rest of Georgia, and were shelling areas across the border. Russian troops occupied several Georgian cities. Russian warships landed troops in Georgia's breakaway Abkhazia region and took up positions off Georgia's Black Sea coast.").

border with Russia.¹¹³ Georgia launched an attack against separatist forces rising up in South Ossetia.¹¹⁴ Russia responded by sending military forces to protect the Ossetia rebels.¹¹⁵ Georgia viewed Russia's military invasion of South Ossetia as a direct act of aggression.¹¹⁶

In the weeks leading up to the conflict of South Ossetia, Russia launched a cyber offensive against Georgia.¹¹⁷ The cyber attacks primarily consisted of propaganda and DDOS attacks.¹¹⁸ For instance, government websites were defaced and replaced with pictures of Adolph Hitler and Mikheil Saakashvili.¹¹⁹ Although the propaganda efforts were juvenile, the DDOS attacks had a real effect on the Georgian people.¹²⁰ The DDOS attacks crippled government web servers, general e-mail servers, news and media websites, and financial websites.¹²¹ Consequently, the attacks: prevented the Georgians from communicating, causing massive confusion throughout the country,¹²² prevented them from acquiring accurate information

¹¹³ Tikk, *supra* note 112, at 4.

¹¹⁴ Nichol, *supra* note 112, at 4.

¹¹⁵ *Id.* at 5.

¹¹⁶ *Id.*

¹¹⁷ TIKK, *supra* note 112, at 4.

¹¹⁸ *Id.* at 7.

¹¹⁹ Clarke, *supra* note 42, at 19.

¹²⁰ *Id.* Georgia connects to the Internet primarily through Russia. *Id.* Because of the DDOS attacks coming into the country, no outbound Internet traffic could get out. *Id.* Georgians could not connect to outside news sources nor send e-mail out of the country. *Id.* "Georgia effectively lost control of the nation's '.ge' domain and was forced to shift many government websites to servers outside the country." *Id.*

¹²¹ See e.g., John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 12, 2008.

¹²² See Lesley Swanson, The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, 32 LOY. L.A. INT'L & COMP. L. REV. 303, 303—04 (2010).

about the war escalation;¹²³ and prevented them from accessing their banking services.¹²⁴

“Whether the world is prepared or not, cyber weapons are becoming a staple of modern war.”¹²⁵ This new weapon uses a target nation’s own technology against it to create an asymmetric war.¹²⁶ For example, military strategist envision China using cyber attacks against the United States,¹²⁷ not in an outright offensive, but to delay the United States long enough for China to seize Taiwan or the disputed islands in the South Sea.¹²⁸

¹²³ Tikk, *supra* note 112, at 8. Georgia’s access to media outlets like CNN and BBC were also blocked. See Clarke, *supra* note 42, at 18.

¹²⁴ Tikk, *supra* note 112, at 8—9. The Georgian banking sector shut down its servers in response to the attacks to prevent from being hacked. Clarke, *supra* note 42, at 19–20. Russia countered by sending DDOS attacks throughout the international banking community, pretending to be DDOS attacks from Georgia. *Id.* Foreign banks in response shut down their connection to the Georgian banking sector. *Id.*

¹²⁵ Swanson, *supra* note 122, at 304.

¹²⁶ *Id.*; see also QIAO LIANG & WANG XIANGSUI, UNRESTRICTED WARFARE: CHINA’S MASTER PLAN TO DESTROY AMERICA 1 (2002) (Asymmetric warfare is a military doctrine in which weaker countries can outmatch traditional military powers by using weapons and tactics that take advantage of weaknesses in superior conventional capabilities).

¹²⁷ See generally, Jason Fritz, *How China Will Use Cyber Warfare to Leapfrog in Military Competiveness*, 8 CULTURE MANDALA 28 (2008). “By the end of the 1990s, China’s strategists had converged on the idea that cyber warfare could be used by China to make up for its qualitative military deficiencies when compared to the United States.” Clarke, *supra* note 42, at 50.

¹²⁸ See Benjamin Kong, *Cyberwar: War in the Fifth Domain*, ECONOMIST, July 1, 2010, available at <http://www.economist.com/node/16478792/comments>. Analyst believe China will find itself with Taiwan in conflict over control of the South Sea. Clarke, *supra* note 42, at 61. The South Sea is highly sought after because it contains undeveloped oil fields estimated to have more natural gas than Kuwait. *Id.*

The following hypothetical illustrates how cyber warfare will be used against the United States:

China has aggressively been pressing other Asian countries to cede their rights to the South Sea. The United States learns that China is preparing for an amphibious landing on the disputed islands in the South Sea. In response, the United States dispatches two U.S. battles groups, including twenty ships and over a hundred aircraft, to the region to deter the Chinese. To send a message to the Chinese, the United States hacks the Chinese power grid, causing rolling blackouts throughout the country. In rebuttal, the Chinese: cause black outs throughout Hawaii, California, and Washington; take down the DOD network; and are prepared to launch a broad attack against the United States' rail network, air traffic control systems, and the financial markets. Realizing the vulnerabilities to the United States, the President is forced to back down and orders the troops to cease offensive action. The Chinese have just used cyber warfare to neutralize the traditional military might of the United States.¹²⁹

III. DANGERS TO CRITICAL INFRASTRUCTURE

The threat facing the United States is that the United States' critical infrastructure will be attacked through cyber warfare.¹³⁰ Critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any

¹²⁹ Clarke, *supra* note 42, at 179—88.

¹³⁰ Natasha Solce, *supra* note 43, at 302 (critical infrastructures in the United States are in more danger of attack because they are now connected to the domain of cyberspace).

combination of those matters.”¹³¹ The following sectors have been identified as critical infrastructure: agriculture, food, water, public health, emergency services, defense industrial base, government, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, and postal and shipping.¹³²

Cyber attacks pose real dangers to the critical infrastructure of the United States.¹³³ First, cyber attacks aimed at the energy industry pose significant dangers.¹³⁴

¹³¹ USA PATRIOT ACT, Pub. L. No. 107—56, 115 Stat. 272 (2001). This paper defines “critical infrastructure” to only encompass the energy, finance, and telecommunications sectors. *See e.g.*, CSIS, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 44 (2008). “These critical cyber sectors are large, interconnected national networks that are the most vulnerable to broad disruption by cyber attack.” *Id.* at 45. Although water systems, emergency services, transportation networks, and health care services are all vital to the United States, they are decentralized to a local level, and are less likely to be adversely affected from a cyber attack. *Id.* (“[P]enetrating and disrupting the water supply of one large city, for example, will not disrupt water supplies elsewhere. If these three networks... can continue to operate in the face of attack, the nation can persevere in cyberspace. If they are crippled, online activities will come to an abrupt halt.”). By contrast, damage to energy, finance, or telecommunication sectors would have a debilitating affect on the United States, because they are nationally connected. *Id.*

¹³² *See generally*, The President of the United States, National Strategy for Homeland Security 30 (2003).

¹³³ *See e.g.*, U.S. Gov’t Accountability Office, GAO-11-463T, Cybersecurity: Continued Attention Needed to Protect Our Nation’s Critical Infrastructure and Federal Information Systems 3 (2011). “Federal law enforcement and intelligence agencies have identified multiple sources of threats to our nation’s critical information systems, including foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors.” *Id.* “The connectivity between information systems, the Internet, and other infrastructures also creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services.” *Id.*

¹³⁴ *Id.* at 1.

For example, in 2003, the SQL Slammer Worm¹³⁵ was able to infiltrate the network systems in the Ohioan Davis-Besse nuclear power plant.¹³⁶ It was able to corrupt the facilities' computer control systems for approximately five hours.¹³⁷ Although the breach did not pose any significant safety hazard, the incident illustrates the growing cyber security problem in critical infrastructure.¹³⁸ The Stuxnet virus is also illustrative.¹³⁹

¹³⁵ W32.SQLEXP.Worm, SYMANTEC (last visited Nov. 28, 2011), www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-99 (The SQL Slammer is a computer worm that indiscriminately spread DDOS attacks across the Internet. The worm was so successful that it dramatically slowed down general Internet traffic).

¹³⁶ Natasha Solce, *supra* note 43, at 302.

¹³⁷ Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant Network*, SECURITY FOCUS, Aug. 19, 2003, <http://www.securityfocus.com/news/6767>.

¹³⁸ *Id.* ("Experts disagree about the vulnerability of systems that run industrial plants, known as supervisory control and data acquisition (SCADA). But more and more of these are being connected to the internet [sic], raising the risk of remote attack. 'Smart' grids, which relay information about energy use to utilities, are promoted as ways of reducing energy waste. But they also increase security worries about both crime (e.g., allowing bills to be falsified) and exposing SCADA networks to attack."). See Benjamin Kong, *Cyberwar: War in the Fifth Domain*, ECONOMIST, July 1, 2010, [available at http://www.economist.com/node/16478792/comments](http://www.economist.com/node/16478792/comments). Operation Night Dragon is also illustrative of the dangers to critical infrastructure. McAfee, GLOBAL ENERGY CYBER ATTACKS: "NIGHT DRAGON" 3 (2011). Classified as Night Dragon, there have been a series of coordinated cyber attacks that occurred against the oil, energy, and petrochemical sectors since 2009. *Id.* These attacks have utilized vulnerabilities in Microsoft Windows operating systems to harvest sensitive proprietary information. *Id.* The attacks have been attributable to China. *Id.* at 4.

¹³⁹ See Bruce Schneier, *The Story Behind the Stuxnet Virus*, Forbes, Oct. 7, 2010, [available at http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html](http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html).

The United States and Israeli government allegedly created Stuxnet to disrupt the Iranian nuclear facility in Natanz.¹⁴⁰ Stuxnet reportedly infected one fifth of Iran's nuclear centrifuges causing them to malfunction.¹⁴¹ This has reportedly delayed Iran's ability to create a nuclear bomb.¹⁴²

¹⁴⁰ *Id.* The true identity of the attackers is unknown, yet it is highly suspected that the United States and/or Israel were involved. *Id.* It is suspected that Stuxnet was created by a government entity because the worm was not criminal in design, it was expensive to create, and because the inscription "myrtus" appears in the worm's code, suggesting Israeli involvement. *Id.* Stuxnet appears to not be criminal designed because the worm does not steal credit card information or herd computers into botnets. *Id.* Because it is estimated that it took eight to ten people six months to create the virus, Stuxnet was most likely financed by a government. *Id.* Further, the word "myrtus" has been linked to Israel because "myrtus" is Hebrew for Hadassah: Queen Esther who saved the Persian Jews from genocide. *Id.*

¹⁴¹ Specifically, Stuxnet is an Internet worm that primarily infects computers through USB sticks. Bruce Schneier, *supra* note 139. Once it has gained access to the host computer, it seeks to infiltrate SCADA systems: industrial control systems generally used in critical infrastructure, e.g., the electric power grid, gas pipelines, and nuclear facilities. Pam Benson, *Computer virus Stuxnet a 'game changer,' DHS official tells Senate*, CNN, Nov. 17, 2010, available at http://articles.cnn.com/2010-11-17/tech/stuxnet.virus_1_stuxnet-nuclear-power-plants-target?_s=PM:TECH. The worm then manipulates the SCADA systems and sends false instructions to the industrial control systems, causing the systems to malfunction. Bruce Schneier, *supra* note 139.

¹⁴² William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, available at <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>.

Second, the financial sectors are also in danger of cyber attacks.¹⁴³ In theory, a hostile entity could infiltrate a victim state's financial sector through a well-crafted cyber attack.¹⁴⁴ Because documentation of wealth and property are generally stored on computer systems, a cyber attack could delete, alter, or crash financial stock markets and paralyze a nation's economy.¹⁴⁵ However, a cyber attack on the financial industry from a nation-state is unlikely because the "cascade effect of international economic interdependency, deters cyber attacks against...financial programs."¹⁴⁶ Nonetheless, a cyber attack on the financial industry of any nation is plausible because cyber terrorists are not influenced by economic

¹⁴³ See U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-03-173, CRITICAL INFRASTRUCTURE PROT.: EFFORTS OF THE FIN. SERV. SECTOR TO ADDRESS CYBER THREATS 22 (2003). Over eighty percent of the financial institutions have had security breaches. *Id.* Financial losses from stolen proprietary information and fraud are in the hundreds of millions. *Id.* Specifically, in 1994, a Russian hacker reportedly broke into Citibank's network and stole \$10 million. *Id.* at 23. Although the hacker was convicted of a felony, Citibank was only able to recover \$400,000 of that loss. *Id.* Additionally, in 2000, two men from Kazakhstan were arrested in London for breaking into Bloomberg L.P.'s computer systems in New York in an attempt to extort \$200,000. *Id.*

¹⁴⁴ See e.g., Josh Smith, *Financial Industry Especially Vulnerable to Cyberattacks, Analysts Say*, NATIONAL JOURNAL, Sep. 14, 2011, <http://www.nationaljournal.com/tech/financial-industry-especially-vulnerable-to-cyberattacks-analysts-say-20110914> ("Because financial institutions are critical to the nation's economic security and handle large sums of money, malicious actors find them to be especially attractive targets.").

¹⁴⁵ CRS REPORT FOR CONGRESS, COMPUTER ATTACK AND CYBER TERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 9—11 (2003). "For example, cyber attacks that secretly corrupt secure credit card transaction data at retail Internet sites, could possibly cause that corrupted data to spread into banking systems and could erode public confidence in the financial sector, or in other computer systems used for global commerce." *Id.*

¹⁴⁶ Natasha Solce, *supra* note 43, at 310.

deterrence.¹⁴⁷ Thus, the financial sector could be a possible target.¹⁴⁸

Third, the dangers posed to civilian government infrastructure are apparent.¹⁴⁹ As governments become more connected, they will be more vulnerable to cyber attacks.¹⁵⁰ The case of Estonia, “e-Stonia,”¹⁵¹ is especially elucidatory.¹⁵² By 2007, Estonia had implemented an online government where ninety percent of governmental services were conducted online.¹⁵³ Estonians conducted most banking through online services, voted for parliamentary elections online, and mostly communicated through Skype, an Internet phone system.¹⁵⁴ Estonia’s dependence on the Internet made cyber attacks against it extremely effective.¹⁵⁵ The cyber attacks occurred because Estonia decided to relocate the Bronze Soldier Tallinn, a soviet-era grave marker honoring fallen soviet soldiers during World War II.¹⁵⁶ In protest, thousands of DDOS attacks from Russia flooded Estonia.¹⁵⁷ The attacks brought down critical

¹⁴⁷ *Id.*

¹⁴⁸ *C.f.* Smith, *supra* note 144.

¹⁴⁹ See Joshua Davis, Hackers Take Down the Most Wired Country in Europe, WIRED MAGAZINE, Aug. 21, 2007.

¹⁵⁰ See *e.g.*, Myriam Dunn Cavelty, Critical information infrastructure: vulnerabilities, threats and responses 17 (2007).

¹⁵¹ How the Tiny Baltic Nation of Estonia is Using its Technological Prowess to Survive in Tough Economic Times, PUBLIC RADIO INTERNATIONAL, Mar. 20, 2009, <http://www.pri.org/stories/world/e-stonia.html>.

¹⁵² See Scott Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, 27 BERKELEY J. INT’L L. 192, 193 (2009).

¹⁵³ *Id.*

¹⁵⁴ *Id.*

¹⁵⁵ *Id.*

¹⁵⁶ Davis, *supra* note 149.

¹⁵⁷ Shackelford, *supra* note 152, at 193.

governmental websites and caused social unrest and rioting.¹⁵⁸

In review, critical infrastructures are defined as those infrastructures so vital to the United States that their destruction would debilitate the country.¹⁵⁹ Cyber attacks have been able to infiltrate nuclear power plants and pose security threats to the electric grid.¹⁶⁰ The financial sector could be decimated by an orchestrated cyber attack.¹⁶¹ Additionally, disruptions to government infrastructure can lead to mass confusion and social unrest.¹⁶² The foregoing evidences the dangers cyber attacks pose to critical infrastructure.¹⁶³

IV. THE LAWLESSNESS OF CYBER WARFARE AND WHY CYBER WARFARE WILL NOT BE STOPPED

No international treaty governs cyber warfare.¹⁶⁴ Consequently, nations must practice law by analogy, applying various legal theories to cyber attacks.¹⁶⁵ However, applying other theories to cyber warfare by analogy does not provide a workable model to govern

¹⁵⁸ *Id.* at 194.

¹⁵⁹ See USA PATRIOT ACT, Pub. L. No. 107—56, 115 Stat. 272 (2001).

¹⁶⁰ See e.g., Schneier, *supra* note 139.

¹⁶¹ See Smith, *supra* note 144.

¹⁶² Shackelford, *supra* note 152, at 193.

¹⁶³ See e.g., George Kurtz, *Critical Infrastructure Not Ready For Cyberattacks*, MCAFEE BLOG CENTRAL (April 20, 2011, 12:38 PM), <http://blogs.mcafee.com/corporate/cto/critical-infrastructure-not-ready-for-cyberattacks> (there is an increased danger to the oil, gas, power, and water industries).

¹⁶⁴ See Christina Hernandez Sherwood, *Cyberwar: Few Rules Govern A Growing Global Threat*, SMART PLANET BLOG (Oct. 28, 2010, 4:00 AM), <http://www.smartplanet.com/blog/pure-genius/cyberwar-few-rules-govern-a-growing-global-threat/4789>.

¹⁶⁵ Carr, *supra* note 44, at 47.

cyber warfare.¹⁶⁶ Alternatively, if actual international legislation is agreed upon to govern cyber warfare, cyber warfare will continue because the responsibility for cyber attacks cannot be attributable to a nation-state, regulating cyber warfare would be impractical, and because weaker military nations will use cyber warfare to combat larger military forces.¹⁶⁷

A. THE FIRST RULE OF CYBER WARFARE, THERE ARE NO RULES OF CYBER WARFARE

The law of cyber warfare is unclear.¹⁶⁸ “Right now, no comprehensive international treaty exists to regulate cyber attacks. Consequently, states must practice law by analogy either equating cyber attacks to traditional armed attacks and responding to them under the law of war or equating them to criminal activity and dealing with them under domestic criminal laws.”¹⁶⁹ Currently, academics have theorized that cyber warfare could be internationally governed by analogizing it to: (1) the Nuclear Non-Proliferation Treaty, (2) the United Nations Charter, or (3) the Outer Space Treaty or the

¹⁶⁶ See e.g., Tom Gjelten, *Extending The Law Of War To Cyberspace*, NPR, Sep. 22, 2010, <http://www.npr.org/templates/story/story.php?storyId=130023318> (understanding the difficulty in attributing responsibility for cyber attacks); but see generally, DONDI S. WEST, A SURVEY AND EXAMINATION OF THE ADEQUACY OF THE LAWS RELATED TO CYBER WARFARE 1 (2010) (arguing that the U.N. Charter should govern cyber war).

¹⁶⁷ See *infra* Part III-B.

¹⁶⁸ Carr, *supra* note 44, at 47.

¹⁶⁹ *Id.*

Antarctic Treaty System.¹⁷⁰ This article argues that none of these analogies provides a workable model to govern cyber warfare.¹⁷¹

¹⁷⁰ See e.g., Shackelford, *supra* note 152, at 150. Some theorists have explained that Mutual Legal Assistance Treaties (“MLATs”) could govern cyber warfare. See generally, Carr, *supra* note 44. MLATs encompass everything from diplomatic relations, extradition, or legal assistance. Shackelford, *supra* note 152, at 228. Specifically, they can be applied to seek criminal prosecution of individuals responsible for cyber attacks, and their extradition to a requesting nation. Shackelford, *supra* note 152, at 228. For example, the Convention on Cybercrime is the first international treaty to address cybercrime by standardizing national laws. See e.g., Amile M. Weber, *The Council of Europe’s Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425 (2003). The convention mandates a list of crimes that each signatory must create into their own law: criminalization of hacking, Internet child pornography, and the increase of liability for intellectual property violations. Budapest, 23.XI.2001. The convention also requires signatory nations to provide international cooperation for international cyber crimes, including the collection of evidence, and the police assistance from participating nations. *Id.* This paper does not address MLATs because they pertain to criminal matters. Accordingly, they have no weight in addressing international warfare.

Theorists have also analogized the law of the sea to cyberspace. See Shackelford, *supra* note 152, at 227. According to UNCLOS Article 19, nations have an obligation to not engage in activities “prejudicial to the peace, good order, or security of the coastal [s]tate.” See United Nations Convention on the Law of the Sea art. 19, Dec. 10, 1982, 1833 U.N.T.S. 243; see also Shackelford, *supra* note 152 at 227 (Nations also have an obligation not to engage in activities such as the collection of information, propaganda, or interfering with telecommunications systems). Additionally, UNCLOS Article 113 requires domestic criminal legislation to penalize intentional damage to submarine cables. United Nations Convention on the Law of the Sea art. 13, Dec. 10, 1982, 1833 U.N.T.S. 243. Applied to cyberspace, “this means that cyber attackers who send code through submarine cables to a coastal state would be in breach of international law obligations.” Shackelford, *supra* note 152, at 227. Similar to MLAT, UNCLOS enforcement mechanism is based on criminal law enforcement and is not addressed in this article.

1. THE NUCLEAR NON-PROLIFERATION TREATY

Some academics have compared nuclear weapons to that of an escalated cyber attack.¹⁷² Accordingly, theorists have suggested that it would be appropriate for a nonproliferation treaty to regulate cyber warfare.¹⁷³ For example, the Nuclear Non-Proliferation Treaty (“NPT”) is an international agreement to limit the spread of nuclear weapons.¹⁷⁴ Each member of the treaty agrees to not transfer nuclear weapons, nor induce any non-nuclear weapon state from developing nuclear weapons.¹⁷⁵ The members also agree to be regulated by the International Atomic Energy Agency (“IAEA”) to

¹⁷¹ See Charles J. Dunlap, *Towards A Cyberspace Legal Regime in the Twenty-First Century: Consideration for American Cyber Warriors*, 87 NEB. L. REV. 712, 714 (discussing the complexities in applying existing law to cyber war issues).

¹⁷² Cyber attacks have been compared to weapons of mass destruction. See e.g., Shackelford, *supra* note 152, at 150, 216 (the Russians have also stated that an attack against the United States’ telecommunications and electric grid would necessarily overlap with the use of weapons of mass destruction); see also Paul Mann, *Cyber-threat Expands with Unchecked Speed*, 145 AVIATION WEEK & SPACE TECH. 63, 64 (1996) (According to former CIA Director John Deutch, cyber warfare is categorized slightly under nuclear, biological, or chemical weapons). Both types of attacks would be unable to distinguish between the civilian and military populations. Shackelford, *supra* note 152, at 218. Further, both types of attacks would “destroy all critical infrastructures, leave the victim nation completely helpless and terrorize its population.” *Id.* “Some of the effects of nuclear weapons can be similar to a worst-case cyber attack on a state. An all-out attack could disable or destroy all critical infrastructures, leave the victim nation completely helpless and terrorize its population.” *Id.* Cyber attacks may be even more harmful to the civilian population because of the anticipated focus on critical infrastructure. Shackelford, *supra* note 152, at 219.

¹⁷³ Shackelford, *supra* note 152, at 219.

¹⁷⁴ Treaty on the Non-Proliferation of Nuclear Weapons art. 1, July 1, 1968, 729 U.N.T.S. 168.

¹⁷⁵ *Id.*

verify that they are not diverting nuclear energy from peaceful use to explosive devices.¹⁷⁶ A cyber warfare nonproliferation treaty could stop the escalation of cyber warfare, ban the creation of cyber weapons, and protect the international community by regulated safeguards.¹⁷⁷

Although a nonproliferation treaty could be applied to cyber warfare in theory, the implementation of the treaty would be unworkable because: (a) there is no international oversight agency that could regulate cyber warfare, and (b) cyber weapons cannot be verified by independent government reconnaissance. First, the NPT is enforceable because the materials required to create a nuclear device are rare.¹⁷⁸ Because nuclear materials are rare, the IAEA is able to monitor and trace them.¹⁷⁹ Conversely, the creation of cyber weapons is vast because it only requires programmers and computer hardware.¹⁸⁰ The abundance of cyber weapons makes it impractical to trace them.¹⁸¹ Further, regulators would need access to all computer databases within a nation, and have the resources to search through billions of lines of code.¹⁸² This is impractical because malicious code

¹⁷⁶ Treaty on the Non-Proliferation of Nuclear Weapons art. 3, July 1, 1968, 729 U.N.T.S. 168.

¹⁷⁷ C.f. Charles Bwele, *Can Deterrence Work in Cyberspace?*, DIPLOWEB, June 13, 2010, <http://www.diploweb.com/Can-deterrence-work-in-cyberspace.html>.

¹⁷⁸ Carr, *supra* note 44, at 32.

¹⁷⁹ *Id.*

¹⁸⁰ Technolytics, Department of Cyber Defense: An Organization Who's Time Has Come! 1—5 (2007).

¹⁸¹ Shackelford, *supra* note 152, at 217. "This difficulty stems from the fact that the computer code that compromise IW are often indistinguishable from innocent information requests." *Id.*

¹⁸² See e.g., CRS Report for Congress, Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress 18 (2003).

created for cyber warfare is often indistinguishable from other innocent data.¹⁸³

Second, nation-states would not be able to verify the existence of cyber weapons through traditional intelligence gathering.¹⁸⁴ The NPT is also enforceable because nations can independently determine nuclear activity in other countries, e.g., spy satellites can verify the creation of nuclear weapons programs.¹⁸⁵ Conversely, cyber weapons can be made anywhere there is an Internet connection.¹⁸⁶ Cyber warriors operate completely invisible from the international community.¹⁸⁷

2. THE UNITED NATIONS CHARTER

Other academics have proposed that the United Nations Charter (“U.N. Charter”) could govern cyber warfare.¹⁸⁸ The U.N. Charter and customary international law governs the use of force by states.¹⁸⁹ It provides the legal framework to understand the availability and limitations on the use of force.¹⁹⁰ Accordingly, theorists

¹⁸³ Shackelford, *supra* note 152, at 217.

¹⁸⁴ See *infra* Part III-B.

¹⁸⁵ See e.g., David E. Sanger & William J. Broad, *Watchdog Finds Evidence That Iran Worked on Nuclear Triggers*, N.Y. TIMES, May 24, 2011.

¹⁸⁶ See Michael Vatis, *Cyber Attacks: Protecting America’s Security Against Digital Threats* 2 (2002); Angel T. Redoble, *An Open Source Research and Analysis On Cyber Weapons Proliferation And Deterrence* 3 (2010).

¹⁸⁷ *Id.*

¹⁸⁸ See e.g., Shaap, *supra* note 58, at 142.

¹⁸⁹ See Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT’L L. STUD. 99, 99 (2002).

¹⁹⁰ McGavran, *supra* note 50, at 269.

suggested that it is appropriate to apply the U.N. Charter to cyber warfare.¹⁹¹

The U.N. Charter prohibits the use of force unless two exceptions apply.¹⁹² According to Article 2(4) of the U.N. Charter: “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.” (emphasis added).¹⁹³

The two exceptions to the prohibition on the use of force are as follows.¹⁹⁴ First, Article 42 permits the Security Council to authorize the use of force to combat any threat to the peace or an act of aggression in order to bring international stability.¹⁹⁵ Second, Article 51 provides: “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 measures necessary to maintain international peace and security.” (emphasis added).¹⁹⁶

Unfortunately, the U.N. Charter does not define “use of force” or “armed attack.”¹⁹⁷ Nonetheless, there is an international consensus that “use of force” or “armed

¹⁹¹ *Id.* The Law of Armed Conflict (“LOAC”) provides the legal framework for modern warfare. Lin, *infra* note 194, at 71. The LOAC is divided into two separate bodies of law: *jus ad bellum*—when it is legal for one nation to use force against another—and *jus in bello*—the rules that govern nations once they are engaged in war. *Id.* The U.N. Charter and customary international law govern *jus ad bellum*. *Id.* .

¹⁹² *Id.*

¹⁹³ U.N. Charter art. 2(4).

¹⁹⁴ See Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT’L SEC. L. & POL’Y 63, 71 (2010).

¹⁹⁵ U.N. Charter art. 42.

¹⁹⁶ U.N. Charter art. 51.

¹⁹⁷ Lin, *supra* note 194, at 71.

attack” means “military force.”¹⁹⁸ For example, declaring war, the occupation of territory, or naval blockades would constitute an armed attack.¹⁹⁹ However, economic coercion would not constitute a use of force.²⁰⁰ For instance, economic sanctions, space-based surveillance, espionage, or political coercion do not amount to a “use of force.”²⁰¹

Regrettably, there is no consensus for how cyber attacks should be regarded under the U.N. Charter.²⁰² The first issue is whether a cyber attack *can* amount to a “use of force” under Article 2(4), or an “armed attack” under Article 51 giving rise to a right of self-defense.²⁰³ Most academics generally believe that a cyber attack could amount to a use of force or an armed attack if it is severe enough.²⁰⁴ Accordingly, the next problem is

¹⁹⁸ *Id.* It is assumed that unfriendly actions such as “unfavorable trade decisions, space-based surveillance, boycotts, severances of diplomatic relations, denial of communications, espionage, economic competition or sanctions, and economic and political coercion do not rise to the threshold of a use of force, regardless of the scale of their effects.” *Id.* at 71–72. *See also* *Nicaragua v. United States*, 1986 I.C.J. 14, 106 (June 27) (“every sovereign [s]tate [has a right] to conduct its affairs without outside interference... [this] is part and parcel of customary international law.”).

¹⁹⁹ Lin, *supra* note 194, at 71.

²⁰⁰ *Id.*

²⁰¹ *Id.*

²⁰² *See e.g.*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT’L SEC. L. POL’Y 87, 90 (2010).

²⁰³ *Id.*; McGavran, *supra* note 50, at 269–70. There are three approaches in analyzing cyber attacks under the U.N. Charter. *Id.* The “Instrumentality approach” would define cyber attacks as being outside the definition of “force” because they are inherently different from kinetic attacks. *Id.* Under the “Target approach,” cyber attacks would constitute “force” if they were able to penetrate critical infrastructures within a nation. *Id.* Under the “Consequentiality approach,” a cyber attack would constitute “force” if it were able to replicate the same damage a traditional kinetic attack could. *Id.*

²⁰⁴ Michael N. Schmitt, Computer network attack and the use of force in international law: thoughts on a normative framework.

determining between cyber attacks that are military force or economic coercion.²⁰⁵

The application of the U.N. Charter to cyber warfare is problematic because cyber warfare can be defined as both military force and economic force.²⁰⁶ The majority view among international scholars is that “use of force” only encompasses the use of military force, *i.e.*, kinetic attacks.²⁰⁷ Economic coercion, such as sanctions, is excluded from the definition.²⁰⁸ A cyber attack can be classified as military force because it could physically, through virtual cyber attacks, destroy operating systems, destroy economic infrastructure, and paralyze a nation’s wealth.²⁰⁹ Alternatively, a cyber attack can also be classified as economic coercion because it could affect the economic infrastructure of a nation by attacking financial markets or otherwise disrupting an economy.²¹⁰

The following is an example that illustrates the problem in determining whether a cyber attack is military force or economic coercion:

Bombs dropped on [the United States’] stock exchange at night, so that casualties were minimized, would be regarded as a use of force or armed attack by most observers, even if physical backup facilities were promptly available so that actual trading was disrupted for only a few hours. The posited cyber attack could have the same

²⁰⁵ See Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), 36 YALE J. INT’L L. 421, 426—37.

²⁰⁶ *Id.* at 422.

²⁰⁷ See LIEUTENANT COLONEL SCOTT W. BEIDLEMAN, DEFINING AND DETERRING CYBER WAR 15 (2009); see also Antolin-Jenkins, *supra* note 34, at 152—53.

²⁰⁸ *Id.*

²⁰⁹ *Id.*

²¹⁰ *C.f.* Antolin-Jenkins, *supra* note 34, at 155.

economic effects, except that the buildings themselves would not be destroyed. In this case, the cyber attack may be less likely to be regarded as a use of force than a kinetic attack with the same (temporary) economic effect, simply because the lack of physical destruction would reduce the scale of the damage caused. However, a cyber attack against the stock exchanges that occurs repeatedly and continually, so that trading is disrupted for an extended period of time, for days or weeks, would surely constitute a use of force or even an armed attack, even if no buildings were destroyed.²¹¹

Because of the difficulty in determining whether a cyber attack is a military force or an economic force, resolving whether a cyber attack is a use of force or armed attack must be determined on a case-by-case basis.²¹² “Some commentators have charted a spectrum of action, where a minor incursion into the sovereign territory of a state with a minimum use of force does not give rise to right to act in self-defense, whereas a more robust action, either causing significant destruction or targeting, does.”²¹³ For example, electronic espionage and the interruption of telecommunications systems may not amount to an armed attack, where a DDOS attack

²¹¹ Lin, *supra* note 194, at 74.

²¹² WALTER GARY SHARP SR., *CYBERSPACE AND THE USE OF FORCE* 135—42 (1999). “The terms ‘use of force,’ ‘armed attack,’ and ‘self-defense’ will never be clearly defined by objective rules of law. The international community has struggled for decades to define these terms, but there are simply too many factual variables involved to capture them in a few simple rules.” *Id.* at 138.

²¹³ Antolin-Jenkins, *supra* note 34, at 162.

could.²¹⁴ However, the determination of what constitutes military force or economic coercion would still be arbitrary.²¹⁵

Further, enforcing cyber warfare under the U.N. Charter would be challenging because it is difficult to attribute responsibility for cyber attacks.²¹⁶ The problem with cyber warfare is that it is extremely difficult to attribute an attack to a specific actor or to determine the intent behind the attack.²¹⁷ The U.N. Charter would only deter cyber warfare if states could retaliate when they have been the victims of a cyber attack.²¹⁸ Because states cannot attribute responsibility for an attack against them, they will be unable to respond with military action.²¹⁹ The lack of attribution in a cyber attack renders the U.N. Charter of limited use.²²⁰

Retaliation also requires attribution because it ensures that the retaliating state will not target innocent

²¹⁴ Joshua E. Kastenber, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 55 (2009) (the majority of the international community agrees that cyber attacks, such as DDOS attacks, violate the international principle of neutrality).

²¹⁵ C.f. Sharp, *supra* note 212, at 138.

²¹⁶ See Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SEC. L. POL'Y 155, 163 (2010) (responding to a cyber attack without properly determining attribution could violate the law of armed conflict).

²¹⁷ Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1, 13 (2010) ("Lacking the capability to determine the intent of the perpetrator makes it almost impossible to structure an appropriate, lawful response, and is likely to leaving a state guessing as to whether it was facing an imminent cyber attack or merely a teen-ager taking the family computer for a spin.").

²¹⁸ C.f. Shackelford, *supra* note 152, at 200.

²¹⁹ *Id.*

²²⁰ See generally, Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971 (2011).

entities.²²¹ A nation quick to react to an attack might wage war with another nation who they suspect is responsible, where in reality the attack came from somewhere else.²²² Further, retaliation requires attribution, because the laws governing self-defense depend on whether the attacker is a state actor or non-state actor.²²³ Retaliation in self-defense must comply with the U.N. Charter if the attacker is a state actor.²²⁴ However, if the attacker is a non-state entity then criminal law will govern the response measures.²²⁵ The victim state needs to be able to immediately attribute responsibility for the attack in order to comply with the legality of self-defense.²²⁶ Therefore, nation-states need to be able to attribute responsibility for cyber attacks for the U.N. Charter to be enforceable.²²⁷

²²¹ Sean M. Condrón, Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 HARV. J.L. & TECH. 403, 414 (2006).

²²² *Id.*

²²³ *Id.*

²²⁴ *Id.*

²²⁵ *Id.* at 415; see also Daniel M. Creekman, Note, A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks From China, 17 AM. U. INT'L L. REV. 641, 661 (2002).

²²⁶ Condrón, *supra* note 221, at 415.

²²⁷ *Id.*

3. THE OUTER SPACE TREATY AND THE ANTARCTIC TREATY SYSTEM

Cyberspace is sometimes referred to as an international “commons,”²²⁸ comparable to outer space²²⁹ or Antarctica.²³⁰ Accordingly, some theorists have explained that cyber warfare could be governed by analogy to the Outer Space Treaty (“OST”), or the Antarctic Treaty System (“ATS”).

i. *The Outer Space Treaty*

Theorists have explained space law could govern cyber warfare.²³¹ The OST states that “outer space, including the Moon and other celestial bodies” are not subject to a “claim of sovereignty, by means of use or occupation, or by any other means.”²³² The OST does

²²⁸ See Patrick W. Franzese, *Sovereignty in Cyberspace: Can it Exist?*, 64 A.F. L. REV. 1, 14—18 (2009) (discussing cyberspace under a global commons theory); Shackelford, *supra* note 152, at 213 (“As applied to cyberspace, this means that although computer networks owned by the private and public sectors provide the infrastructure for the information superhighway, they cannot actually own the data packets (the cars) on the Internet. Thus, the various government institutions and telecommunications firms that issue Internet protocol (IP) addresses within their countries do in a sense own Internet Access, but not the Internet itself.”); *but see* James A. Lewis, *Sovereignty and the Role of Government in Cyberspace*, 16 BROWN J. WORLD AFF. 55, 62 (2009) (although ownership of Internet networks are fragmented, ownership and sovereignty still exists, even if it is not usually enforced).

²²⁹ See Carr, *supra* note 44, at 33 (the comparisons to outer space are evident; both boundless and unregulated).

²³⁰ See generally, Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. & TECH. L. REV. 69 (1997).

²³¹ *Id.*

²³² The Outer Space Treaty art. 2, Jan. 1, 1967, 610 U.N.T.S. 205.

not prohibit the militarization of space.²³³ It only prohibits placing nuclear weapons, or weapons of mass destruction, in orbit, or placing them on celestial bodies.²³⁴ Application of the OST to cyber warfare would prevent the Internet from becoming nationalized and prohibit cyber weapons of mass destruction in cyberspace.²³⁵

Unfortunately, analogizing the OST to cyber warfare provides an inadequate model to govern cyber warfare.²³⁶ First, the analogy of cyberspace to outer space is tenuous: cyberspace is not a “commons,” but it is network of privatized networks.²³⁷ More importantly, it is unclear how the OST would be applied.²³⁸ Can nations militarize cyberspace, so long as their cyber weapons do not rise to the level of nuclear weapons? Assuming the affirmative, what kind of cyber attack would rise to the level of a nuclear weapon? Because it is unlikely that a cyber attack could equate to a nuclear weapon, applying the OST to cyber warfare would actually permit the militarization of cyberspace.²³⁹

Further, enforcing an outer space-type treaty would be difficult because cyber weapons are hard to

²³³ Shackelford, *supra* note 152, at 220 (“The military use of space was not completely forbidden by the 1967 U.N. Outer Space Treaty, as evidenced by the existence of earth-orbit military reconnaissance satellites, remote-sensing satellites, military global-positioning systems, and space-based aspects of an antiballistic missile system.”).

²³⁴ The Outer Space Treaty art. 5, Jan. 1, 1967, 610 U.N.T.S. 205.

²³⁵ *C.f. Id.*

²³⁶ See generally, Christopher Petras, The Use of Force in Response to Cyber Attacks on Commercial Space Systems—Reexamining “Self Defense” in Outer Space in Light of the Convergence of U.S. Military and Commercial Space Activities, 67 J. AIR. L. & COM. 1213, 1214 (2002).

²³⁷ *Reno*, 929 F. Supp. at 830.

²³⁸ Carr, *supra* note 44, at 33.

²³⁹ Shackelford, *supra* note 152, at 222.

trace.²⁴⁰ The OST is enforceable because it is easy to attribute responsibility for weapons in space.²⁴¹ In contrast, locating cyber weapons in cyberspace would require finding a single strand of malicious code in billions of lines of code and then determining who created the code.²⁴² Attributing responsibility for space weapons is also practical because only a few nations have space capabilities.²⁴³ Conversely, one hundred and twenty nations have the capability to engage in cyber warfare.²⁴⁴ Therefore, the OST model, as applied to cyber warfare, would be difficult to enforce.²⁴⁵

ii. *The Antarctic Treaty System*

Theorists have also explained that the ATS could be applied to cyber warfare.²⁴⁶ The ATS establishes Antarctica as a scientific preserve and bans

²⁴⁰ Carr, *supra* note 44, at 33.

²⁴¹ *Id.*

²⁴² *Id.*

²⁴³ *Id.*

²⁴⁴ *Id.*

²⁴⁵ *Id.*

²⁴⁶ *Id.*; see also Menthe, *supra* note 230, at 88 (analogizing the law of Antarctica to cyberspace). “The Antarctic Treaty, the earliest of the post-World War II arms limitation agreements, has significance both in itself and as a precedent. It demilitarized the Antarctic Continent and provided for its cooperative exploration and future use. It has been cited as an example of nations exercising foresight and working in concert to prevent conflict before it develops. Based on the premise that to exclude armaments is easier than to eliminate or control them once they have been introduced, the treaty served as a model, in its approach and even in its specific provisions, for later ‘non-armament’ treaties -- the treaties that excluded nuclear weapons from outer space, from Latin America, and from the seabed.” U.S. DEP’T OF STATE, <http://www.state.gov/t/isn/4700.htm> (last visited Nov. 24, 2011).

all military activity on the continent.²⁴⁷ The purpose of the treaty is assurance “that Antarctica shall continue forever to be used exclusively for peaceful purposes and shall not become the scene or object of international discord.”²⁴⁸ Applying the ATS to cyber warfare would mean preserving cyberspace by banning all cyber weapons in cyberspace.²⁴⁹

Lamentably, applying the ATS to cyber warfare is problematic and unworkable.²⁵⁰ The application of the ATS to cyber warfare would hinder Internet innovation.²⁵¹ The ban on cyber weapons would be a detriment to the Internet because “imposing such a freeze on developing new software capable of malicious attacks...stifles innovation.”²⁵² The enforcement of the ATS-model would also be questionable because it is impractical to identify malicious code in cyberspace,²⁵³ Antarctica has definite borders whereas cyberspace is limitless.²⁵⁴ Consequently, the application of the ATS to cyber warfare provides a difficult model to implement.²⁵⁵

iii. *Space Law and Antarctic Treaty in Review*

To conclude, applying the OST or the ATS to cyber warfare would not provide a workable structure to govern cyber warfare.²⁵⁶ First, it is uncertain how the

²⁴⁷ The Antarctic Treaty art. 1, Dec. 1, 1959, 402 U.N.T.S. 73. “Rather than banning only the most egregious cyber use, it may be more thorough to regulate all hacking that could become a cyber attack.” Shackelford, *supra* note 152, at 221.

²⁴⁸ The Antarctic Treaty, Dec. 1, 1959, 402 U.N.T.S. 73.

²⁴⁹ Carr, *supra* note 44, at 33.

²⁵⁰ *Id.*

²⁵¹ Shackelford, *supra* note 152, at 222.

²⁵² *Id.*

²⁵³ Carr, *supra* note 44, at 33.

²⁵⁴ *Id.*

²⁵⁵ *Id.*

²⁵⁶ See *supra* Part III-A-3.

applications will functionally work.²⁵⁷ Second, it is difficult to enforce the applications because it is hard to police cyber weapons and attribute responsibility for them.²⁵⁸ Third, the applications could stifle Internet innovation.²⁵⁹ For the foregoing reasons, the OST or the ATS do not provide adequate legal analogies to regulate cyber warfare.²⁶⁰

B. CYBER WARFARE IS HERE TO STAY

Assuming a comprehensive international treaty is agreed upon to specifically govern cyber warfare, nations will continue to use cyber warfare regardless of the treaty.²⁶¹ Nations will reserve cyber warfare as part of their military operations because: (1) attributing responsibility for cyber attacks is problematic; (2) cyber warfare regulations cannot be enforced; (3) the decentralized nature of the Internet fosters cyber exploitation; (4) most cyber attacks go unreported; (5) the entry costs of cyber warfare is minimal; (6) cyber warfare can be used to coerce superior military forces into asymmetric warfare; and (7) attacking a nation's critical infrastructure destroys the victim state's internal operational viability.²⁶²

Nations will use cyber warfare to conduct military operations because attributing responsibility for cyber attacks is problematic.²⁶³ First, determining the

²⁵⁷ *Id.*

²⁵⁸ *Id.*

²⁵⁹ *Id.*

²⁶⁰ *Id.*

²⁶¹ See Swaine, *supra* note 96.

²⁶² See *infra* Part III-B.

²⁶³ *Attribution in Cyber Attacks is Difficult, But Not Impossible*, SECURE NATION (Feb. 4, 2010), <http://securenation.wordpress.com/2010/02/27/attribution-in-cyber-attacks-is-difficult-but-not-impossible/> (Although there is no technology that can automatically determine an attack origin, it is possible to identify the attackers through traditional detective work).

location where the cyber attack originated is challenging.²⁶⁴ Cyber attackers deliberately disguise the origin of their attacks by rerouting them through various Internet servers.²⁶⁵ Generally, cyberwarriors route their attacks through innocent servers—“stepping stones”—located throughout the world.²⁶⁶ For example, an attack traced to Russian servers is not determinative that the attack originated from Russia.²⁶⁷ The attack might actually be from Estonia, New Zealand, or the United States, using Russia as a stepping-stone to conceal the originating nation’s true identity.²⁶⁸ Therefore, attribution cannot be conclusively determined through evidence of attack origin.²⁶⁹

Second, determining the identity of the attacker is full of twists and turns.²⁷⁰ Although cyber attacks may be traced to a particular nation, the government, terrorists, or criminals may be responsible for the attacks.²⁷¹ Conclusively ascertaining the identity of the attacker requires an intensive investigation with the assistance of the forum state.²⁷² However, it is unlikely the forum state will give assistance, because it is common for states to incite cybercriminals within their territory to commit cyber attacks against other nation-

²⁶⁴ Shackelford, *supra* note 152, at 203—09 (“There are no flags or tanks in a cyber attack and the identity of the perpetrators is likely concealed.”).

²⁶⁵ *Id.*

²⁶⁶ See Susan W. Brenner, At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare, 97 J. CRIM. L. & CRIMINOLOGY 379, 409 (2006).

²⁶⁷ *Id.*

²⁶⁸ *Id.*

²⁶⁹ *Id.*

²⁷⁰ Shackelford, *supra* note 152, at 200—01.

²⁷¹ *Id.*

²⁷² See Carr, *supra* note 44, at 47 (Russia and China harbor cyber attackers).

states.²⁷³ These harbor states then hide behind their cyber minions in a “veil of plausible deniability and thus escape accountability.”²⁷⁴

Nations will conduct cyber warfare, because cyber warfare regulations are realistically unenforceable.²⁷⁵ Until a cyber attack is launched, regulators would not be able to police cyber warfare, rendering them completely useless in peacetime.²⁷⁶ Regulators would need access to *all* computer databases within the forum state because attacks could originate from any server within the forum state.²⁷⁷ If that were possible, regulators would then need to be able to identify malicious code through billions of lines of computer data.²⁷⁸ “To spot a cyber attacker from all the normal cross-border data flows would be like picking out a single person with more luggage than usual from the thousands of passengers that pass through JFK Airport daily.”²⁷⁹

²⁷³ McAfee, Virtual Criminology Report: Cybercrime Versus Cyberlaw 15 (2008).

²⁷⁴ See Shackelford, *supra* note 152, at 233. In return for their services, the cyber attackers, assuming they can be identified, are likely to receive asylum within the forum state. MCAFEE, *supra* note 273, at 15. Russia and China provide a safe haven to individuals suspected of committing cyber attacks within their territories. *Id.* The implication is that Russia and China’s intelligence agencies are protecting the country’s cybercriminals. *Id.*

²⁷⁵ See generally, McGavran, *supra* note 50, at 268.

²⁷⁶ See *supra* Part III-A. Regulators may conduct a cyber forensic investigation once cyber attacks occur. Until then, however, regulators would have to sit on their hands, figuratively speaking.

²⁷⁷ C.f. Duncan Gardham, *Cold war enemies Russia and China launch a cyber attack every day*, THE TELEGRAPH, Dec. 4, 2009, www.telegraph.co.uk/technology/news/6727100/Cold-war-enemies-Russia-and-China-launch-a-cyber-attack-every-day.html.

²⁷⁸ Shackelford, *supra* note 152, at 200.

²⁷⁹ *Id.*

Nations will continue to use cyber warfare because of the loose nature of the Internet.²⁸⁰ The Internet fosters an environment of porous security, resulting in network vulnerabilities.²⁸¹ This is mainly because the Internet was designed to be a decentralized collaborative communications system.²⁸² Security and identity management were not structural priorities.²⁸³ As a result, cybersecurity will always be one step behind cyber attackers.²⁸⁴ Cyber attackers will eventually find vulnerabilities and defeat security measures put in place to prevent cyber attacks.²⁸⁵

Nations will implement cyber warfare because most cyber intrusions go unreported and many more are not even detected, which allows the attackers to escape accountability.²⁸⁶ Currently, approximately ninety percent of cyber attacks go unreported.²⁸⁷ Apparently, corporations would rather absorb the costs of cyber

²⁸⁰ See Natasha Solce, *supra* note 43, at 307 (discussing a non-exhaustive list of why cyber attacks will occur).

²⁸¹ *Id.*

²⁸² See William F. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFF. 97, 99 (2010).

²⁸³ *Id.*

²⁸⁴ *Id.*

²⁸⁵ *Id.*

²⁸⁶ See Kevin Voigt, *Analysis: The Hidden Cost of Cybercrime*, CNN (June 7, 2011), <http://edition.cnn.com/2011/BUSINESS/06/06/cybercrime.cost/index.html> (organizations are cautious to publicize breaches to their corporate security). Recently, there have been many high profile cyber attacks against large organizations. *Id.* For example, Sony's PlayStation Network was compromised in May 2011, resulting in \$171 million in damage. *Id.* Lockheed Martin and Google's computer networks were also recently breached. *Id.*

²⁸⁷ Natasha Solce, *supra* note 43, at 307 (at least eighty percent of security intrusions go unreported); Marc Goodman & Susan W. Brenner, *Emerging Consensus on Criminal Conduct in Cyberspace*, 10 Int'l J.L. & Info. Tech. 139, 157 (2002) (only ten percent of cyber attacks are reported to any kind of authority).

attacks than face the negative publicity that their systems have been compromised.²⁸⁸ Further, cyber attacks are covert and do not leave easily identifiable evidence of their assault.²⁸⁹ As a result, most organizations are unaware their networks have even been infiltrated.²⁹⁰ This allows hackers to commit attacks with practical impunity.²⁹¹

Additionally, cyber attacks will become increasingly used in modern warfare because of its low costs.²⁹² Cyber warfare is inexpensive relative to the costs of developing and maintaining twenty-first century kinetic weapons.²⁹³ Because the battlefield of cyber warfare occurs over publically accessible networks, the only expenses incurred to conduct cyber war pertain to training cyber warriors and acquiring the computer hardware needed to launch cyber attacks.²⁹⁴ “The low entry cost of cyberspace appeals to nations, criminals, and terrorist organizations that cannot outmatch or inflict harm upon the United States in an alternative manner.”²⁹⁵

²⁸⁸ Goodman, *supra* note 287, at 157.

²⁸⁹ *Id.*; see also David Goldman, *Massive hack hit 760 companies*, CNN MONEY, Oct. 28, 2011, http://money.cnn.com/2011/10/27/technology/rsa_hack_widespread/index.htm (multiple fortune 500 companies were victims of cyber attacks recently, and most of these companies were probably unaware of the attacks).

²⁹⁰ Martin Sutherland, *Know your enemy, know your risk*, NEW EUROPE, June 12—18, 2011, at 10.

²⁹¹ *C.f.* Goodman, *supra* note 287, at 157.

²⁹² See Susan W. Brenner & Leo L. Clarke, *Civilians in Cyber warfare: Casualties*, 13 SMU SCI. & TECH. L. REV. 249, 250 (2009).

²⁹³ See, e.g., MARTIN C. LIBICKI, RAND CORPORATION, CYBERDETERRENCE AND CYBERWAR xvi, 177 (2009). “Because a devastating cyber attack may facilitate or amplify physical operations and because an operational cyber war capability is relatively inexpensive (especially if the Air Force can leverage investments in CNE), an offensive cyber- war capability is worth developing.” *Id.*

²⁹⁴ See Brenner, *supra* note 292, at 250.

²⁹⁵ Natasha Solce, *supra* note 43, at 307.

Furthermore, nations will use cyber warfare because it can force a stronger military power into asymmetric warfare.²⁹⁶ Opponents will not challenge the United States' traditional military superiority.²⁹⁷ The United States allocates more to defense spending than the next seventeen largest nations combined.²⁹⁸ Because of this, militaries will instead resort to asymmetric tactics and exploit the United States' vulnerabilities in cyberspace.²⁹⁹

Cyber warfare is now the "great equalizer,"³⁰⁰ because weaker military nations can now defend

²⁹⁶ See generally, Ekaterina Stepanova, *Terrorism in Asymmetrical Conflict*, 23 STOCKHOLM INT'L PEACE RES. INST. RES. REP. 1 (2008) (the classic definition of asymmetric warfare refers to weaker military units using unconventional tactics to offset their military deficiencies. Asymmetric warfare includes terrorism, guerilla tactics, hostage situations, insurgency tactics, and other unconventional military strategy).

²⁹⁷ C.f. The Economist Online, *Defence Cost: The Biggest Military Spenders*, DAILY CHART BLOG (Jun 8th 2011, 14:00), <http://www.economist.com/blogs/dailychart/2011/06/military-spending>; see also Frank J. Cilluffo & Paul Bryon Pattak, *Cyber Threats: Ten Issues for Consideration*, 1 GEO. J. INT'L AFF. 41, 42 (2000) ("Bits and bytes will never completely replace bullets and bombs, but they can be synergistically combined. Imagine if the Oklahoma City bombing had been accomplished by electronic disruptions of federal, state and local emergency and public safety communications systems, including Emergency-911.").

²⁹⁸ Daily Chart Blog, *supra* note 297.

²⁹⁹ See generally, Steven Lambakis, James Kiras & Kristin Kolet, Understanding "Asymmetric" Threats to the United States 1 (2002).

³⁰⁰ See Mac Slocum, *Cyber Warfare: Don't Inflate it, Don't Underestimate it*, O'REILLY RADAR (Feb. 11, 2010), <http://radar.oreilly.com/2010/02/cyber-warfare-dont-inflate-it.html> (cyber warfare "balances the scales" traditional warfare).

themselves through cyberspace.³⁰¹ Nations no longer need to acquire expensive stockpiles of weapons, such as stealth fighters, to counteract the United States' military capabilities.³⁰² "A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target."³⁰³

Lastly, nations will resort to cyber warfare because attacking a nation's critical infrastructure destroys the victim state's internal operational viability.³⁰⁴ Attacking critical infrastructure, such as power, emergency response systems, or banking, would

³⁰¹ See Kamal, *supra* note 6, at 78. "Current military theory suggests therefore that attacking a nation's center of gravity, in addition to its armed forces, is the most effective way to destroy the state. In today's societies centers of gravity include telecommunications networks, energy and power sources, transportation systems, and financial centers and networks. Thus, the destruction of these systems becomes just as important as destroying an adversary's military forces. Not only will cyber-war be a force in future warfare, it may also turn out to be the great equalizer for nations attacking adversaries with superior conventional military power. Most nations lack the resources to build a military machine and may use information technologies to overcome their battlefield inferiority." *Id.*

³⁰² See Lynn, *supra* note 282, at 98.

³⁰³ *Id.* at 99.

³⁰⁴ See Susan Brenner & Leo L. Clarke, *Civilians in Cyber warfare: Conscripts*, 43 VAND. J. TRANSAT'L L. 1011, 1029 (2010) (civilians affect the defense of cyber warfare because they generally own and operate the nation's critical infrastructure). Throughout history, warring nations have sought to demolish enemy critical infrastructure in order to cripple that nation. See Kamal, *supra* note 6, at 76 ("In previous wars, critical infrastructure components such as airports, power plants, water systems, railroads, oil and gas pipelines, and communication centers were targeted by the military because their destruction could help cripple a nation."). This theory is founded on the principle that victory need only be achieved through attacking enemy infrastructure in conjunction with defeating its military forces. *Id.*

create a loss of confidence in the United States government and wreak economic havoc.³⁰⁵ These attacks deprive the victim state of its civilian infrastructure used to support military operations, such as electric power.³⁰⁶ Military dependence on civilian infrastructure has progressed to the point where victory in war can only be attained through the annihilation of the state itself, and the morale of its civilian population.³⁰⁷

In review, states will use cyber warfare regardless of an international treaty prohibiting the use of cyber weapons.³⁰⁸ First, attributing responsibility for cyber attacks is problematic.³⁰⁹ Second, cyber warfare

³⁰⁵ See Brian M. Mazanec, *The Art of (Cyber) War*, 16 J. INT'L SEC. AFF. (2009), available at www.securityaffairs.org/issues/2009/16/mazanec.php. "Strategic cyber warfare attacks during a total war with the U.S. would destroy critical infrastructure and wreak economic havoc, but their most critical impact may be on the will of the U.S. population. By creating a chronic loss of services such as power, emergency response, television and telephony across the U.S., citizens would suffer a loss of confidence in the U.S. government. Individuals would question the status and security of their personal finances in savings and retirement accounts, and uncertainty could lead to rioting and hoarding that would act as a force multiplier, further stressing an already damaged infrastructure." *Id.*

³⁰⁶ See Brenner & Leo L. Clarke, *Civilians in Cyber warfare: Conscripts*, 43 VAND. J. TRANSAT'L L. 1011, 1029 (2010). For example, "coordinating the deployment and resupply of U.S. troops with goods from private vendors necessarily requires using unclassified networks that are linked to the open Internet." See Lynn, *supra* note 282, at 100. Attacking these civilian networks could create large logistic problems for the United States in wartime. *Id.*

³⁰⁷ Kamal, *supra* note 6, at 78. ("In the late nineteenth century, military forces began to rely on industry for sustenance. This dependence has progressed to the point where wars are no longer aimed at defeating the enemy on the battlefield; they are wars of attrition, in which victory can be attained only through the destruction of the state itself, and the morale of its civilian population.").

³⁰⁸ See *supra* Part III-B.

³⁰⁹ *Id.*

regulations cannot be realistically enforced.³¹⁰ Third, the decentralized structure of the Internet fosters an environment of cyber exploitation.³¹¹ Fourth, most cyber attacks go unreported allowing cyber attacks to escape accountability.³¹² Fifth, the costs to operate in cyberspace are nominal.³¹³ Sixth, cyber warfare can be used to circumvent traditional military forces.³¹⁴ Seventh, cyber attacks can destroy a victim state's internal operations viability.³¹⁵ For the foregoing reasons, nations will use cyber warfare regardless of any international treaty.³¹⁶

V. PROPOSAL

The Federal government should protect critical infrastructure in the United States, because cyber threats towards critical infrastructure endangers national security.³¹⁷ Civilian infrastructure in the United States supports the military in significant ways.³¹⁸ They help provide power, telecommunications, and logistics.³¹⁹ Unfortunately, the private sector is not able to provide adequate protections against major military attacks through cyberspace.³²⁰ The federal government needs to

³¹⁰ *Id.*

³¹¹ *Id.*

³¹² *Id.*

³¹³ *Id.*

³¹⁴ *Id.*

³¹⁵ *Id.*

³¹⁶ *Id.*

³¹⁷ *See supra* Part II.

³¹⁸ *See e.g.*, U.S. Gov't Accountability Office, GAO-10-147, Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical power Risks and Vulnerabilities to DOD Critical Assets (2009) (the DOD relies heavily on a network of defense orientated critical infrastructure).

³¹⁹ *Id.*

³²⁰ Executive Branch of the U.S. Gov't, The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets 8 (2003).

be able to monitor the networks of these critical infrastructures in order to safeguard national security.

First, the federal government should implement active computer defenses to protect private sector critical infrastructure networks. The National Security Agency has created an advanced active cyber security defense system that can be applied to private critical infrastructure.³²¹ These defense systems work by implementing scanning technology at the interface of military Internet networks to detect malicious code before it enters the network.³²² These active defenses protect all networks under the “.mil” domain.³²³ Because active cyber security systems can prevent cyber attacks from entering targeted networks, the federal government should implement them on private critical infrastructure networks.

Second, the federal government needs to be able to regularly monitor critical infrastructure networks, because cyber defenses are not absolute.³²⁴ Some attacks will be able to infiltrate the networks and evade detection.³²⁵ This requires cyber warriors to be able to detect intruders and malicious code once it has been

³²¹ See Lynn, *supra* note 282, at 103; see also DEP'T OF DEF., DEP'T OF DEF. STRATEGY FOR OPERATING IN CYBERSPACE 7 (2011). “Active cyber defense is DOD’s synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DOD networks and systems, supplementing best practices with new operating concepts.” *Id.*

³²² See Lynn, *supra* note 282, at 103; Strategy for Operating in Cyberspace, *supra* note 321, at 7 (active cyber defenses operate in real time “by using sensors, software, and intelligence to detect and stop malicious activity” before it can affect networks).

³²³ Lynn, *supra* note 282, at 103.

³²⁴ See Strategy for Operating in Cyberspace, *supra* note 321, at 7 (“[I]ntrusions may not always be stopped at the network boundary.”).

³²⁵ Lynn, *supra* note 282, at 103.

installed in the target network.³²⁶ Cyber warriors would need to be able to search through the private networks in order to hunt for malicious code and intrusions.³²⁷

Active defense measures against United States private companies may infringe upon certain civil liberties enjoyed under the Constitution.³²⁸ Cyber warriors will have to search throughout private networks for intrusions. This raises concerns for private companies because of the expectation of privacy in their networks, and the sensitive proprietary information contained on it.³²⁹ “The law must therefore adjust traditional understandings of the right to privacy, the right to protection against an unreasonable search, and the right to due process.”³³⁰

To preserve civil liberties, Congress should enact legislation that allows Cyber Command to monitor private networks upon judicial approval. Foremost, Congress should enact the Critical Infrastructure Cyberspace Surveillance Act (“CICSA”).³³¹ Such an act would establish a CICSA Court.³³² CICSA would authorize Cyber Command to electronically monitor private sector critical infrastructure networks for up to

³²⁶ *Id.*

³²⁷ *Id.*

³²⁸ See Condrón, *supra* note 221, at 416.

³²⁹ U.S. CONST. amend. IV; *Katz v. United States*, 389 U.S. 347 (1967) (a search occurs when there is a reasonable expectation of privacy).

³³⁰ See Condrón, *supra* note 221, at 416.

³³¹ *C.f.* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801—1811 (2006).

³³² See *e.g.*, Foreign Intelligence Surveillance Court Rules of Procedure 4, 5 (2006). The CICSA Court shall consist of United States District Court Judges appointed by the Chief Justice of the United States Supreme Court. Each Judge may exercise the authority vested by CICSA and such other authority as consistent with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.

one year.³³³ In order to obtain authorization, Cyber Command would be required to show certain specific findings,³³⁴ and would obtain authorization only if approved through a CICA Court judge.³³⁵ Cyber Command would then have the authority to only monitor private networks for malicious code. They would not have the authority delete malicious code from private networks. Instead, Cyber Command would be limited to acquire a court order forcing the private entity to fix their network vulnerabilities.

VI. CONCLUSION

To conclude, this article has demonstrated that: (1) nations around the world have militarized the power of cyberspace;³³⁶ (2) cyber warfare represents a serious threat to critical infrastructure within the United

³³³ One year's time may be needed in order to conduct a forensic computer investigation.

³³⁴ Each application for an order approving electronic surveillance under CICA shall include:

(1) the identity of the Cyber Command officer making the application;

(2) the identity and description of the specific target of the electronic surveillance;

(3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—

(A) the target of the electronic surveillance is or has been the victim of cyber attacks within the past three years; and

(B) the cyber attacks were caused by a foreign nation or an agent of a foreign nation;

(4) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance.

See e.g., 50 U.S.C. § 1804 (2006).

³³⁵ For a judge to issue a surveillance order, probable cause must show that (1) the target of the surveillance has been the victim of cyber attack(s), and (2) the cyber attack(s) were caused by a foreign nation or an agent of a foreign nation.

³³⁶ *See supra* Part I-C.

States;³³⁷ and (3) international treaties do not provide adequate legal mechanisms to govern cyber warfare.³³⁸ For the foregoing reasons, the United States should not depend on international legislation to protect its' critical infrastructure from cyber attacks.³³⁹ Instead, the United States should take an active defensive approach, by monitoring the networks of private companies that own and maintain critical infrastructure within the United States.³⁴⁰

³³⁷ *See supra* Part II.

³³⁸ *See supra* Part III.

³³⁹ *See supra* Part IV.

³⁴⁰ *Id.*

