Denver Journal of International Law & Policy

Volume 40
Number 4 *Fall 2012*

Article 5

January 2012

Science Fiction No More: Cyber Warfare and the United States

Cassandra M. Kirsch

Science Fiction No More: Cyber Warfare and the United States

Keywords

States, Government, War, International Law: History

SCIENCE FICTION NO MORE: CYBER WARFARE AND THE UNITED STATES

*Cassandra M. Kirsch**

ABSTRACT

Faced with the increased propensity for cyber tools to damage state computer networks and power grids with the click of a mouse, politicians and academics from around the world have called for the creation of a Geneva Convention equivalent in cyberspace. Yet, members of United Nations Security Council continue to disagree as to what cyber activities might rise to the level of an armed attack under the existing Law of Armed Conflict. Activities once limited to cyber espionage, and outside the reach of international law, are now the very same tools utilized in cyber operations to disable state communications and wreak havoc on state infrastructure. Wars, traditionally waged between nations and clearly defined groups, can now be fought behind the veil of anonymity inherent of the Internet. While acts of war have yet to happen openly on the Internet, accusations have already been made against Russia for the 2007 cyber attacks on Estonia and against Israel for the Stuxnet worm unleashed on Iran's nuclear reactors. Just as aerial bombing and nuclear arms revolutionized the battlefield, cyber attacks, and the mechanisms behind them, stand poised as the next evolution in weapons of war and any multilateral treaty must take these facts into consideration.

INTRODUCTION

Throughout history, technology has revolutionized the manner in which wars are fought. In the eighteenth century, gunpowder brought an end to the days of castles and knights, ushering in a period of battalions and infantrymen. Two hundred years later, the invention of the aircraft gave rise to the Hague Rules of Air Warfare after the widespread destruction caused by strategic bombing campaigns during the First World War. The atrocities wrought by the atom bomb at Hiroshima and Nagasaki still burn in the memories of many and is responsible for the proliferation of espionage and intelligence gathering continuing to this day in our international community. Now, at the dawn of the twenty-first century, information technology stands to once again change the landscape of war. While the Internet transformed society in the nineties by allowing computer users to access information across the globe with the click of a mouse, the spread of information technology comes at a cost. The more people become dependent on the

Internet, and the more data we move from paper to digital format, then the more vulnerable our society becomes to a cyber attack.

Formerly the substance of science fiction, cyber warfare is one of the most serious national security threats in recent years. Cyber warfare covers the doctrine regarding the tactics, techniques, and procedures of Computer Network Operations (CNO) including attacks, defense, and exploitation, plus the new aspect of social engineering.[1] While the technology used in cyber warfare has been traditionally characteristic of espionage activities in the last twenty years, this same technology is capable of creating real damage to a nation-state. In 2007, Estonia suffered the first ever reported state-wide incident of cyber assault when Estonia's banks, online newspapers, and government communications were shut down for two weeks by a group of Russian hackers who were believed to be tied to the Kremlin.[2] One of the most wired societies in the world, the people of Estonia quickly turned to the streets in riot, leaving at least one person dead and 150 people injured.[3] Similar attacks predated the weeks leading up to the 2008 Georgian bombings by Russia, but it was not until the United States Department of Defense ("DoD") suffered a massive compromise of military defense networks that the United States issued a Cyberspace Policy Review and established the United States Cyber Command ("USCYBERCOM") to protect DoD networks.[4]

---

* J.D., University of Denver Sturm College of Law (2013); B.A., The University of Texas (2008). Cassandra M. Kirsch is a 2013 Juris Doctorate candidate at the University of Denver Sturm College of Law pursuing studies in the areas of information privacy law and Internet law. The author would like to extend special thanks to Professor John T. Soma, the Executive Director of the University of Denver Privacy Foundation, for his encouragement, mentorship, and support of her research on the implications of cyber warfare and cyber crime on international law.

1. STEPHEN NORTHCUTT, *Foreword* to CYBER WARFARE: TECHNIQUES, TACTICS AND TOOLS FOR SECURITY PRACTITIONERS xx (JASON ANDRESS & STEVE WINTERFELD, 2011).

2. *See War in the Fifth Domain*, ECONOMIST, July 3, 2010, at 25, *available at* http://www.economist.com/node/16478792; Noah Shachtman, *Kremlin Kids: We Launched the Estonian Cyber War*, WIRED (Mar. 11, 2009), http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro. A Pro-Kremlin youth group took responsibility for the attacks on Estonia in 2007. However, the group has a track record of conducting operations on behalf of the government.

3. *Estonia Hit by "Moscow Cyber War,"* BBC NEWS, http://news.bbc.co.uk/2/hi/europe/6665145.stm (last updated May 17, 2007).

4. *See* William J. Lynn III, *Defending a New Domain: The Pentagon's Cyber Strategy*, FOREIGN AFFAIRS, Sept./Oct. 2010, at 97, *available at* www.foreignaffairs.com articles.66552/william-j-lynn-iii/defending-a-new-domain; *US Needs "Digital Warfare Force,"* BBC NEWS, http://news.bbc.co.uk/2/hi/technology /8033440.stm (last updated May 5, 2009). In what was the most significant United States military computer data breach to date, an infected flash drive was inserted into a United States military laptop at a base in the Middle East and the code on the flash drive uploaded itself onto a network run by U.S. Central Command and transferred data to servers controlled by foreign intelligence agencies. The code resulted in "Operation Buckshot Yankee," a 14-month effort to remove

Despite various initial steps to deter a massive cyber attack on DoD networks, the United States is largely unprepared to respond to an act of cyber warfare. In fact, the United States military does not even have a definition for cyber warfare nor does the legal community understand how it applies to legal norms, specifically the Law of Armed Conflict.[5] The lack of a definition of cyber warfare is especially problematic as the President, in responding to a cyber attack must first determine whether such an attack rises to the level of an "armed attack," and thus justifies self-defense. However, much of what transpires in the cyber realm does not resemble traditional military threats. Whether it is appropriate to characterize cyber attacks as "weapons, means or methods of warfare" and subject them to legal review is an issue because the legal architecture for the Law of Armed Conflict is founded on the concept of traditional military threats.

This paper focuses not only on the current state of the law regarding cyber warfare, but also what cyber warfare could and should be. Part I looks at the nature and history of cyber attacks to provide an understanding of their capabilities as weapons of war as compared to espionage. Part II examines the applicability of the Law of Armed Conflict to cyber attacks, including how the elements of proportionality, attribution, and necessity apply to the most common forms of cyber attacks. Part III discusses how cyber warfare is currently being addressed by the United States, the recent proposals for an international treaty on cyber warfare, and the obstacles to establishing a multilateral international treaty. Finally, Part IV looks ahead to the future of American civil liberties post-normalization of cyber warfare.

I. THE NATURE AND HISTORY OF CYBER ATTACKS: WEAPONS OF WAR OR ESPIONAGE?

In the last decade, the rate of cyber attacks increased exponentially, along with their propensity for actual harms. Faced with the growing reality of cyber attacks from foreign state actors, talk of a Geneva Convention equivalent for cyber space made headlines in the news and at academic conferences in 2010 and 2011.[6] Politicians and

---

the code from all networks. *See also* Kim Zetter, *The Return of the Worm that Ate the Pentagon*, WIRED (Dec. 9, 2011), http://www.wired.com/dangerroom/2011/12/worm-pentagon/#more-66316.

5. *See* U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, 2-4 (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf. While the Pentagon has concluded that computer sabotage may constitute an act of war in its first formal cyber strategy report, the report does not detail what kind of cyber attacks justify the use of force.

6. *See, e.g.*, KARL FREDERICK RAUSCHER & ANDREY KOROTKOV, EASTWEST INST., WORKING TOWARDS RULES FOR GOVERNING CYBER CONFLICT: RENDERING THE GENEVA AND HAGUE CONVENTIONS IN CYBERSPACE 6-14 (2011), *available at* http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24a6a8c70

academics alike agree that a treaty would lessen the chance of a real cyber war, arguing the world is now in the early stages of a Cyber Arms Race.[7] In evaluating how domestic and international law might be used by the United States in response to cyber attacks, the international legal community must first discern the nature, purpose, and scope of cyber attacks. While the use of terms like "war" and "attacks" espouse an offensive military nature, threats to our national computer systems frequently fall under the category of espionage due to their data gathering nature.[8] Espionage, while punishable under domestic laws, is not listed as a crime by the International Court of Justice. Rather, the International Court of Justice reserves the term crime against international law for acts of aggressive war, serious war crimes or crimes against humanity, all of which presume harm to citizens to a nation-state.[9] The establishment of any sort of international regime, consequently, turns on delineating cyber activities that are used as weapons versus those limited to state espionage.

Although cyber tools used for espionage activities are often the same tools used to attack a nation's computer networks, acts of cyber warfare deviate from their espionage counterparts by going beyond compromising a computer network.[10] Rather than passively monitor state activities on a computer network or copy data,[11] a cyber attack actively "penetrates another nation's computer systems or networks for the purposes of causing damage or disruption."[12] While the United States military has yet to settle on official definitions for both cyber

---

60233&lng=en&id=127333; Bruce Schneier, *It Will Soon Be Too Late to Stop the Cyberwars*, LONDON FINANCIAL TIMES, Dec. 2, 2010, at 9, *available at* http://www.ft.com/intl/cms/s/0/f863fb4c-fe53-11df-abac-00144feab49a.html; Maggie Shiels, *Cyber War Threat Exaggerated Claims Security Expert*, BBC NEWS, http://www.bbc.co.uk/news/technology-12473809 (last updated Feb. 16, 2011). Cyber warfare and its relation to the Geneva Convention was a popular topic at the 2011 RSA Security Conference in San Francisco and the East West Institute has conducted a joint report between Russian and American scholars to define rules of cyber warfare based on the Geneva Convention. Although he has argued in the past that the threat of cyber war is exaggerated, IT Security Expert Bruce Schneier says that the Geneva Conventions need to be updated to manage the current reality of cyber war and cyber attacks.

7. Hamish Barwick, *Global Cyber War Treaties Urgently Needed: Bruce Schneier*, COMPUTERWORLD (Nov. 8, 2011), http://www.computerworld.com.au/article/406751/global_cyber_war_treaties_urgently_needed_bruce_schneier.

8. *See* JEFFREY T. RICHELSON, *Espionage, in* THE READER'S COMPANION TO MILITARY HISTORY 156-57 (Robert Cowley & Geoffrey Parker eds., 1996).

9. *See* LAWRENCE MALKIN, *Genocide, in* THE READER'S COMPANION TO MILITARY HISTORY 181 (Robert Cowley & Geoffrey Parker eds., 1996).

10. *See* JEFFREY CARR & LEWIS SHEPHERD, INSIDE CYBER WARFARE: MAPPING THE CYBER UNDERWORLD 1-5 (2009); RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 228-32 (2010); RICHARD STIENNON, SURVIVING CYBERWAR 20 (2010).

11. STIENNON, *supra* note 10, at 20-22.

12. CLARKE & KNAKE, *supra* note 10, at 6.

attacks and cyber warfare,[13] the DoD recently adopted an effects-based approach, or consequence-based model, for determining when a cyber activity becomes a cyber attack.[14] Under the current approach by the DoD, the damage caused by the activity to computer networks and infrastructure is compared with the consequences of traditional armed attacks.[15] In other words, when the effect of a cyber attack is analogous to those that would invoke U.N. Charter terms of "armed attack," then the cyber operation rises to the level of an armed attack. For example, if a cyber attack takes critical state infrastructure, such as an electricity grid offline or a dam, offline and collateral damage spills over into the civilian realm, then the cyber attack would likely count as an armed attack.[16] On the other hand, a cyber operation that interferes with intelligence activities shares more similarities with espionage activities than the kinetic effects of armed attacks. Recently, NATO also adopted the effects-approach, concluding in an expert report led by Madeline Albright that a cyber attack on the critical infrastructure of a NATO country may equate to an armed attack and justifies retaliation.[17] Despite support of this approach by the United States and NATO, Russia and China have both rejected the effects-approach in favor of a broad definition of cyber warfare that encompasses any use of a computer technology to wage an attack on another country, including online acts to undermine the political and social harmony of the state.[18]

---

13. *See* U.S. DEP'T OF DEF., *supra* note 5, at 2-4.

14. *See id.* at 3-4. The Department of Defense refers to cyber attacks as cyber threats, stating adversaries may seek to "exploit, disrupt, deny, and degrade the networks and systems that DoD depends on." Also, cyber threats include "destructive action[s]" that threaten to destroy or degrade networks, as well as attacks on both military targets and critical civilian infrastructure. *See also* NAT'L RES. COUNCIL, TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBER ATTACK CAPABILITIES (WILLIAM A. OWENS, et al. eds., 2009); U.S ARMY TRAINING & DOCTRINE COMMAND, THE UNITED STATES ARMY CYBERSPACE OPERATIONS CONCEPT CAPABILITY PLAN 2016-2028, at 67 (2010), *available at* http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf.

15. Michael N. Schmitt, *Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 913-14 (1999). This approach appears to draw on the kinetic-effect approach coined by Michael Schmitt. In an attempt to resolve the definitional problem of armed attack, Schmitt removes economic and political coercion by focusing on the kinetic effects of the cyber attacks on the actual nation-state.

16. YORAM DINSTEIN, WAR, AGGRESSION, AND SELF-DEFENCE 196 (4th ed. 2005). International Legal Scholar Yoram Dinstein agrees with the effects-approach. Dinstein argues that what counts in determining whether an electronic computer network attack rises to the level of an armed attack under the U.N. Charter is the consequence of the assault. In his opinion, shutting down computers that control dams and causing wide-scale flooding that results in casualties is the equivalent of an armed attack.

17. N. Atlantic Treaty Org., *NATO 2020: Assured Security; Dynamic Engagement* 6-7 (May 17, 2010), *available at* http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf.

18. Declaration of the Heads of the SCO Member States on International Information Security, June 15, 2006, *unofficial translation available at* http://www.fidh.

Although Russia, China and the United States began official talks nearly two years ago,[19] state representatives have yet to reach a consensus as to when a cyber attack rises to the level of an armed attack and, in turn, when a cyber attack violates international law.[20]

Just as the definitions of cyber attacks vary among nations, the variety of hostile activities capable of being carried out over computer networks is equally vast, ranging from malicious defacement of websites to large-scale destruction of SCADA[21] infrastructures that civilians depend upon. The most common cyber tools employed by private and state hackers are Structured Query Language ("SQL") code injection, Distributed Denial of Service ("DDoS"), and Worms. While many of these cyber tools characterize recent developments in cyber espionage and the use of each tool alone does not result in damage, their objective and combined use can quickly breed an atmosphere of war. Keeping the United States effects-based approach in mind, the following descriptions illustrate the wide-range and scope of recent

---

org/IMG/article_PDF/article_a11315.pdf. The Shanghai Cooperation Organization, an intergovernmental mutual-security organization founded in 2001 by Russia and China, appears to have adopted an expansive vision of cyber-attacks to include the use of cyber-technology to undermine political stability. The organization has "express[ed] concern about the threats posed by possible use of [new information and communication] technologies and means for the purposes [sic] incompatible with ensuring international security and stability in both civil and military spheres." *See* CARR, *supra* note 10, at 1-10.

19. *See* John Markoff & Andrew E. Kramer, *In Shift, U.S. Talks to Russia on Internet Security*, N.Y. TIMES, Dec. 12, 2009, at A1, *available at* http://www.nytimes.com/2009/12/13/science/13cyber.html; Claudine Beaumont, *US and Russia in "Secret" Cyber Warfare Talks*, TELEGRAPH (Dec. 14, 2009), http://www.telegraph.co.uk/technology/news/6808883/US-and-Russia-in-secret-cyber-warfare-talks.html; Cheng Guangjin, *US Official Rules Out Chance of "Cyber War" with China*, CHINA DAILY (Oct. 20, 2011), http://usa.chinadaily.com.cn/us/2011-10/20/content_13938436.htm. In 2009, the United States began talks with Russia and a United Nations arms control committee about limiting the militarization of cyberspace. The United States has also been holding discussions with China over the last two years as well.

20. Diane Bartz & Paul Eckert, *U.S. and China Face Vast Divide on Cyber Issues*, REUTERS (July 14, 2011), http://www.reuters.com/article/2011/07/14/us-usa-china-cyber-idUSTRE76D3K020110714; Guangjin, *supra* note 19; John Markoff, *Step Taken to End Impasse Over Cybersecurity Talks*, N.Y. TIMES, July 16, 2010, at A7, *available at* http://www.nytimes.com/2010/07/17/world/17cyber.html. A group of cyber security specialists and diplomats representing fifteen countries agreed on a set of recommendations to the United Nations Secretary General for negotiations on an international computer security treaty, but was subsequently rejected by the United States for censorship concerns. Two years later at the 2011 annual cabinet-level U.S.-China Strategic and Economic Dialogue, the conference included cyber security for the first time, but produced no breakthroughs. Bilateral discussions between the United States, China, and Russia are ongoing.

21. SCADA (supervisory control and data acquisition) generally refers to industrial control systems (ICS): computer systems that monitor and control industrial, infrastructure, or facility-based processes. *See* Donald B. Ashton & Daniel W Nagala, *SCADA*, PIPELINE AND GAS TECHNOLOGY, Nov./Dec. 2004, at 26-27; Graham Nasby & Matthew Phillips, *SCADA Standardization*, INTECH, May/June 2011, at 18.

attacks, emphasizing that their objective use transforms them beyond tools for espionage and into weapons of war.

SQL Code Injection

Long used as an essential part of any hacking activity, the dangers of SQL code injection became known to the public in 2011 when online group Lulzsec shutdown the Sony Playstation Network for over a month.[22] SQL code, an international programming language designed for managing data in relational database management systems ("RDBMS"),[23] serves as the current industry-standard for website database language.[24] However, such standardization of web sites makes it easy for hackers to gain access to multiple databases as the Achilles' heel of one website is often the same as another. SQL injections alter the predefined logical expressions within a predefined query by injecting operations which always result in true or false statements.[25] In turn, hackers can run random SQL queries and extract sensitive user information from applications or bypass security mechanisms and compromise the backend of server or network.[26] Hackers utilizing SQL injection techniques may gain legitimate username and password information to sensitive government databases and aid in intelligence gathering or espionage activities. However, passive cyber activities that merely observe or gather data, as previously mentioned, are not weapons or acts of war. Rather, SQL injection enters the realm of cyber warfare by operating as a stepping-stone for further cyber attacks: Once a computer network is infiltrated, a hacker can execute a variety of attacks, including planting logic bombs or other malicious coding to damage the computer network.

---

22. Adam Clark Estes, *The Hacks that Mattered in the Year of the Hack*, ATLANTIC WIRE (Dec. 28, 2011), http://www.theatlanticwire.com/technology/2011/12/hacks-mattered-year-hack/46731.

23. Christine McGeever, *Structured Query Language*, COMPUTERWORLD, May 15, 2000, at 70. Structured Query Language (SQL) is a programming language designed to get information out of and put it into a relational database. Queries are constructed from a command that lets you select, insert, update, and locate data.

24. *See, e.g.*, KEVIN KLINE ET AL., TRANSACT-SQL PROGRAMMING 52 (1999); Orest Halustchak, *Proposed Spatial Data Handling Extensions to SQL*, *in* TOWARDS SQL DATABASE LANGUAGE EXTENSIONS: FOR GEOGRAPHIC INFORMATION SYSTEMS 69 (VINCENT B. ROBINSON & HENRY TOM eds.,1993); DEJAN SARKA, ITZIK BEN-GAN, LUBOR KOLLAR & STEVE KASS, INSIDE MICROSOFT® SQL SERVER® 2008: T-SQL QUERYING 273 (2009).

25. Theodoros Tzouramanis, *SQL Code Poisoning: The Most Prevalent Technique for Attacking Web Powered Databases*, *in* CYBER WARFARE AND CYBER TERRORISM 161 (Lech J. Janczewski & Andrew M. Colarik eds., 2008).

26. CHRIS ANLEY, NEXT GENERATION SEC. SOFTWARE RESEARCH, ADVANCED SQL INJECTION IN SQL SERVER APPLICATIONS 3-4 (2002), *available at* http://www.cgi security.com/lib/advanced_sql_injection.pdf.

Distributed Denial of Service Attacks

DDoS attacks have been the most prevalent form of cyber attack in recent years[27] and predated both the 2007 attacks on Estonia and the 2008 Georgian bombings. DDoS attacks use an unknown number of servers to deny access to a specific site by overloading the network with data packets, thus preventing it from processing legitimate requests.[28] Using a DDoS attack disguises the attack as a legitimate attempt to access the server or web site through controlling a collective of computers at different locations called "zombies." Although current software can detect basic DDoS attacks, prevention remains extremely difficult as intrusion software cannot distinguish whether the data request is an attack or real connection attempt.[29]

Although damages from a DDoS attack against a web site range from user inconvenience from lack of site reliability to the complete shut down of the server and delay,[30] a strong enough DDoS attack may effectively serve as the equivalent of a military blockade. Just like the blockade of East Germany during World War II, the DDoS attacks on Estonia might also be analogized to a military blockade. For example, the 2007 DDoS attacks on the government of Estonia were so severe that the attacks effectively shut down government communications for weeks, knocking out the emergency lines for hours.[31] Georgia fell under a similar fate in 2008, when a DDoS attack prevented it from communicating with the outside world.[32] Though inconvenience and delay in communications are often not considered acts of war, these scenarios are analogous to a missile being used to take out a government's communication center: such a DDoS attack would constitute an act of war.

Worms

Worms have come to light in recent years with the advent of wide-scale disabling network attacks, such as the Conficker worm and the Stuxnet attack on Iran's nuclear reactors. Another threat to cyber security and military networks across the globe, worms are self-

27. George Disterer et al., *Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation*, *in* CYBER WARFARE AND CYBER TERRORISM 262-63 (Lech Janczewski & Andrew M. Colarik eds., 2008).

28. John Worthy & Martin Fannin, *Denial-of-Service: Plugging the Legal Loopholes*, COMPUTER LAW & SECURITY REPORT 194-98 (2007).

29. Disterer et al., *supra* note 27, at 263.

30. *Id.*

31. *Cyberwarfare: Newly Nasty*, ECONOMIST, May 24, 2007, *available at* http://www.economist.com/node/9228757.

32. Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: the Need for Individual Accountability on Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV. 3, 3-6 (2010).

replicating malware computer programs, which use a computer network to send copies of itself to computers on a network, sometimes without any user intervention.[33] Due to the security shortcomings on the target computer, the worm begins replicating and sending out hundreds or thousands of copies of itself. Unlike DDoS attacks, the presence of a worm almost always results in damage to the computer network.[34] Although worms wreak havoc on computer networks, the nature of worms is rooted in espionage and data gathering through electronic eavesdropping.[35] Worms function primarily by hiding on a computer and through their presence granting access to the device. While the presence is not generally enough to cause a problem, worms more often than not multiply at an unprecedented rate, consuming large amounts of bandwidth and corrupting computer network performance[36]

Over the last half decade, worms have become major tools in toppling entire computer networks. In the summer of 2010, a computer worm coined "Stuxnet" had the world's leading cyber security experts up in arms as the self-replicating computer worm made its way through computers the world over. The goal of the Stuxnet worm was to physically, not figuratively, destroy a military target.[37] Believed to be distantly related to the Conficker[38] worm, Stuxnet targeted Siemens industrial software and equipment, specifically the computer systems that run Iran's main nuclear enrichment facilities, by activating when

33. Kevin Curran et al., *Hacking and Eavesdropping, in* CYBER WARFARE AND TERRORISM 308 (Lech Janczewski & Andrew M. Colarik eds., 2008).

34. *See* O. Toutonji & S. Yoo, *An Approach against a Computer Worm Attack*, 1.2 INT'L J. COMM. NETWORKS AND INFORMATION SEC. 47, 53 (2009); R.D. VINES, WIRELESS SECURITY ESSENTIALS, DEFENDING MOBILE SYSTEMS FROM DATA PIRACY 200 (2002).

35. Curran et al., *supra* note 33.

36. *United States v. Morris*, 928 F.2d 504, 505 (2d Cir. 1991). The Morris worm on November 2, 1988, was one of the first computer worms distributed via the Internet. According to its creator, the Morris worm was not written to cause damage, but to gauge the size of the Internet. A supposedly unintended consequence of the code, however, caused it to be more damaging: a computer could be infected multiple times and each additional process would slow the machine down, eventually to the point of being unusable.

37. William J. Broad, et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 16, 2011, at A1, *available at* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&pagewanted=all.

38. *Protect Yourself from the Conficker Worm*, MICROSOFT (Apr. 4, 2009), http://www.microsoft.com/security/pc-security/conficker.aspx; John Markoff, *Worm Infects Millions of Computers Worldwide*, N.Y. TIMES, Jan. 23, 2009, at A12, *available at* http://www.nytimes.com/2009/01/23/technology/internet/23worm.html; John Markoff, *Defying Experts, Rogue Computer Code Still Lurks*, N.Y. TIMES, Aug. 27, 2009, at A1, *available at* http://www.nytimes.com/2009/08/27/technology/27compute.html. Conficker uses flaws in Windows software to co-opt machines and link them into a virtual computer that can be commanded remotely by its authors. With more than five million of these zombies now under its control — government, business and home computers in more than 200 countries.

the worm detected the presence of a specific configuration of Siemens controller that appear to exist only in a centrifuge plant.[39] Creators of Stuxnet designed the computer worm to remain inert long periods before accelerating the spinning rotors in the centrifuges beyond the burst frequency, resulting in both the bearings and tubes of the rotors breaking.[40] Stuxnet also included a man-in-the-middle code that sent out false industrial process control signals, rendering the aberrant behavior undetectable to diagnostic systems.[41] In turn, the man-in-the-middle code prevented the safety system from engaging, which would shut down the centrifuge plant before self-destruction.

As demonstrated in the preceding paragraphs, cyber tools, like Stuxnet and the wide-scale DDoS attacks on Estonia, have the potential to inflict massive amounts of damage on a state computer network, or even a nuclear reactor. On their own, these tools of the hacker trade may look like espionage activities, but used in conjunction and with the right intent, may bring about effects similar or equivalent to those of an armed attack. Recognizing that cyber tools can rise to the level of armed attacks, the next issue facing the United States and the international community is how to regulate and limit the use of this technology in the fifth domain of battle, cyberspace.

In the last fifty years, the control of the production and use of certain weapons has taken on increasing urgency as technological progress during the Cold War opened doors for the development of far more devastating weapons than any means of prior conventional warfare.[42] In the post-WWII environment, arms control treaties have burgeoned, prohibiting or regulating under the Law of Armed Conflict the use of new weaponry developments ranging from chemical and biological, to nuclear arms.[43] As little to no difference exists between benevolent and malevolent coding[44] and the use of coding is available to anyone with a computer, completely banning these cyber weapons remains highly unlikely and equally ineffective. Cyber weapons, with their increasing propensity for harms to state infrastructure and computer networks, stand posed as the next evolution of warfare and in turn, weapons governed or prohibited by the Law of Armed Conflict.

---

39. Broad, et al., *supra* note 37.

40. *Id.*

41. *Id.*

42. *See* GEOFFREY BEST, HUMANITY IN WARFARE 304-05 (1983); WILLIAM BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 357 (2009); MICHAEL E. O'HANLON & MICHAEL A. LEVI, THE FUTURE OF ARMS CONTROL 1-12 (2004).

43. O'HANLON & LEVI, *supra* note 42, at 62, 159.

44. J. Morales et al., Symptoms-Based Detection of Bot Processes, Proceedings of the Mathematical Methods, Models and Architectures for Computer Network Security Conference (Sept. 7-10, 2010).

II. THE LAW OF ARMED CONFLICT AND CYBER WARFARE

The Law of Armed Conflict is the legal corpus comprised of the Geneva Conventions and the Hague Conventions, as well as subsequent treaties, case law, and customary international law.[45] The Law of Armed Conflict "arises from a desire among civilized nations to prevent unnecessary suffering and destruction while not impeding the effective waging of war."[46] A part of public international law, the Law of Armed Conflict regulates armed hostilities and applies to military operations and related activities conducted during an international armed conflict.[47] In the case of cyber attacks, the form and degree of network attacks are a major factor in determining whether a nation may respond by force in self-defense. The language used to develop these rules does not easily translate into cyberspace so there is no common understanding on how they will apply to this new war-fighting domain. Not only must Internet activity rise to the level of an armed attack under the Law of Armed Conflict, but must also meet the required elements of necessity, proportionality, and attribution.

Serving as the pillar of the right to self-defense within the Law of Armed Conflict, Article 51 of the U.N. Charter provides for the right of countries to engage in military action in self-defense, including collective self-defense, if they come under an "armed attack" from another state.[48] If the attack is real or the threat has proceeded beyond the point of no return, the victim state of a cyber attack, without any alternative means, may use self-defense to justify reasonable, necessary, and proportional measures to maintain the security of the state under Article 2(4) of the U.N. Charter.[49] In turn, the armed attack requires a precondition that the use of force produces or is liable to produce serious consequences. When no such results materialize, Article 51 does not come into play. However, many nations, particularly members of the U.N. Security Council, have yet to arrive at a consensus

45. GARY SOLIS, THE LAW OF ARMED CONFLICT 7-10 (2010); *What is International Humanitarian Law?*, INT'L COMMITTEE OF THE RED CROSS, 1 (July 2004), http://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf.

46. Solis, *supra* note 45; Leslie Green, *What is--Why is there- the Law of War?*, *in* 71 INTERNATIONAL LAW STUDIES: THE LAW OF ARMED CONFLICT INTO THE NEXT MILLENNIUM 141, 161 (Schmitt & Green eds., 1998); Thomas W. Pittman & Linda S. Murnane, *The Law of Armed Conflict in Modern Warfare*, 42 JUDGES' J. 18, 18 (2003).

47. SOLIS, *supra* note 45, at 23; ROBERT KOLB & RICHARD HYDE, AN INTRODUCTION TO THE INTERNATIONAL LAW OF ARMED CONFLICTS 65 (2008); William Taft, *The Law of Armed Conflict after 9/11: Some Salient Features*, 28 YALE J. INT'L L. 319, 319 (2003).

48. U.N. Charter art. 51.

49. JEFFREY CARR & LEWIS SHEPHERD, INSIDE CYBER WARFARE: MAPPING THE CYBER UNDERWORLD 56 (2009).

on what the right to self-defense means in the event of an attack on a country's computer networks.[50]

In determining whether a cyber attack constitutes an armed attack warranting self-defense, any examination under Article 51 must also consider Articles 41 and 42. Article 41 lists measures "not involving the use of armed force," including "complete or partial interruption . . . of telegraphic, radio, and other means of communication."[51] Since Article 41 describes actions not involving the use of force, a cyber attack initially does not appear to fall into the category of armed attack. However, this ignores the vast propensity described in Part I of this paper for a cyber attack to wreck wide-spread damage and harm on vital civilian and military networks, resulting in equally or more devastating harm than that brought about by more traditional modes of warfare.

If a cyber attack is determined to have risen to the level of an armed attack, the response of the state must be necessary, proportional, and attributive.[52] In its *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, the International Court of Justice stated, "the submission of the exercise of the right of self-defense to the conditions of necessity and proportionality is a rule of customary international law" and "this dual condition applies equally to Article 51 of the Charter, whatever the means of force employed."[53] Necessity entails that the state invoking self-defense establish that a genuine armed attack, not an accident or mistake, was launched by a particular country and that the immediacy of the danger provides no reasonable alternative means for responding.[54] However, the condition of necessity is inherent in responding to any state-sponsored cyber attack; all cyber attacks call for immediate self-defense if there is any chance for the extremely destructive potential of cyber tools to be stopped from spreading into the civilian realm or wreck wide-spread damage.

Under the Law of Armed Conflict, the proportionality doctrine forbids the use of any kind or degree of force that exceeds that required to fulfill the military objective.[55] Article 51(5)(b) of the U.N. Charter codifies proportionality and directs that attacks on a specific military objective are impermissible if they "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a

50. 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, 426-27 (2011).

51. U.N. Charter art. 41.

52. CARR, *supra* note 18, at 56.

53. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 245 (July 8).

54. Beth M. Polebaum, *National Self-Defense in International Law: An Emerging Standard for a Nuclear Age*, 59 N.Y.U. L. REV. 187, 198 (1984).

55. *Id.* at 198-200.

combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[56] A responsible state actor intent on a particular target must then first determine if it is a military objective, and then whether the collateral damage from destruction of the target is proportionate to the military advantage of destroying it.[57] These articles do not entirely prohibit civilian casualties under international law, but rather attempt to minimize the number of civilian casualties as much as possible and ensure that any injury is sufficiently justified.[58] In preparation for an attack, Article 57 requires planners to "take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[59] In other words, if a weapon cannot discriminate between military and civilian objects, the use of such weapon is illegitimate.[60]

Due to the high level of interconnectivity between civilian and military networks, cyber warfare operations risk producing collateral damage in the civilian realm that is far beyond the intended effects of the attack.[61] Regardless of whether cyber attacks result in damage beyond the target computer program or data, the estimated amount of damage done would need to come from the victim state as the effects on civilian networks or infrastructure are often not immediately visible.[62] For example, 95 percent of the United States military information transfers, and 90 percent of major corporation information transfers, take place or depend on civilian networks.[63] Should a state interfere

56. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 51, 1125 U.N.T.S. 3 (*entered into force* Dec. 7, 1978) [hereinafter Protocol I].

57. Jefferson D. Reynolds, *Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground*, 56 A.F. L. REV. 1, 25 (2005).

58. *See* Protocol I, *supra* note 56 (stating an indiscriminate attack is one that an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated); Thomas & Murnane, *supra* note 46; Wolff Heintschel von Heinegg, *Asymmetric Warfare: How to Respond*, 87 INT'L L. STUD. 463, 470 (2011).

59. Protocol I, *supra* note 56, art. 57.

60. *Id.* art. 51(4) (stating that indiscriminate attacks are prohibited and include attacks that indiscriminate attacks are not directed at a specific military objective, employ a method or means of combat which cannot be directed at a specific military objective; or which employ a method or means of combat the effects of which cannot be limited).

61. JASON ANDRESS & STEVE WINTERFIELD, CYBER WARFARE: TECHNIQUES, TACTICS AND TOOLS FOR SECURITY PRACTITIONERS 233 (2011).

62. *Id.*

63. Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV 132, 132-33 (2005).

with a military information transfer, the attack could easily spillover into civilian communications by sheer virtue of occurring on the same computer network.

While the effects of a proposed cyber attack may be difficult to estimate, ascertaining or gauging the extent of damage to civilians is not impossible. In fact, cyber attacks generally target a specific database or network through code design. Although criticized for allowing a specifically targeted attack to enter into public networks around the globe,[64] the creators of Stuxnet could feasibly have refined the coding so as not to spread outside the intended network.[65] In addition to code design, deleting military files, or even disabling military computer networks, would limit damages to a proper military target. Combining these aforementioned activities with proper intelligence gathering and operational planning, the state hacker could restrict their activities to military networks and avoid networks dedicated solely to medical or other public facilities. Otherwise, the cyber attacks will likely be indiscriminate and spillover into the civilian realm.

Even if a response meets the requirements of proportionality and necessity, an attack must be attributable to a state because the laws governing an action of self-defense depend upon whether the attacker is a nation-state or a non-state actor.[66] Generally, the international law of self-defense prohibits the use of force by a victim state, unless the act of aggression can be conclusively attributed to a state or an agent thereof.[67] As the Article 2(4) prohibition on the use of force applies only

---

64. Michael Gross, *A Declaration of Cyber-War*, VANITY FAIR (Apr. 2011), http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104; Gregg Keizer, *Secrets of the Stuxnet Worm's Travels*, COMPUTERWORLD (Oct. 3, 2010), http://www.pcworld.com/article/206822/secrets_of_the_stuxnet_worms_travels.html?tk=hp_new (explaining that Stuxnet was aimed at a specific target list, but spread to thousands of PCs outside Iran, in countries including China, Germany, Kazakhstan, and Indonesia); John Markoff, *A Silent Attack, but Not a Subtle One*, NY TIMES, Sept. 27, 2010, at A6, *available at* http://www.nytimes.com/2010/09/27/technology/27virus.html?partner=rss&emc=rss; Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1.

65. Gregg Keizer, *supra* note 64; *Unraveling Stuxnet*, KASPERSKY LABS (Jan. 16, 2011), http://www.youtube.com/watch?v=5YpwNBTdO18. Senior Antivirus Expert at Kaspersky Lab Roel Schouwenberg believes that because an initial infected-USB based attack failed, the creators of Stuxnet took the risk of it spreading by adding more functionality to the worm. Liam O Murchu, operations manager with Symantec's security response, agrees with Schouwenberg.

66. Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 451 (2009).

67. JACKSON NYAMUYA MAOGOTO, BATTLING TERRORISM: LEGAL PERSPECTIVES ON THE USE OF FORCE AND THE WAR ON TERROR 169 (2005); Michael Glennon, *The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter*, 25 HARV. J.L. & PUB. POL'Y 539 (2002); Levi Grosswald, *Cyberattack Attribution Matters*

to states and not to individuals, attribution to a state actor is inescapable.[68] However, knowledge of the state of origin of a cyber attack, alone, does not identify the individual, or country, that initiated the attack.

An experienced hacker can easily hide their tracks by routing through zombie computers that are hacked or compromised without the knowledge of the owner, as seen in the attacks on Estonia.[69] More recently, a detailed study by the Information Warfare Monitor uncovered "Ghostnet," a cyber espionage plot based in China that compromised more than a thousand sensitive government and commercial computer systems from around the world.[70] The plot managed to infiltrate computer systems belonging to embassies, foreign ministries and other government offices in India, London, and New York City.[71] However, the report could not conclude whether the Chinese government or private hackers working in their own political interest controlled the plot. At the same time, the report could neither reject the possibility that a state other than China was behind the plot, routing through zombie computers in China to "deliberately mislead observers as to the true operator and purpose of the Ghostnet system."[72] Even with today's highly advanced trace-back and forensic technologies, the attribution of a cyber attack remains exceedingly difficult.[73] Consequently, states acting on the legal requirement of attribution continue to handle transnational cyber attacks as any other criminal matter on the Internet, resorting to traditional public sector cyber security measures and leaving investigation and prosecution to the originating state. However, even the best cyber security framework is not invincible and countries are often unwilling to investigate.

Under Article 51 of the U.N. Charter, 36 BROOK. J. INT'L L. 1151, 1155 (2011). Article 51 U.N. Charter requires that the attack be carried out as an "act of a state," which means that it must be attributable to a state.

68. Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defense*, 38 STAN. J. INT'L L. 207, 232-35 (2002).

69. Ryan Singel, *Zombie Computers Decried as Imminent National Threat*, WIRED (Apr. 9, 2008), http://www.wired.com/threatlevel/2008/04/zombie-computer.

70. John Markoff, *Vast Spy System Loots Computers in 103 Countries*, N.Y. TIMES, Mar. 29, 2009, at A1, *available at* http://www.nytimes.com/2009/03/29/technology/29spy.html?pagewanted=all.

71. *Id.*

72. Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC (June 7, 2010), http://www.tnr.com/article/books-and-arts/75262/the-new-vulnerability?page=0,2.

73. Andre Arnes, *Identification and Localization of Digital Addresses on the Internet*, *in* CYBER WARFARE AND CYBER TERRORISM 368-69 (Lech J. Janczewski & Andrew M. Colarik eds., 2008).

Duties Between States and The Doctrine of Imputability

Given the difficulties raised by the attribution requirement of the Law of Armed Conflict and increasing fear of another attack similar to Stuxnet, the international community has seen considerable activity by various state actors over the last half decade in the pursuit of feasible options to conclusive attribution. Prior to 1972, state responsibility only extended to those acts committed through state "agents."[74] International law, nevertheless, started to shift towards a doctrine of indirect responsibility with the International Tribunal for the former Yugoslavia's seminal opinion on state responsibility in the *Tadic* case.[75] In *Tadic*, the court found that even though the state may not have directed a particular act, the state still exercised "overall control" for the actions of combatants.[76] Although overall control denotes a manner of direct state control, the *Tadic* ruling signals a shift in international law towards holding states responsible for the acts of persons within their borders.

This shift continued through the last decade with the events of the September 11 terrorist attacks on the United States. Now, a large amount of the international community generally accepts that non-state actors who have committed armed attacks against other states can impute responsibility onto the state they are operating within.[77] This doctrine of state imputability rests upon the premise of a positive obligation of states to prevent their territories from being used as safe havens for not only terrorist attacks, but any attack that would inflict harm on a foreign state.[78] Consequently, U.N. declarations have increasingly concerned cyber attacks, with the U.N. General Assembly calling upon states to institute domestic criminal charges for persons engaging in malicious cyber activity and to take proactive measures to prevent becoming safe havens for such criminals.[79]

---

74. The Diplomatic and Consular Staff Case (U.S. v. Iran), 1980 I.C.J. 3, 29 (May 24).

75. *Prosecutor v. Tadic*, Case No. IT-94-1, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995). *See also* Rachael Lorna Johnstone, *State Responsibility: A Concerto for Court, Council and Committee*, 37 DENV. J. INT'L L. & POL'Y 63 (2008).

76. Tadic ¶ 70. The court distinguished between state responsibility for individual actors and responsibility for operations of "organized and hierarchical structured groups," such as military units where effective control may not be necessary to carry out state objectives. The court also drew on the substantial political, military, and financial aid provided to the combatants. The court found that atrocities only need to be committed in part with the state resources and that the state have knowledge of the circumstances by an organ of the state to be responsible.

77. CARR, *supra* note 18, at 53.

78. TAL BECKER, TERRORISM AND THE STATE: RETHINKING THE RULES OF STATE RESPONSIBILITY 3 (2006).

79. G.A. Res. 55/63, U.N. Doc. A/RES/55/63 (Dec. 4, 2000).

The doctrine of state imputability turns upon the requirement of due diligence, a long held principle of international law.[80] Under international law, a state must "use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people."[81] Following on this principle, the U.N. General Assembly maintains that a state has an obligation to prevent and punish these injurious acts.[82] When the actions of a state do not conform to this international obligation, that obligation is breached. As such, a breach of an international obligation is an international wrong and that state is then responsible to other states for the injury inflicted as a result of that wrongful act.[83] In order to effectively impute responsibility onto a nation-state for a breach of due diligence, the victim state must at "minimum examine a sanctuary state's criminal law dealing with cyber attacks, its enforcement of the law, and its demonstrated record of cooperation with the victim states' own investigations and prosecutions of cyber offenders who have acted across borders."[84] This became a recent political reality when responsibility for the September 11 attacks by al Qaeda was extended to the Taliban Government of Afghanistan after evidence revealed that the Taliban Government following the September 11attacks continued to provide safe harbor to al Qaeda after multiple warnings to stop.[85] Adhering to this rationale, a sanctuary state's indifference to cyber attacks launched from within its borders and its failure to cooperate with investigation efforts may very well result in charges of imputed responsibility.

Admittedly, placing the responsibility on states for cyber attacks committed within their borders potentially unleashes a Pandora's box of

---

80. *See* Robert Perry Barnidge Jr., *The Due Diligence Principle Under International Law*, 8 INT'L COMMUNITY L. REV. 81 (2006); Jan Hessbruege, *Historical Development of the Doctrines of Attribution and Due Diligence in International Law*, 36 N.Y.U. J. INT'L. L. & POL'Y 265 (2004).

81. S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 9 (Sept. 7). *See also* Corfu Channel (U.K. v. Alb.), 1949, I.C.J. 4, 18 (Apr. 9). The post-Charter court ruled that every state has an obligation to not knowingly allow its territory to be used for acts contrary to the rights of other states.

82. Responsibility of States for Internationally Wrongful Acts, G.A Res. 56/83, U.N. Doc. A/RES/56/83 (Jan. 28, 2002). *See also* U.N. Charter art. 2, para. 4. Any state acquiescing to terrorist activities will be held in violation of Article 2(4).

83. G.A. Res. 56/83, *supra* note 82, art. 31, para. 1.

84. David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L & POL'Y 87, 94 (2010).

85. Vincent-Joël Proulx, *Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?*, 23 BERKELEY J. INT'L L. 615, 619-20 (2005). *See also* S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001). Security Council Resolution 1368 includes the harboring of those perpetrators, organizers, and sponsors of terrorist acts as imputing state responsibility. The term "those" is sufficiently broad to include non-state actors.

problems, particularly in determining whether the state initiated adequate control measures over the hackers. Regardless, the current status quo is unacceptable; in several recent cases of cyber attacks on states, countries from which the attacks originated refused to accept responsibility and even refused to cooperate with investigations.[86] Furthermore, many countries have yet to enact any sort of cyber crime laws or the existing laws are rendered ineffective through gaps in the statutory language.[87] In light of these considerations, the international community must continue to advocate for greater recognition of each state's positive duty under international law to actively prevent the use of its territory for acts harmful to another state and the international community.

III. THE FUTURE OF U.S. CYBER WAR STRATEGY: BILATERAL TREATIES

Expanding the doctrine of state imputability to attacks waged in cyberspace requires codification, similar to an arms control treaty,[88] recognizing the role of computer technology and the Internet to conduct attacks on other nations within the Geneva Convention and the Law of Armed Conflict. Much as arms control treaties are used to limit the damage done in warfare by restricting the usage of new innovative

86. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 46 (2009).

87. Jonah Fisher, *Efforts to steer young Nigerians away from cybercrime*, BBC (Dec. 15, 2011), http://www.bbc.co.uk/news/world-africa-16192839; John Leyden, *Nigeria Fails to Enact Cyber Crime Laws*, REGISTER (Apr. 1, 2011), http://www.theregister.co.uk/2011/04/01/nigeria_cybercrime_law_fail; *Brazilian justice minister urges inclusion of cyber crime into criminal code*, XINHUA NEWS (June 30, 2011), http://news.xinhuanet.com/english2010/world/2011-06/30/c_13957924.htm. Both Brazil and Nigeria continually rank high for cyber crime, but neither country has a set of cyber crime laws.

88. Paul Wagenseil, *Cyberweapons Treaties Might Help Prevent Cyberwar*, SECURITY NEWS DAILY (Oct. 26, 2011), http://www.securitynewsdaily.com/cyberweapons-treaties-cyberwar-1276/. At the 2011 Hacker Halter cyber security conference, BT chief cyber security officer, Bruce Schneier, proposed establishing a cyber weapons treaty, crediting former presidential adviser Richard Clarke for the idea from his 2010 book "Cyber War: The Next Threat to National Security and What to Do About It." Schneier claims that just as there are mechanisms for enforcing nuclear arms and chemical weapons treaties, the same could be developed for cyber weapons. He recommends a no first use policy, outlawing unaimed weapons, and mandating weapons that self-destruct at the end of hostilities. *See also* Hamish Barwick, *Global cyber war treaties urgently needed: Bruce Schneier*, COMPUTERWORLD (Nov. 8, 2011), http://www.computerworld.com.au/article/406751/global_cyber_war_treaties_ urgently_needed_bruce_schneier; Barbara Honegger, *Former Counterterrorism Czar Richard Clarke Calls for New National Cyber Defense Policy to Prevent a Cyber 9/11*, NAVAL POSTGRADUATE SCH. NEWS (Dec. 9, 2011), http://www.nps.edu/About/News/Former-Counterterrorism-Czar-Richard-Clarke-Calls-for-New-National-Cyber-Defense-Policy-to-Prevent-a-Cyber-9/11-.html; Bruce Schneier, *It Will Soon be Too Late to Stop the Cyberwars*, LONDON FIN. TIMES (Dec. 2, 2010), http://www.ft.com/cms/s/f863fb4c-fe53-11df-abac.

weaponry,[89] states have a similar interest in limiting the use of cyber tools in armed conflicts to minimize, or altogether prevent, collateral damage to civilian populations and damage of both critical governmental and civil infrastructure.[90] Unfortunately, the United States and several Security Council members vary widely as to what activity by a state on the Internet arises to the level of an act of aggression or armed attack in the digital world. For example, the Shanghai Cooperation Organization, of which members include China and Russia, asserts cyber war includes the dissemination of information "harmful to the spiritual, moral and cultural spheres of other states."[91] Russia maintains that anytime a government promotes ideas on the Internet with the goal of subverting another country's government that it has committed an illegal act of aggression under the U.N. Charter.[92] In contrast, the United States would rather not include political acts that may result in censorship and freedom of speech issues, and instead focuses on the physical and economic damage and injury caused by cyber attacks.[93] The United States also remains skeptical of Russian ideas of an international agreement, since a multilateral treaty could provide cover for totalitarian regimes to censor the Internet in the fashion of Egypt and Libya prior to the Arab Spring.[94] This difference in opinion has led to reluctance by the United States to pursue multilateral international cyber arms control agreements with both Russia and China.

Following recent international treaty trends, the United States is pursuing bilateral treaty agreements to fit the DoD effects-based

89. GUIDO DEN DEKKER, THE LAW OF ARMS CONTROL: INTERNATIONAL SUPERVISION 22 (2001). Arms control agreements refer to all agreements between two or more states to limit or reduce certain categories of weapons or military operations to diminish tensions and the possibility of conflict.

90. *Id.* at 1. The international community benefits more from limited warfare than a peaceful situation in which a state is allowed to pose a serious threat to international peace. *See also* Siobhan Gorman, *U.S. Backs Talks on Cyber Warfare*, WALL ST. J. (June 4, 2010), *available at* http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html Markoff, *supra* note 19, at A1; Andrew Nagorski, *Cyberwar Is Hell*, NEWSWEEK, July 28, 2011, *available at* http://www.thedailybeast.com/newsweek/2010/07/28/cyberwar-is-hell.html. After years of talks that went nowhere, the United States, Russia, China, India, and several others have agreed to begin cyber war limitation talks at the United Nations due to the increase in cyber attacks and their transnational nature.

91. Tom Gjelten, *Seeing the Internet as an "Information Weapon,"* NAT'L PUB. RADIO (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

92. Sergei Korotkov, *Legal Aspects of Informational Operations*, U.N. INSTITUTE FOR DISARMAMENT RESEARCH (Apr. 24, 2008), http://www.unidir.org/audio/2008/Information_Security/08-Korotkov.m3u (last visited Oct. 3, 2011).

93. *See* Grosswald, *supra* note 67, at 1158 n. 39.

94. John Markoff & Andrew E. Kramer, *U.S. and Russia Differ on a Treaty for Cyberspace*, N.Y. TIMES, June 28, 2009, at A1, *available at* http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all.

approach to cyber warfare.[95] Through the course of the last five decades, the international economic legal regime transformed from one of multilateralism to that of a bilateral regime, in large part, due to conflicting national interests, global imbalances and lack of effective global governance. Presumably, nation-states are rational actors, acting out of a cost-benefit mindset of absolute and relative gains.[96] As rational actors, nation-states ratify treaties when the anticipated net-transaction benefits are positive for all ratifying parties at the time of signing.[97] However, treaties generally involve transaction costs for administration, communications, enforcement, and monitoring; all of which can hamper treaty formation and adherence. Monitoring can be extremely difficult and costly in larger treaties as each party must monitor the other in order to guard against treaty violations.[98] Even after detecting a violation, the cost of enforcement is generally high and often uncertain.[99] If countries anticipate a net gain from adhering to treaty stipulations, despite changing circumstances, the treaty becomes self-enforcing.[100] While the treaty must be incentive compatible, signing parties must also perceive a net gain over the threshold transaction

95. White House, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

96. Robert Powell, *Absolute and Relative Gains in International Relations Theory*, 85 AM. POL. SCI. REV. 1303, 1316 (1991). Both contemporary competing theories of Structural Realism and Neoliberal Institutionalism focus on the states balancing gains and losses, however they differ on whether the focus is primarily on absolute or relative gains. Powell resolves the two systems by arguing that states initially look at absolute gains, but then consider the future relative losses that affect the gains.

97. Robert E. Scott & Paul B. Stephan, *Self-Enforcing International Agreements and the Limits of Coercion*, 2004 WIS. L. REV. 551, 583 (2004).

98. U.S. Costs of Verification and Compliance Under Pending Arms Treaties, Congressional Budget Office, xi-xii (1990), *available at* http://www.cbo.gov/ftpdocs/77xx/doc7775/90-CBO-043.pdf. Costs of treaties can be illustrated by the 1990 CBO report on the cost of pending arms treaties. For the five accords together, the total one-time costs of compliance and on-site inspection would range from $0.6 billion to $3.0 billion in 1990 dollars. Recurring costs, beginning with the first year of implementation and continuing indefinitely, are estimated to range from $0.2 billion to$0.7 billion per year for the five accords. More recently, the estimated cost of ratifying the Additional Protocol to the Nuclear Non-Proliferation Treaty was estimated at $20 -$30 million in one time fees, and then a recurring $10-$15 million per year. An estimated $160 million would go to the salaries of 230 inspectors and 200 administrative personnel. *See also* The Cost of Implementing the Additional Protocol to the Treaty on the Non-Proliferation of Nuclear Weapons, Congressional Budget Office (2004), http://www.cbo.gov/doc.cfm?index=5160&type=0.

99. George Downs & Michael Jones, *Reputation, Compliance, and International Law*, 31 J. LEGAL STUD. 95, 104 (2002); Andrew Guzman, *The Design of International Agreements*, 16 EUR. J. INT'L. L. 579, 590 (2005).

100. Todd Sandler, *Treaties: Strategic Considerations*, 2008 U. ILL. L. REV 155, 157 (2008); Scott Barrett, *Self-Enforcing International Environmental Agreements*, 46 OXFORD ECON. PAPERS 878 (1994).

costs. Consequently, nonparticipating nations to a multilateral treaty risk altogether negating the net gains of the treaty.

Nonparticipating states are considered *sine qua non*[101] states by some academics as the absence of their participation gives the law no realistic meaning.[102] These states are pertinent to achieving the objectives of the treaty for without them, there is no restriction or change regarding the cause of the problem.[103] Support for the necessity of *sine qua non* states can be found in recent political and legal reality. For example, in recent years, nations have attempted to create regional agreements to fight terrorism by agreeing not to provide their territories as safe havens for such activities.[104] A single nation, however, offering sanctuary to terrorists can undermine much of the gains for states who deny safe havens by allowing such activities to persist unchecked.[105] Other examples of this are found in the area of environmental law, such as the International Convention for the Prevention of Pollution from Ships (MARPOL) requires the treaty only enters into force after participation by states that represent over 85 percent of the world's gross merchant tonnage.[106] While signatories to the treaty totaled less than half of the globe, the signatories represented over 85 percent of the world's major shipping states and in turn ensured gains by limiting the activities of the biggest polluters.[107]

---

101. Latin for "without which not." An indispensable condition or thing; something on which something else necessarily depends. BLACK'S LAW DICTIONARY (9th ed. 2009)

102. Gary L. Scott & Craig L. Carr, *Multilateral Treaties and the Formation of Customary International Law*, 25 DENV. J. INT'L L. & POL'Y 71, 87 (1997). *See also* Review of the Multilateral Treaty-making Process, U.N. Doc. ST LEG SER.B 21, U.N. Sales No. E F.83.V.8 (1985) (stating that a treaty cannot be effective if not ratified by states whose participation is crucial for implementation of the provision); Andrew Michie, *Provisional Application of Arms Control Treaties*, 10 J. CONFLICT & SEC. L. 349 (2005). Several major arms treaties, including the 1972 Biological Weapons Convention and the 1963 Partial Test Ban Treaty, require that their entry into force is conditional upon the adherence of those states that are militarily or technologically the most significant as the subject matter of the treaty. Arms control treaties that fail to attract adherence of states actually possessing weapons have little practical value.

103. Scott & Carr, *supra* note 102, at 87.

104. *See* Eric Rosand et al., *The UN Global Counter-Terrorism Strategy and Regional and Subregional Bodies: Strengthening a Critical Partnership*, CENTER ON GLOBAL COUNTERTERRORISM COOPERATION (2008), *available at* http://www.globalct.org/images/content/pdf/reports/strengthening_a_critical_partnership.pdf.

105. Todd Sandler, *Collective Versus Unilateral Responses to Terrorism*, 124 PUB. CHOICE 75, 85-87 (2005). *See also* Michie, *supra* note 102 (explaining that the failure of pertinent states to ratify can compromise the security of those states that become party to the agreement because it allows the non-signatory parties to pursue a strategic advantage).

106. Marine Pollution: International Convention for the Prevention of Pollution from Ships (MARPOL), Nov. 2, 1973, 34 U.S.T. 3407, 1340 U.N.T.S. 184.

107. List of Contracting Parties to MARPOL Convention, *available at* https://imo.amsa.gov.au/public/parties/marpol78.html.

The area of cyber crime further reflects this reality as many countries have been hesitant to sign the Convention on Cyber Crime following Russia and China's refusals to sign.[108] As China and Russia serve as the two main hubs for international cyber crime and activity, their absence from the treaty arguably negates the gains in failing to manage the source of the problem.[109] NATO has recommended pushing "notable" non-participants Russia and China to sign onto the Convention on Cyber Crime as a recommended cyber defense initiative.[110] In sum, no net gains exist if the cause of the problem is not part of the agreement and bound by restrictions.

With China, Russia, and the United States unable to reach a consensus, a multilateral international treaty on cyber war currently seems implausible. However, their absence does not mean that states have no options to build a regulatory regime for cyber warfare. While establishing accepted international norms for behavior on the Internet requires time, bilateral treaties provide an alternative to allowing the global community to act arbitrarily as to their own views of cyber warfare. Bilateral treaties not only codify existing customary international law, but also "begin an evolution that creates it."[111] As it currently stands, the United States has committed itself to working "with like-minded states to establish an environment of expectations or norms of behavior, that ground foreign and defense polices and guide international partnerships."[112] The United States viewpoint is that only after governments widely come to a general consensus will analysts be able to develop coordinated policy recommendations and will countries be able to act multilaterally to create a sufficient treaty. In turn, the United States has signed a Memorandum of Understanding with India on Cyber Attacks and added an extension to the Australia, New Zealand, United States Security Treaty (ANZUS or ANZUS Treaty) that extension allows the United States and Australia to use technology

108. Markoff & Kramer, *supra* note 94.

109. Lolita C. Baldor, *U.S. Report Blasts China, Russia For Cyber Crime*, USA TODAY (Nov. 3, 2011), http://www.usatoday.com/money/industries/technology/story/2011-11-03/Cyber-attacks/51058852/1. The United States has known for years, but finally publicly announced that China and Russia are responsible for harboring cyber crimes and stealing sensitive United States technology data in an attempt to highlight the risks of cyber attacks in a growing high-tech society.

110. Sverre Myrli, *173 DSCFC 09 E bis - NATO and Cyber Defense - 2009 Annual Session*, ¶ 64, *available at* http://www.nato-pa.int/default.Asp?SHORTCUT=1782.

111. M. Cherif Bassiouni, INTERNATIONAL CRIMINAL LAW: MULTILATERAL AND BILATERAL ENFORCEMENT MECHANISMS 127 (2008).

112. White House, *supra* note 95, at 9. The United States is currently prepared to build bilateral and multilateral partnerships, to work with regional organizations, and to collaborate with the private sector.

to cooperate in the event of a large-scale cyber attack.[113] The United States has chosen to first pursue bilateral arms-control and defense treaties since multilateral treaties are inherently harder to monitor and figure out which states follow their obligations, rather than hiding behind the guise of proxies.[114] In turn, the United States posits itself to quickly determine which countries will be not only accept their definition of cyber warfare, but also adhere to the guidelines being established.

While the turning point for Russia and China is the dissemination of information harmful to "political, economic, and social systems" as well as "spiritual, moral and cultural,"[115] parties to a multilateral treaty could feasibly tackle these discrepancies in the future by treaty reservations or reaching a compromise. However, such resolutions of divergent views on cyber attacks cannot be resolved for a country housing one of the largest cyber commands: Iran. The Iranian government blames the United States and Israel for the release of the debilitating Stuxnet work into its nuclear reactor computer networks.[116] Exactly who created Stuxnet remains unproven, but many experts now acknowledge the high likelihood that Israel was behind the attack, possibly aided by the United States.[117] As a result, Iran believes that the United States and Israel initiated the first stages of cyber war, setting the stage for Iran to create their own cyber command to respond to a future Stuxnet.[118] Part of the mission of Iran's new cyber command is the implementation of "retaliatory measures" against a host of nations the Iranian government deems hostile, including the United States and Israel.[119] In fact, Iranian engineers claim the recent drone "crash" in Iran is the beginning of cyber attacks by the Iranian cyber

113. *See* Press Release, *United States and India Sign Cybersecurity Agreement*, DEP'T OF HOMELAND SEC. (July 19, 2011), http://www.dhs.gov/ynews/releases/20110719-us-india-cybersecurity-agreement.shtm.

114. Clarke, *supra* note 10, at 235, 237. *See also* Gabriella Blum, *Bilateralism, Multilateralism, and the Architecture of International Law*, 49 HARV. INT'L L.J. 323, 351-57 (2008).

115. Tom Gjelten, *Seeing the Internet as an "Information Weapon,"* NAT'L PUB. RADIO (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

116. Broad, *supra* note 37; *Stuxnet Worm Hits Iran Nuclear Plant Staff Computers*, BBC (Sept. 26, 2010), http://www.bbc.co.uk/news/world-middle-east-11414483. Following Stuxnet, Mahmoud Liayi, head of the information technology council at the ministry of industries announced to the press that "an electronic war has been launched against Iran." *See also* Gross, *supra* note 64.

117. Broad, *supra* note 37.

118. Atul Aneja, *Under Cyber-attack, Says Iran*, HINDU (Sept. 26, 2010), http://www.thehindu.com/news/international/article797363.ece.

119. Ilan Berman, *Iranian Cyberwar: U.S. Must Prepare for Possible Confrontation*, DEFENSENEWS (Sept. 11, 2011), http://mobile.defensenews.com/story.php?i=7650158.

command to hijack and redirect the drones.[120] Following the drone crash, Iran removed 90 percent of all websites to a local server to protect against anticipated cyber attacks.[121] These factors combined with the fact that the United States has not had formal diplomatic relations with Iran in over three decades,[122] contribute to the unlikelihood that Iran will participate in any multilateral treaty or bilateral treaty involving the United States.

Due to their contribution and potential to wage cyber attacks, Iran is a net loss for any international multilateral cyber warfare treaty. Rather than view Iran's absence from the treaty as destroying its effectiveness, the United States can mitigate the loss with net gains through collective defense and creating international intolerance for certain conduct when engaging in cyber warfare. As Iran now houses one of the largest cyber commands in the world and have stated their intent to implement "retaliatory measures" against hostile nations, it is even more imperative that widespread international norms and guidelines are established before the United States or any other nation is put in the position of another Estonia.

---

120. Rick Gladstone, *Iran Complains to Security Council About Spy Drone*, N.Y. TIMES, Dec. 10, 2011, at A12, *available at* http://www.nytimes.com/2011/12/10/world/middleeast/iran-complains-to-security-council-about-spy-drone.html?ref=iran; Adam Rawnsley, *Iran's Alleged Drone Hack: Tough, but Possible*, WIRED (Dec. 14, 2011), www.wired.com/dangerroom/2011/12/iran-drone-hack-gps. Iran claims to have managed to jam the drone's communication links to American operators by forcing it to shift into autopilot mode. With its communications down, the drone allegedly kicked into autopilot mode, relying on GPS to fly back to base in Afghanistan. With the GPS autopilot on, the engineer claims Iran spoofed the drone's GPS system with false coordinates, fooling it into thinking it was close to home and landing into Iran's clutches.

121. Ramin Mostafavi, *Iran Moves Websites to Guard Against Cyber Attacks*, REUTERS (Dec. 20, 2011), http://www.reuters.com/article/2011/12/20/us-iran-internet-idUSTRE7BJ1VB20111220; *Iran Hosts Local Websites to Avoid Cyber Attacks*, XINHUA NEWS (Dec. 21, 2011), http://news.xinhuanet.com/english/sci/2011-12/21/c_131319917.htm. Iran's deputy minister for communications and information technology said that the Islamic republic transferred the locations more than 30,000 Iranian websites from foreign-based hosting agencies to new computer facilities inside the country to avert potential cyber attacks.

122. Bureau of Near Eastern Affairs, *Background Note: Iran*, U.S DEP'T OF STATE (Feb. 1, 2012), http://www.state.gov/r/pa/ei/bgn/5314.htm; Lionel Beehner, *Timeline: U.S.-Iran Contacts*, COUNCIL ON FOREIGN RELATIONS (Mar. 9, 2007), http://www.cfr.org/iran/timeline-us-iran-contacts/p12806. Following the Iranian Hostage Crisis in 1979, on April 7, 1980, the United States broke diplomatic relations with Iran, and on April 24, 1981, the Swiss Government assumed representation of United States interests in Tehran. Due to poor relations between the two countries, instead of exchanging ambassadors Iran maintains an interests section at the Pakistani embassy in Washington, D.C., while the United States, since 1980, has maintained an interests section at the Swiss embassy in Tehran.

IV. POST NORMALIZATION OF CYBER WARFARE: U.S. CONSTITUTIONAL IMPACTS

While the creation of norms for the realm of cyber warfare is imperative, conflating cyber conflicts with the language of war poses dangers for the future of the Internet and how Americans everywhere use it. Following the passing of the Patriot Act, government agencies have expanded their ability to control the Internet and monitor computer use under the guise of the War on Terror.[123] Should the United States government officially announce the onset of a "Cyber War," the American public could quickly witness the militarization of the Internet, where traditional notions of freedom of information are displaced by national security concerns.[124]

Although there is no direct reference or declaration on rights to privacy in the United States Constitution, the American people have come to expect at the very least the right "to be secure in their persons, houses, papers, and effects against unreasonable search and seizure."[125] The framers of the Constitution intended the Fourth Amendment as a prohibition on law enforcement from gathering more information than is required, but unfortunately, the phrase "unreasonable" was never well defined, and its definition has become increasingly blurred by the normative idea of what level of privacy a person should expect with the technological advances of the last century.[126] For example, the Supreme Court ruled in *United States Telecommunications Association v. FCC* that the Fourth Amendment protects digits that convey context,[127] however Title II of the Patriot Act (Enhanced Surveillance Procedures) was passed in part to allow for the FBI to run packet-sniffing software to intercept email sent by a suspect.[128] The software can be configured

123. *See* Laurie Thomas Lee, *The USA Patriot Act and Telecommunications: Privacy Under Attack*, 29 RUTGERS COMPUTER & TECH. L.J. 371, 373-78 (2003); Sunya Kashan, *The USA Patriot Act: Impact on Freedoms and Civil Liberties*, 7 ESSAI 87, 88 (2010).

124. *See* William J. Lynn III, *The Pentagon's Cyberstrategy, One Year Later*, FOREIGN AFFAIRS (Sept. 28, 2011), http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later?page=show (referencing William J. Lynn III, Deputy Secretary of Defense, Remarks on the Department of Defense Cyber Strategy (July 14, 2011), *available at* www.defense.gov/speeches/speech.aspx?speechid=1593). Ninety percent of United States military voice and Internet communications travel over the same private networks that service private homes and businesses.

125. U.S. CONST. amend. IV.

126. Thomas Y. Davies, *The Supreme Court Giveth and the Supreme Court Taketh Away: The Century of Fourth Amendment "Search and Seizure" Doctrine*, 100 J. CRIM. L. & CRIMINOLOGY 933, 1020 (2010); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1006-07 (2010).

127. *United States Telecom Ass'n v. Fed. Commc'n Comm'n*, 227 F.3d 450 (D.C. Cir. 2010).

128. Stefanie Olsen, *Patriot Act Draws Privacy Concerns*, CNET (Oct. 26, 2001), http://news.cnet.com/2100-1023-275026.html. *See also* Tom Cohen, *Obama Approves Extension of Expiring Patriot Act Provisions*, CNN (May 27, 2011), http://articles

either to record the email content, which are arguable digits that convey a plethora of personal context.[129] Beyond allowing the FBI to intercept emails, Title II of the Patriot Act covers all aspects of the surveillance of suspected terrorists, those suspected of engaging in computer fraud or abuse, and agents of a foreign power who are engaged in clandestine activities.[130] Specifically, Title II authorizes government agencies to gather "foreign intelligence information" from both U.S. and non-U.S. citizens.[131] As Title II of the Patriot Act is still in effect and allows for a government agency to at-will monitor a person's e-mails, Congress could very well create another extension or strengthen the U.S Patriot Act that provide for heightened surveillance of electronic transmissions from personal computers.

Considering that hundreds of American computers were used unsuspectingly to wage the DDoS attacks that shut Estonia's government down for weeks,[132] the FBI and other agencies could feasibly argue that the risk of infected zombie computers within our nation's borders should grant the federal government access to monitor electronic transmissions in order to protect national security interests.[133] The domino effect this sort of precedent could cause is

---

.cnn.com/2011-05-27/politics/congress.patriot.act_1_lone-wolf-provision-patriot-act-provisions-fisa-court?_s=PM:POLITICS; David Kravets, *Patriot Act Turns 10, With No Signs of Retirement*, WIRED (Oct. 26, 2011), http://www.wired.com/threatlevel/2011/10/patriot-act-turns-ten/. Section 505 of the Patriot Act gives the government powers to acquire phone, banking, and other records via the power of a so-called "national security letter," which does not require a court warrant. National security letters, perhaps the most invasive facet of the law, are written demands from the FBI that compel Internet service providers, financial institutions, and others to hand over confidential records about their customers, such as subscriber information, phone numbers, and e-mail addresses, and arguably websites you have visited. They require no probable cause or judicial oversight and also contain a gag order, preventing the recipient of the letter from disclosing that the letter was ever issued. In addition, the "lone wolf" measure under Section 207 of the Patriot Act allows FISA court warrants for e-monitoring of non-U.S citizens, even without showing that the suspect is an agent of a foreign power or a terrorist. It has never been invoked, but the authority is retained. The provision has been extended through June 1, 2015.

129. Olsen, *supra* note 128.

130. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

131. *Id.*

132. Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all. Estonian officials reported that over a million computers were used during the 2007 DDoS attacks, including American computers. *See also* James Sterngold, *U.S. on Guard Against Computer Attacks*, SAN FRANCISCO CHRONICLE, June 24, 2007, at A4, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/06/24/MNGCDQKS241.DTL&ao=all.

133. Singel, *supra* note 69. Department of Homeland Security representative Jordana Siegel said botnets were imminent threats to national security. *See also* Ryan Singel, *NSA*

frightening: any American computer could be logged into and monitored for suspicion of being a zombie computer for a future DDoS attack. With that in mind, cyber warfare tactics and policy need to recognize that much of the American public, despite the ease millions place private information onto Facebook, still expect a level of privacy in the home and at work in this post-September 11 society. In respecting and honoring the rights of the American people, any resulting domestic cyber warfare policy needs to take privacy concerns into consideration.[134]

CONCLUSION

When the Law of Armed Conflict was first codified into the Geneva Convention, the Internet may as well have been the subject of a science fiction novel. Now the United States and the international community are faced with questions of how to apply nearly a century-old charter to a technology that allows the aggressor to hide behind a veil of anonymity. Despite this obstacle to enforcing the current Law of Armed Conflict, cyber warfare remains a serious threat that can no longer be swept under the proverbial rug. At the onset of the decade, cyber attacks, with their inherent anonymity and propensity to cause real transnational harms, pose one of the most serious and evasive asymmetric threats to the United States and all other members of the international community, along with terrorism and nuclear proliferation.[135] Under the current environment, international peace is threatened, unless the United States and other nations have the ability to respond in self-defense to cyber attacks without being restrained by outdated interpretations of international law governing the right to

---

Must Examine All Internet Traffic to Prevent Cyber Nine-Eleven, Top Spy Says, WIRED (Jan. 15, 2008), www.wired.com/threatlevel/2008/01/feds-must-exami; Lawrence Wright, *The Spymaster: Can Mike McConnell Fix America's Intelligence Community?*, NEW YORKER (Jan. 21, 2008), http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright. Though he later retracted his statement, one of the lead United States spies initially argued for monitoring all Internet traffic after the attacks on Estonia.

134. *Compare* IBOPE Zogby International, *What is Privacy? Poll Exposes Generational Divide on Expectations of Privacy, According to Zogby/Congressional Internet Caucus Advisory Committee Survey*, Jan. 31, 2007, http://www.zogby.com/news/2007/01/31/what-is-privacy-poll-exposes-generational-divide-on-expectations-of-privacy-according-to-zogbycongre/ (explaining in 2007, IBOPE Zogby found that over 80 percent of Americans polled were concerned about the security and privacy of their personal information on the Internet.) *with* Mary Madden & Aaron Smith, *Reputation Management and Social Media*, PEW RESEARCH CENTER (May 2010), http://www.pewInternet.org/Reports/2010/Reputation-Management/Summary-of-Findings.aspx. IBOPE Zogby's number is comparable with the 2010 Pew Research Center poll that found nearly 44 percent of adults 18-29 actively take steps to limit the amount of their personal information that is available online, while 71 percent of social network users actively changed their privacy settings to limit what is shared.

135. Symposium, *Cyber Threats to National Security*, CACI INTERNATIONAL (2010).

respond in self-defense with force. The global and open architecture of the Internet, while an environment necessary to encourage innovation, makes defending against cyber attacks an exceedingly onerous task for state actors; effective international cooperation and trust building are critical to successfully protecting both state and non-state actors on the Internet in the years to come.

Although state practice in the aftermath of cyber attacks suggests widespread condemnation, cyber warfare remains a legal gray zone. Recently, policy debates on the subject have yielded little consensus in the way of an agreement on how to address a cyber attack, or even at what level a cyber attack becomes an armed attack. In the absence of custom, bilateral treaty regimes may provide a basis for the regulation of cyber attacks in international law. The regional and bilateral treaty regimes pursued by the United States not only offer some form of recourse in the absence of a comprehensive multilateral treaty, but also begin setting the early stages of precedent, based on their effectiveness, for a future treaty regime. However, while establishing accepted international norms through bilateral treaties is useful, doing so does not provide governments a codified definition of cyber attack or written guidelines on how states should respond in the event of a foreign-state taking aggression against them over the Internet. Cyber attacks are by their very nature transnational; cyber weapons are often designed by authors in multiple countries to run through computer networks without respect of state borders in hopes of undermining a computer system on the other side of the globe. In turn, this global threat can only be effectively met by increased diplomatic relations between the United States and the international legal community working together to solidarize a new treaty regime for cyber attacks.