War of the Cyber World: The Law of Cyber Warfare

PHILLIP POOL*

Abstract

With the rapid advancement in communication technology, there has been an increase in computer-related attacks aimed at both the hardware and software of countries' computer systems. Some of these attacks are private actors working for their own goals, but other attacks are committed by nations seeking to exploit weaknesses in their adversaries' computer technology systems. Despite more frequent occurrences of these cyber attacks, the international community has yet to adopt a framework to govern the rules nations are to follow in this new arena of warfare. This comment describes the history of cyber warfare and the modern cyber weapons nations and private actors are utilizing in this new battlefield. This comment then describes the existing legal framework governing armed conflicts and its applicability to cyber warfare. Also discussed within this comment is how cyber espionage could play a role in shaping international law. Finally, this comment covers proposed ideas relating to what framework could govern cyber warfare and what that framework could substantively entail.

I. Introduction

With the advent of computers, and subsequently the networks that connected them, a new door was opened in the hallways of warfare. Now, not only are conventional military weapons guided, tracked, and targeted by computers, but the computer systems themselves have become weapons. Much like other facets of technology, these new cyber weapons have evolved rapidly, much quicker than the legal frameworks that govern armed conflicts. But this has not helped slow the pace at which attacks involving cyber weapons have taken place. In fact, even as this comment was being researched and written, another round of cyber attacks was launched, this time at the United States, and major news out-

* Phillip Pool is a student at the SMU Dedman School of Law. He would like to thank the men and women in the armed forces and government agencies for their diligence in safeguarding the technology that helps keep the modern world running—they keep watch of what most people do not know exists. Also, the author expresses his appreciation to Teri and Wes Pool for years of providing subscriptions to multiple news outlets that helped him discover this issue.

lets reported the discovery of large scale cyber espionage operations.[1] Due to the nature of cyber warfare, the frequency of such attacks is only going to increase, which is why nations must understand and clarify the appropriate legal frameworks that govern such weapons in international law.

This comment will discuss cyber warfare and the applicable legal regimes that may govern this area of law. The first portion will give a history of the technology that allowed cyber warfare to come into existence, while also describing common cyber weapons at play in the global theatre. Additionally, recent notable attacks will be described and used throughout the paper as examples of the difficulties inherent in applying a legal framework to such a modern and evolving type of warfare. Next, this comment will analyze various legal frameworks that cyber warfare may apply to, highlighting the difficulties each faces in governing cyber warfare. A brief mention will be given to the area known as cyber espionage and its legality in the international community. It should be noted that during the process of researching and writing this comment, developments in the geopolitical realm involving cyber espionage, specifically allegations that a Chinese cyber unit has been involved in numerous operations against large American corporations and other entities within the United States, necessitated a longer discussion of cyber espionage that led to the addition of some materials contained within that section. Nevertheless, most of this comment deals primarily with cyber warfare and its accompanying legal regime. Finally, the comment will conclude with a discussion of what, if any, international treaty could be formulated to govern the law of cyber warfare and the hurdles such a treaty would face given disparities in individual nations objectives and paradigms in relation to conducting and protecting against cyber warfare.

II. How Computers Became Weapons of War

A. Connectivity

The rise of cyber weapons traces its history back to the cold war. Because of the Soviet Union's perceived advantage in technology after the launch of Sputnik, the Advanced Research Projects Agency (ARPA) was founded by the Department of Defense in order to ensure the United States would maintain a competitive military edge with its communist rival in the fields of technology and science.[2] One of the findings that ARPA discovered was that, in the event of a nuclear attack on the United States, the communication network that was vital to transferring information would be wiped out, leaving the United States silent.[3]

In response to this danger, ARPA and its scientists developed the "distributed communication" paradigm for communications.[4] This paradigm meant that instead of relying on the hierarchal pathway communication transfers that had been used previously, such as telephone calls being transmitted to switchboards, ARPA developed a system whereby

1. Siobhan Gorman & Danny Yadro, *Bank Seeks U.S. Help on Iran Cyberattacks*, Wall St. J. (Jan. 16, 2013, 12:01 AM) http://online.wsj.com/article/SB10001424127887324734904578244302923178548.html.

2. Michael Gervais, *Cyber Attack and the Laws of War*, 30 Berkeley J. Int'l L., 525, 527 (2012).

3. *Id.* at 528.

4. *Id.* (citing Janet Abbate, Inventing the Internet 11 (Wiebe E. Bijker et al. eds., 2000)).

multiple nodes would do the transmitting, away from population centers.[5] These nodes had attached links to other nodes that ensured that if one node went down, the information, which traveled "packaged" in binary numbers (bits), would simply be diverted and reassembled at another node, ensuring that the message eventually arrived at its desired destination.[6] Because of the immense cost of the project ARPA was undertaking, the project leaders decided to have the remote projects share computing resources, making it a "network of networks," and to use civilian infrastructure that was already in place (which, as will be discussed later, led to many of the problems inherent in cyber warfare).[7] Because the computers were all linked together, a common computer language was created, known as the Transmission Control Protocol/Internet Protocol (TCP/IP), which is still the language computers communicate in to this day.[8] With this final piece, the Internet came into existence.

B. The Arsenal of a Digital Warrior

Almost as soon as there was an Internet, people were creating ways to sabotage or simply annoy other users with software. These more mundane hindrances gave rise to much more powerful and dangerous computer programs that exist in many nations' digital armories.

One of these programs is known as a Denial of Service program, which creates a digital assault on a network, resulting in a flood of requests to said network. This results in the networking slowing to a crawl or even being frozen altogether.[9] A distributed denial-of-service program is a more severe, complex version of a denial-of-service program. A distributed denial-of-service program uses multiple computers, ranging from several to thousands of "zombie" computers, to coordinate a massive attack on a single network, lasting as long as the attacker wishes it to.[10] This exponentially strengthens the effect of a standard denial-of-service attack at a very low cost, making it an effective and affordable attack choice for a cyber aggressor.[11] Another version of a denial-of-service attack is a permanent denial-of-service attack.[12] This denial-of-service attack is of sufficient severity and causes enough damage to the network it has targeted that the network is permanently brought down and the users must replace the hardware before accessing the network again.[13]

Malicious programming is a type of cyber weapon that allows a user to disrupt the normal computer functions of a computer or allow entry through the "back door" for a

5. *Id.*

6. *Id.*

7. *Id.* at 529; Cassandra M. Kirsch, *Science Fiction No More: Cyber Warfare*, 40 Denv. J. Int'l L. & Pol'y 620, 632 (2012).

8. Gervais, *supra* note 2, at 530.

9. Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. Nat'l Ass'n Admin. L. Judiciary 602, 611 (2011).

10. *Id.* at 612

11. *Id.*

12. Major Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. Rev., 121, 135 (2009).

13. *Id.*

user to then become in control of the machine.[14] A common form of malicious programming is a virus, which lays dormant in a computer until accessed by a user, which then can corrupt data or, because they are self-replicating, can consume so much memory on the computer that the computer itself no longer functions.[15] An upgraded version of a virus is what is known as a worm, which acts similar to a virus except that a worm uses information transfer systems to spread from computer to computer, making it a much more aggressive and pervasive weapon of malicious programming, which may even allow remote control of a computer.[16] An interesting development in malicious programming is polymorphic malicious programming. This type allows the malicious software to change its computer code each time that it replicates (which can be millions of times), allowing it to be undetected by detection software.[17] This is just one of many examples of how intricate and deceptive cyber weapons can be, making them difficult to catch and difficult to disable.

Another form of malicious programming is the logic bomb. This is a more advanced type of malicious programming. The logic bomb's key strength is that it may lay dormant for long periods of time until becoming activated.[18] This makes it much more likely that the damage done upon activation is more severe and widespread. The Trojan horse is another type of malicious software, which, as the name implies, uses deceit to gain a user's trust. It tricks a user into thinking that the program will actually perform some beneficial function but, in reality, the program allows unauthorized access and control of a computer's network and files.[19] This access also allows the attacker remote access to the computer, which enables the host computer to become a zombie computer for a distributed denial-of-service attack.[20]

An interesting weapon of the cyber warrior is digital manipulation. This takes place when an attacker alters an image or video to change the meaning of the image or video.[21] In fact, modern technology allows the manipulation of live video because video editing, which used to take an hour, now takes a sixtieth of a second.[22] Bolstering digital manipulation's usefulness, scientists at the Los Alamos laboratories created cloning of speech patterns that allows for a person's voice to become nearly identical to that of a desired speaker, which means the credibility of a documented video would be greatly enhanced.[23]

IP Spoofing is another tool that allows a hacker to create a web page that appears identical to a trusted web page online, which deceives the user into entering private information.[24] Upon the user interacting with this fraudulent web page, the hacker is allowed to

14. Raboin, *supra* note 9, at 612.

15. *Id.* at 612–613 (citing *Malware*, TECHTERMS.COM, http://www.techterms.com/definition/malware (last visited Nov. 4, 2013)).

16. *Id.* at 613–14.

17. Schaap, *supra* note 12, at 137.

18. Raboin, *supra* note 9, at 614.

19. *Id.* at 615.

20. *Id.*

21. Schaap, *supra* note 12, at 137.

22. *Id.* at 138.

23. *Id.* at 139.

24. Raboin, *supra* note 9, at 614–615 (citing *IP spoofing (IP address forgery or a host file hijack)*, SEARCH SECURITY.COM, http://searchsecurity.techtarget.com/definition/IP-spoofing (last visited Nov. 4, 2013)).

hijack the computer to gain access to sensitive network information or computer program functions, whichever they desire.[25]

The last weapon in the cyber arsenal this comment will discuss is the SQL injection. SQL is international coding that serves as the language for database management systems; hackers use this standard language to gain access to multiple databases by inserting predetermined queries that always result in either true or false answers.[26] By doing so, a hacker may obtain usernames and passwords within the database to conduct cyber espionage of sensitive documents or as a platform to launch other malicious cyber attacks such as logic bombs.[27]

All of these weapons are appealing to countries around the globe because they require only a computer, making their cost minimal when compared to that of traditional kinetic warfare. In fact, the Rand Corporation has noted that almost all states can afford cyber weapons because they are "extremely modest" in price.[28] They can also be launched from the comfort of a cyber operations war room instead of on another country's sovereign soil. It is no surprise that smaller, less wealthy nations see these weapons and tactics as a way to even the playing field against larger, more technologically advanced countries whose kinetic armies are much stronger than their own. And, as will be discussed below, the inability to know exactly who perpetrated a cyber-attack makes these weapons even more appealing.

C. Notable Instances of Cyber Attacks or Espionage

1. *Cyber Attacks*

Many nations around the globe are actively building and maintaining cyber warfare divisions within their traditional armed forces.[29] The United States created the 24th Air Force, which deals exclusively with cyber operations and warfare, and in 2005 China began incorporating offensive cyber warfare exercises in their cyber-operations training.[30] Russia has also stated that it utilizes cyber operations to act as a force multiplier of its more traditional, kinetic components of its armed forces.[31] Additionally, North Korea created Unit 121 specifically for cyber warfare operations and also tested its first logic bomb in 2007, which caused the United Nations Security Council to ban imports of mainframe computer and laptop sales to the country.[32] The reason that these countries, along with others across the globe, have sought to stay ahead of the game in the realm of cyber warfare is a result of the following incidents of either cyber espionage or cyber warfare.

25. *Id.*

26. Kirsch, *supra* note 7, at 626.

27. *Id.*

28. Schaap, *supra* note 12, at 134 (citing Kevin Coleman, *The Cyber Arms Race Has Begun*, CSOonline (Jan. 28, 2008), http://www.csoonline.com/article/216991/coleman-the-cyber-arms-race-has-begun).

29. *Id.* at 132 (citing Kevin Coleman, *China's Cyber Forces*, Defensetech, (May 8, 2008), http://defensetech.org/2008/05/08/chinas-cyber-forces/).

30. *Id.* at 132.

31. *Id.* at 133.

32. *Id.*

In 2007 Estonia was attacked by a cyber-warfare operation.[33] The attack was a distributed denial-of-service operation, which within hours led to the shutdown of the nation's largest banks, severed online access to the nation's newspapers, slowed web traffic to a crawl, and also shutdown phone lines used for emergency service operators.[34] This attack was likely the result of Estonia deciding to tear down a World War II era bronze statute of a Russian solider, which caused Russian "hacktivists" to retaliate by launching this massive distributed denial-of-service attack.[35] It was reported that the pro-Kremlin Russian group known as Nashi, which was founded by Vladmir Putin and is funded by the Russian Business Network, was responsible for the attacks on Estonia.[36]

Another incident of cyber attacks occurred in Georgia in 2008.[37] After Georgia had responded militarily to separatist actions in South Ossetia and Abkhazia, shortly thereafter a severe yet simple distributed denial-of-service attack was launched at Georgian networks, which crippled government websites and state media outlets.[38] Shortly after this cyber attack had occurred, Russian kinetic military forces launched offensives into the territorial integrity of Georgia.[39] Although the distributed denial-of-service attacks could not directly be traced back to Russia, their coinciding with Russian kinetic military offensives and the overall objective of the cyber attack lead some to believe that at least some degree of Russian state sponsorship was involved in the cyber attack.[40] Officially, the attacks were claimed to have been perpetrated by the Kremlin Kids, a hacktivist group from Russia with no official ties to the state.[41]

Another example of a cyber-attack being used in conjunction with a traditional kinetic military operation is the Israeli strike on a Syrian weapons facility.[42] The air strike succeeded in large part because Israeli cyber soldiers had infiltrated into the Syrian air defense network.[43] The Israelis used what is known as a semantic attack, meaning there was no damage done to the networks of the Syrian air defense network, but false information was uploaded to the network that made the computers operating it believe that the skies above Syria were clear, when, in reality, Israeli war planes were conducting an air strike on Syrian facilities.[44]

An example of an attack infiltrating a separate state network, as well as one whose intentions were not to cause destruction but to hedge against it, occurred in 2003.[45] Shortly before the United States began operations against Iraq, the United States infiltrated the

33. Scott J. Shackelford, *Estonia Three Years Later: A Progress Report on Combating Cyber Attacks*, 13 J. INTERNET L. 22, 22 (2010).

34. *Id.*; Gervais, *supra* note 2, at 539–540.

35. Gervais, *supra* note 2, at 539–540.

36. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber Attack*, 100 CALIF. L. REV. 817, 854 (2012).

37. Raboin, *supra* note 9, at 619.

38. *Id.*

39. *Id.* at 619–620.

40. *Id.* at 619.

41. Hathaway, *supra* note 36, at 831.

42. Alexander Melnitzky, *Defending America Against Chinese Cyber Espionage Through the Use of Active Defense*, 20 CARDOZO J. INT'L & COMP. L., 537, 542 (2012).

43. *Id.*

44. Hathaway, *supra* note 36, at 838.

45. *Id.* at 839.

Iraqi Defense Ministry email system.[46] The United States' goal was to contact Iraqi officers and inform them that the United States did not seek their destruction but only to depose their leader Sadaam Hussein.[47] The United States also told the officers what to do with their equipment and weapons and told the Iraqi officers to simply leave and order their subordinate enlisted men to do the same.[48] In large part, this operation worked; some coalition forces arrived in Iraq and found outposts that had been deserted and weapons left according to the email's instructions.[49] This was a unique operation that showed that cyber weapons could be used to save lives and limit more destructive, kinetic operations.

One of the most impressive and technically intricate examples of a cyber attack to date is the release of the Stuxnet worm. In 2010, a worm was released into the cyber world that was targeted at industrial control systems.[50] This worm managed to get into Siemens' network in Iran, which ran the centrifuge control system.[51] The worm had two parts; one was designed to force Iran's centrifuges to spin uncontrollably and the other part was designed to make it appear as if the centrifuges were operating normally.[52] The brilliance of Stuxnet was that, although it infected computers worldwide, it was designed to only become operational when it detected controllers that run configurations only for nuclear conductors—and even then it was designed to only deliver its payload when arriving at the Iranian nuclear program.[53] The worm allowed the users to upload information from the target, allowing the users to know what target they were dealing with and change how it operated.[54] Thus, when activated, the Stuxnet worm disabled the Iranian centrifuges and disabled a portion of the Iranian nuclear program.[55] It was unknown what countries were behind one of the most technologically advanced cyber attacks in the world until 2012, when it was reported that both the United States and Israel were behind the development and implementation of the worm.[56] What was impressive about Stuxnet was that it was an example of a cyber weapon that caused kinetic damage to Iranian nuclear reactors.[57] It did not only slow down a system network but caused real damage—the same as if a country had bombed the centrifuges. This was an impressive feat that grabbed the attention of the cyber community.

---

46. *Id.*

47. Gervais, *supra* note 2, at 574.

48. Hathaway, *supra* note 36, at 839.

49. *Id.*

50. Gervais, *supra* note 2, at 570.

51. Kirsch, *supra* note 7, at 628 (citing William J. Broad, et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan 16, 2011, at A1).

52. Gervais, *supra* note 2, at 570.

53. *Id.* at 570–71.

54. *Id.* at 570.

55. Ellen Nakashima & Joby Warrick, *Stuxnet was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST, June 1, 2012, http://articles.washingtonpost.com/2012-06-01/world/35459494_1_nuclear-program-stuxnet-senior-iranian-officials.

56. *Id.*

57. *See id.*

2. *Cyber Espionage*

Cyber attacks are when some damage or disruption occurs in a nation's network or systems, but cyber espionage's goal is to obtain data or state documents without being detected.[58] As will be discussed later, the applicability of certain laws of war to cyber espionage is debatable, but the ease of access and amount of data enabled to be stolen by cyber espionage is a stark reality.

Operation Titan Rain is an example of cyber espionage on a massive scale.[59] China used hackers to download the equivalent of ten terabytes worth of digital information over a period of time from non-classified sources from the Department of Defense.[60] To put this into perspective, this amount of information is the equivalent of the entire collection of data stored in the Library of Congress.[61]

Another instance of cyber espionage, Operation Moonlight Maze, was a Russian operation that consisted of hackers targeting the Department of Defense, NASA, Department of Energy, and certain military contractors.[62] The goal was not to damage any network but to steal file listings and observe what was in certain peoples' directories.[63] Richard Clark, a well-known security expert in the field of cyber security, likened this espionage to a pre-war reconnaissance to see where key weaknesses are in a system.[64] A similar incident occurred when spies were able to gain access to Lockheed Martin's networks and stole terabytes of information on the F-35 fighter aircraft being developed by the United States Air Force.[65] For such a breach to have occurred in the era of non-digital espionage, a spy would have had to have a large truck and hours alone in a secure facility in order to carry out such a plot.[66] Such is the nature of cyber espionage; it allows for more efficient spying with much less risk.

Another incident of cyber espionage took place in the Middle East at a U.S. military base.[67] A compromised hard drive was inserted into a laptop that had access to classified networks and files.[68] This breach in security allowed the cyber operator access to those classified and unclassified networks and gave that person a "digital beachhead" from which to transfer large amounts of data to servers under foreign control.[69]

Even as this paper was being written, a new spotlight was shown on the world of cyber attacks and espionage and what actually constitutes such an attack by international standards.[70] China's alleged state-sponsored hacking program by its military cyber command unit has raised the global community's awareness of the size of cyber espionage and the

58. Schaap, *supra* note 12, at 139–140.
59. Gervais, *supra* note 2, at 533.
60. *Id.*
61. *Id.*
62. Schaap, *supra* note 12, at 141.
63. *Id.*
64. *Id.* (citing Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 Eur. J. Int'l. L., 825, 841 (2001)).
65. Melnitzky, *supra* note 42, at 545.
66. *See id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. *Room for Debate: What is an Act of Cyberwar?*, N.Y. Times (Feb. 28, 2013), http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar (follow the "Read the Discussion" link).

large amounts of data that can be stolen in minimal time.[71] A large report compiled by a private U.S. security firm shows what the report alleges to have been a Chinese military group—which allegedly has stolen large amounts of information from Coca-Cola and other commercial entities in the past—has now taken interest in large energy companies with access to gas and oil fields in the United States.[72] Said military group, named Unit 61398, "has stolen technology blueprints, manufacturing processes, clinical trial results, pricing documents [and] negotiation strategies," among other proprietary information.[73] But what makes U.S. officials particularly concerned is that this alleged group located in Shanghai is now trying to gain the ability to manipulate critical infrastructure, such as power plants and other utilities.[74]

This report by the U.S. firm has sparked debate about whether such large-scale cyber espionage operations should be considered an act of war, specifically cyber war.[75] One industry expert believes that certain irregular forces, such as those who would use zombie computers or "botnets" to attack another country, should be made wholly illegal under a new international regime.[76] Additionally, this expert believes that in order for one country to conduct an attack using another country's networks, the attacking nation must obtain permission from the host country first.[77] Also voiced by this expert is the need for cooperation amongst countries in investigating an attack if one were to occur.[78] Another expert has voiced concern that, unless the critical infrastructure of a nation (water, finance, power, energy) is attacked, the blowback from escalating cyber espionage into cyber war may be too severe, and thus acts of mere cyber espionage should not be considered an act of cyber war.[79] This expert believes that cyber espionage should be dealt with as a trade war would be, with trade levers and sanctions, to make those responsible for cyber espionage responsible for their actions.[80] Yet another expert advocates for military use that would not need high-level clearance, such as the President of the United States, but only when critical infrastructure has been attacked.[81] Another concludes that an act of cyber war does not jeopardize a country's national security, in part because one cannot occupy another nation's capitol solely with cyber weapons (even if one can cause massive damage with them).[82]

---

71. David E. Sanger, *In Cyberspace, New Cold War*, N.Y. Times, Feb. 24, 2013, at A1.

72. David E. Sanger, David Barboza & Nichole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. Times, Feb. 18, 2013, at A1.

73. *Id.*

74. *Id.*

75. Jody R. Westby, *We Need New Rules For Cyberwar*, N.Y. Times (Mar. 1, 2013, 6:11 PM) *available at* http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/we-need-new-rules-of-engagment-for-cyberwar.

76. *Id.*

77. *Id.*

78. *Id.*

79. Anup Ghosh, *Trade War Versus Cyberwar*, N.Y. Times (Feb. 28, 2013) http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/trade-war-versus-cyberwar.

80. *Id.*

81. Candace Yu, *We Have an Antiquated Framework*, N.Y. Times (Feb. 28, 2013) http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/we-have-an-antiquated-framework-for-dealing-with-cyberthreats.

82. Martin Libicki, *It's a Decision, Not a Conclusion*, N.Y. Times (Feb. 28, 2013) http://www.nytimes.com/roomfordebate/2013/02/28/what-is-an-act-of-cyberwar/an-act-of-war-even-cyberwar-is-a-decision.

It is clear from these recent news stories that cyber espionage is going to be a new diplomatic as well as geopolitical issue for the United States and other developed countries. Given that the United States is a large exporter of high-technology products, protecting the intellectual property of corporations and other critical information state agencies hold will be a topic in diplomatic discussions between China and the United States. This is a developing issue that will likely receive more attention in the coming months and beyond.

III. Considerations of the Applicable Legal Regimes of Cyber Warfare

Now that readers have a sense of how cyber warfare became a reality and what types of weapons are being utilized in today's digital battlefield, the next step must be to analyze the applicable legal regimes relating to war and the difficulties faced in applying these regimes to cyber warfare.

A. Defining Terms is an Obstacle

Because cyber warfare has only come into existence in recent years, different nations have different definitions for similar terms, if they even have a definition at all.[83] Even within a nation, because this concept of cyber warfare is so new, government agencies differ in their definitions of certain terms. For example, the United States Department of Defense defines cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[84] But the 2001 Congressional Research Service Report defined cyberspace as the "total inter-connectedness of human beings through computers and telecommunication without regard to physical geography."[85] Additionally, the National Military Strategy for Cyberspace Operations has yet another definition of cyberspace: a "domain characterized by the use of computers and other electronic devices to store, modify, and exchange data via networked systems and associated physical infrastructures."[86]

It should be noted that this multiplicity of definitions goes toward defining cyber *space*, not cyber *warfare*, a much more controversial subject that must find common terminology if a treaty or other international legal framework is to ever be constructed.[87] Clarke, the above mentioned cyber security expert, defines a cyber attack as "actions by a nation-state to penetrate another nation's computer or networks for the purposes of causing damage or disruption."[88] Some scholars have criticized this definition because it does not distinguish between cyber crime, cyber attack, or cyber war and also does not mention non-state actors (who frequently are perpetrators of cyber attacks).[89] The Joint Chiefs of Staff have

83. Hathaway, *supra* note 36, at 818, 823–825.
84. Schaap, *supra* note 12, at 125.
85. *Id.* at 126.
86. *Id.*
87. Hathaway, *supra* note 36, at 823.
88. *Id.* at 823 (citing Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It 6 (2010).
89. Hathaway, *supra* note 36, at 823–24.

also put forth a military definition for cyber attack, stating a cyber attack is a "hostile act using computer or related networks or . . . systems, assets, or functions."[90]

Differences between states in defining an armed attack play a key role in the difficulties of establishing a legal framework.[91] The Shanghai Cooperation is an agreement signed by Russia, China, and other central Asian countries that defines cyber warfare more expansively than the United States because included within the context of cyber warfare is "information war," meaning a "mass psychological brainwashing to destabilize society and state, as well as to force the state to take decisions in the interest of an opposing party."[92] Western democracies are concerned with this inclusion of information war in the Shanghai Cooperation's definition of cyber warfare because the political stability wording could be used to justify censoring dissident political speech online.[93] Interestingly, Russia has stated that it will consider any information warfare against it or its military as a military phase of a conflict.[94] Another definition that has been composed by a group of scholars to solve some of the legal applicability problems that will be discussed below describes a cyber attack as "any action taken to undermine the functions of a computer network for a political or national security purpose."[95] This definition will be discussed in relation to other issues concerning applicable law throughout the following portions of this article.

B. Jus Ad Bellum

The law of armed conflict governs military actions between states during a time of an ongoing armed conflict.[96] Key to the analysis of cyber warfare is Article 51 of the U.N. Charter, which states "[n]othing in the present charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs."[97] Herein lies a large part of why Jus Ad Bellum presents difficulties in governing cyber warfare; when is a cyber attack considered an armed attack under Article 51?

1. *An Armed Attack That Is Attributable*

One must perform an analysis of what force means in order to place cyber warfare within this framework. Article 2(4) of the U.N. Charter prohibits the threat or use of force against another state.[98] In *Armed Activities in Territory of the Congo*, the International Court of Justice ("ICJ") said that magnitude and duration of a state's actions are factors to be used in analyzing whether force was used against another state.[99] But this case did not contemplate the subtleties inherent in cyber operations. Another way to analyze force is

90. *Id.* at 824.

91. Kirsch, *supra* note 7, at 641.

92. Hathaway, *supra* note 36, at 825 (quoting Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, Dec. 2, 2008, Annex 1, at 209 [hereinafter SCO Agreement]).

93. *Id.*

94. Schaap, *supra* note 12, at 124.

95. Hathaway, *supra* note 36, at 826.

96. Kirsch, *supra* note 7, at 630.

97. U.N. Charter, art. 51, para. 1.

98. U.N. Charter, art. 2, para. 4.

99. *Cases Concerning Armed Activities on the Territory of the Congo* (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 165 (Dec. 19).

to look at delivery, meaning to look at the vehicle that the force stems from, such as a virus, worm, or denial-of-service attack.[100] One proposal has been to simply impute strict liability on any states executing cyber-attacks; but some have criticized this approach as too lenient because it allows self-defense measures for less severe offenses, such as a disruption in website access for a short period of time.[101] Another approach is the target-based approach, which looks to the target of the cyber-attack in order to decide if an armed attack occurred.[102] Some suggest that this approach is also too lenient in allowing self-defense because a critical structure need only be targeted before force could be applied in response.[103] One additional way of looking at whether force and, through that, an armed attack had occurred against a victim-state is the effects-based approach.[104] This approach looks at the direct effect the cyber attack had on the victim-state, but the problem some see in this approach is that cyber attacks do not usually *directly* cause damage.[105] Cyber attacks may cause harm through indirect means, such as someone dying as a result of a phone line being disconnected to an emergency call center due to a distributed denial-of-service attack.[106]

One proposal to the problem of deciding whether an armed attack has occurred is proposed by Michael Schmitt, who offers a modified approach to the effects-based test, called the consequences approach.[107] It uses several factors to analyze whether an armed attack has occurred: (1) severity: type or scale of the harm caused by the attack; (2) immediacy: how quickly harm materializes after the cyber attack has been launched; (3) directness: the length of the causal chain between attack and the harm ensuing from said attack; (4) invasiveness: the degree to which the attack penetrates the victim state's territory; (5) measurability: the degree of harm resulting from the attack that can be quantified; and (6) presumptive legitimacy: the weight given to the fact that, in the field of cyber activities as a whole, attacks constituting an armed attack are the exception rather than the rule.[108] This approach allows for a case-by-case analysis that takes into consideration the uniqueness of the damage done by cyber weapons, while recognizing that such weapons usually do not amount to an armed attack. To understand Schmitt's proposed framework, the Estonian attack can be used as an example. In the Estonian attack, the severity would not have risen to the level of a use of force because the damage was more an inconvenience than anything else, the consequences were immediate, there was no measurable damage or suffering, and the attack was intrusive and carried a presumption that it was illegitimate.[109]

Daniel Silver, the former General Counsel of the CIA, says that the severity of the cyber-attack is the critical question when determining if an armed attack has occurred and that an armed response in self-defense could only be done if the consequences from the attack were *foreseeable* to the aggressor when he launched the cyber attack.[110]

100. Gervais, *supra* note 2, at 538. .
101. *Id.*
102. Hathaway, *supra* note 36, at 845.
103. *Id.* at 846–47.
104. Gervais, *supra* note 2, at 538–39; Hathaway, *supra* note 36, at 847.
105. Gervais, *supra* note 2, at 539.
106. *Id.*
107. Hathaway, *supra* note 36, at 847.
108. *Id.*
109. Gervais, *supra* note 2, at 540.
110. Hathaway, *supra* note 36, at 848.

It should be noted that before a state can use force in self-defense, the state must be able to attribute the armed attack against its territory to another state. The ICJ addressed this issue in its *Nicaragua* case, saying that the armed attack would be judged under the "scale and effects" test. This means that if the armed attack, even if carried out by irregular forces, would amount to an armed attack if carried out by regular military personnel, then the state who conducted those irregulars would be liable.[111] Also, the court in *Nicaragua* stated that if a state has "effective control" of the non-state actors who carried out the attack, that state will be held accountable for the attack.[112] But the International Tribunal for Former Yugoslavia stated a lower standard, saying that "overall control" was all that was necessary in order for state responsibility to be imputed.[113] This difference in standards could play a role in cyber warfare; for example, the Russian Business Network that was involved in the Estonia attacks has many powerful military and political elite who are members, which could be used to impute responsibility onto Russia itself.[114] Some argue that there can be no attribution of conduct on the Internet because of the "placelessness" inherent on the web; thus, there is no state sovereignty on the web.[115] One author has refuted this proposition because the Internet is man-made and thus political in nature, meaning that people consciously shape the Internet and thus can regulate and control it.[116] This author uses the example of China regulating its ISP for subversive material that, if detected, instead of allowing a user to access the subversive-content, sends the user to a state-approved clone of the site.[117]

But attribution is incredibly difficult in the realm of cyber warfare due to the nature of the weapons and tactics used. As mentioned above, states or non-state parties can employ zombie computers all over the world to carry out a specific attack, leaving the victim country little opportunity to discover who was operating behind the mask of the zombie computers around the globe. For example, the "Ghostnet" hacker organization that was located in China had infiltrated thousands of computers worldwide, from India to New York to London.[118] Even though authorities in these respective countries knew that the hackers were located in China, they could not ascertain whether these Chinese computers were merely zombie computers used to throw off the scent of the real perpetrators' location or the real computers of the perpetrators themselves.[119] If, however, a state ever does conclude and can prove the attribution of a cyber attack, the question remains whether, if the actors are non-state actors, the host state is held accountable. The United Nation Security Council's Resolution 1368, passed shortly after the September 11, 2001, attacks against the United States, states that nations that knowingly harbor perpetrators of the

111. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 195 (June 27).

112. Gervais, *supra* note 2, at 547 (citing *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 202 (June 27)).

113. *Id.*

114. *Id.* at 548.

115. Melnitzsky, *supra* note 42, at 557 – 58.

116. *Id.* at 559.

117. *Id.*

118. Hathaway, *supra* note 36, at 847.

119. *Id.*

September 11th attacks would be held responsible for their actions, which could be applicable to non-state actors perpetrating cyber attacks.[120]

One note concerning cyber espionage should be mentioned; under international law, cyber espionage, which at its heart is information gathering, is not illegal under international law and thus could not be considered an armed attack for the purposes of self-defense. But cyber espionage is illegal under most nations' domestic laws.[121] One scholar argues that a spy plane may be shot down in the name of self-defense because of the plane's ability to launch a kinetic attack and that because with a few key strokes, a cyber warrior can transform an information gathering operation into an actual cyber attack, this merits cyber espionage being considered—at least in some circumstances—an armed attack.[122] Using the effects-based approach, the syllogism is explained as follows: if a continual cyber attack, such as a distributed denial-of-service attack, were launched and led to economic damage to a country, this would likely be ruled a cyber attack. Thus, if cyber espionage, which is occurring at an unprecedented scale in the technological age, does the same economic harm (estimated at one trillion dollars in 2008 in the United States), then it also should be considered a cyber attack.[123] If this theory were unpersuasive, then the theory of preventative war could be used to justify allowing some instances of cyber espionage to be considered an armed attack. But the main problem with this paradigm is that the most beneficial aspect of preventative war (loss of life in preventing potential conflicts) does not exist with cyber espionage.[124]

2. *Necessity and Proportionality*

Even if a cyber attack is launched and the aggressor state or non-state actors are identified, the response in self-defense must follow the international rules of necessity and proportionality. These rules stem from Article 2(4) of the United Nations charter, as well as Article 51(5)(b) and Article 57.[125] Article 57 states a country should "[t]ake all feasible precautions in the choice of means and method 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."[126] This addresses proportionality and could be problematic with cyber warfare because, as explained above, the civilian and military worlds share many of the networks that they use on a day-to-day basis. Ninety-five percent of military and 90 percent of major corporate transfers occur on civilian networks, which could lead to incidental loss of life of civilians—depending on the severity, target, and duration of the cyber attack.[127] This is why the language of Article 51(5)(b) bans attacks on military targets if they "may be expected to cause incidental loss of civilian life, injury to civilians, damage to

120. *See* Gervais, *supra* note 2, at 549 (citing S.C. Res. 1368, ¶ 3, U.N. Doc. S/RES/1368 (Sept. 12, 2001)).

121. Melnitzky, *supra* note 42, at 564.

122. *Id.* at 565.

123. *Id.* at 566.

124. *Id.* at 568–69.

125. Kirsch, *supra* note 7, at 630–32.

126. *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. 57(2)(a)(ii), Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol Additional I]).

127. Kirsch, *supra* note 7, at 632.

civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[128]

It should be noted that the proportionality and necessity elements of Jus Ad Bellum do not require that the act of self-defense be the same type of conduct or attack that was initiated by the aggressor.[129] This means that, for example, if a state was the victim of a cyber attack such as a distributed denial-of-service, the injured state, if all above described legal requirements were met, could then launch a kinetic attack, such as an air strike and destroy whatever facility the cyber attack was originating from.

C. Jus In Bello

1. *Necessity*

The following section will cover the issue of how nations would know what actions they could take within the framework of Jus In Bello—or the international laws governing military actions—given that an armed attack has occurred triggering a response in self-defense. The law of armed conflict stems from multiple sources and consists of four criteria: (1) Necessity, (2) Distinction, (3) Perfidy, and (4) Neutrality.[130] Article 52(2) of the Additional Protocol I to the Geneva Convention discusses military necessity, stating that a military attack is lawful only against "those objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization . . . offers a definite military advantage."[131] It can be difficult to know beforehand that the target destroyed created a military advantage, but a state could keep a record of what that state knew of the computer network that it had targeted in order to defend its actions, should they come under question from the international community.[132]

2. *Distinction*

Distinction is governed by the Additional Protocol II of the Geneva Convention, which states that "the civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations."[133] Additionally, Additional Protocol I to the Geneva Conventions indicates that civilians who take part in hostilities will be targetable "for such time as they take a direct part in hostilities."[134] This raises the possibility that a non-state actor, or "hacktivist," would be targetable while he or she is sitting at the computer launching the attack, but then, upon conclusion of that attack, would become an untargetable civilian, thus complicating when a non-state actor could be targeted.[135] Another problem that a state could face when attacked by a non-state actor is

128. *Id.* at 631–32 (citing Protocol Additional I, *supra* note 124, art. 51).
129. Schaap, *supra* note 12, at 148.
130. *Id.* at 149.
131. *Id.* at 150 (quoting Protocol Additional I, *supra* note 126, art. 52(2)).
132. Gervais, *supra* note 2, at 564.
133. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) art. 13, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Protocol Additional II].
134. Protocol Additional I, *supra* note 126, art. 51(3).
135. Gervais, *supra* note 2, at 566.

similar to that faced by a state targeting terrorists acting against that state; Additional Protocol I requires that a combatant needs "organized or state command responsibility," which many non-state hacktivists do not have.[136] To suggest that a state monitor their networks for these hacktivists brings questions of whether this would violate the freedom of the Internet and its facilitating of ideas, which would be of concern to western democracies but presumably not of concern to China and Russia.[137]

If a scientist or technical engineer were to be employed by a state to work on the computer code that would later be used in a cyber attack and if that civilian works on the code until the time shortly before it is launched as an attack, that civilian may be targetable under the principals of distinction due to his "continuous function [that] involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities."[138] But a state that employs civilian experts in the fields of science and technology could undermine the purposes of distinction by placing non-combatant civilians in roles that place them outside the realm of protection offered to them by jus in bello, especially because the Fourth Geneva Convention bans placing protected personnel on assignments directly related to military tasks.[139] Another problem associated with cyber warfare is that certain attacks, such a distributed denial-of-service attacks, potentially bring into the fray zombie computers that are owned by civilians who have no idea their machines are being used for such attacks. This act could be comparable to the use of "human shields," a known tactic in warfare that is prohibited under the Fourth Geneva Convention.[140]

So-called dual-use targets, such as air traffic control towers or entire communication networks, would be an area of interest to potential cyber attackers. The Eritrea-Ethiopia Claims Commission found that the bombardment of a power station that was to power a large naval base and port was legal under Additional Protocol I of the Addition to the Geneva Convention.[141] But to satisfy the requirement of necessity, the aggressor state must make sure that the target offers a distinct military objective; this means it would likely be illegal for a cyber aggressor to shut down an entire communication network of a large city whose military presence is minimal because the first objective would be civilian morale, which is not a legitimate military objective.[142] Thus, the intent of the attack is key to determining whether it meets the requirements of distinction; to undermine political support for certain figures or acts may be an unlawful attack but to undermine the military is likely lawful.[143]

One of the biggest advantages of a cyber attack as opposed to a more traditional kinetic attack, is that with a cyber attack, a state can shut down a radar dish that is being employed by the enemy state, whereas with a kinetic attack, the state would need to destroy the

136. *Id.*

137. *Id.* at 566–67.

138. Hathaway, *supra* note 36, at 853 (quoting NILS. MELZER, INT'L COMM'N OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INT'L HUMANITARIAN LAW 34 (2009)).

139. *Id.* at 854; Gervais, *supra* note 2, at 567 (quoting Geneva Convention Relative to the Protection of Civilian Persons in Time of War art. 40, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287).

140. Gervais, *supra* note 2, at 567.

141. Schaap, *supra* note 12, at 157.

142. *Id.*

143. Gervais, *supra* note 2, at 569.

radar dish with a missile or other explosive. This first scenario means that the scientist or technician operating the radar dish has a much less likely chance of being killed in the attack.[144] The downside of a cyber attack in this regard is that in order to assure that the self-defense response or attack a state is about to execute is legal, the state must have done extensive intelligence gathering to make sure that the system the state is going to strike does not allow for the attack to spill into the civilian network, causing more damage than was originally planned.[145] Stuxnet is an example of a cyber attack that was built around a single objective and implemented to only attack that objective, which can be ascertained by the fact that, although it infected thousands of computer operating systems worldwide, it only damaged the system that it was intended to damage and nothing else.[146] In order to keep unsubstantiated claims from arising from a cyber attack, it has been suggested that the burden of proof remain with the victim state to show that the attack launched upon it was indiscriminate based on what the military objective was behind the attack.[147]

3. *Perfidious Conduct*

Another rule of jus in bello is the ban on perfidious conduct, which is in place to facilitate a short period of violence and a quick restoration of peace.[148] The Hague Convention IV, Article 23(b) states that "to kill or wound treacherously individuals belonging to the hostile nation or army," is against the laws of war.[149] Further, Additional Protocol I, Article 37(1) states, "it is prohibited to kill, injure, or capture an adversary by resort to perfidy," and "acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable to armed conflict, with intent to betray that confidence, shall constitute perfidy."[150] An example of this behavior in traditional war would be a combatant raising the white flag, and then when his enemies approach him, he uses violence against them.[151] In the cyber warfare context, an act of perfidy could be considered when analyzing the Georgian attack. The Kremlin Kids used computers within Georgia to attack networks of the international banking community through a distributed denial-of-service attack, which led the banking security operators to believe the access came from Georgian computers, even though no one in Georgia was actually trying to harm or disrupt the banking network.[152] Another way perfidy could be demonstrated in cyber warfare is for a state to entice a third-party state to attack the aggressor state's enemy (instead of international banks), which could lead to more problematic issues involving diplomacy and other international affairs due to the involvement of a third-party country.[153]

144. *Id.* at 569–70.

145. *See* Katharine Hinkle, Note, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE 11, 18 (2011).

146. Gervais, *supra* note 2, at 571.

147. *Id.* at 573.

148. Schaap, *supra* note 12, at 151.

149. *Id.* (quoting Convention Respecting the Laws and Customs of War on Land, and its Annex: Regulation Concerning the Laws and Customs of War on Land art. 37(b), Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631).

150. Schapp, *supra* note 12, at 152 (quoting Protocol Additional I, *supra* note 126, art. 52(2)).

151. David Rhode, *Perfidy and Treachery*, CRIMES OF WAR, http://www.crimesofwar.org/a-z-guide/perfidy-and-treachery/ (last visited Nov. 4, 2013).

152. Gervais, *supra* note 2, at 574–75.

153. *Id.* at 575.

4. *Neutrality*

The aspect of neutrality is described in the Hague Conventions, specifically Hague Convention V, and states the rights of neutral states and their requirement to not become involved in an armed conflict, as well as belligerents' requirements to respect the inviolability of said neutral states.[154] A neutral state may stay neutral permanently, such as Switzerland, or may choose which armed conflicts it wishes to maintain its neutrality for.[155] Interestingly, the Hague Conventions allow a neutral state to allow belligerents access to their telephone lines for communication purposes but when dealing with cyber attacks (which are carried through those communication networks), this portion of the Hague Conventions may need revising if a state is to maintain neutrality and still allow belligerents access to its telephone networks.[156]

There is debate amongst legal scholars and states as to the liability of a neutral state when dealing with a cyber attack that originated, albeit unintentionally, from within its borders (such as zombie computers accessed via a worm and used for a distributed denial-of-service attack). Some argue that because of the packet switching system of electronic information that is the foundation of transmissions, and its subsequent unpredictable pathways that information will take to reach its destination, no one can predict the pathways that a cyber attack could follow on its way to its target.[157] Thus, these advocates contend, the servers that are used to transmit the attack are not targetable.[158] Others contend that if a state is either unable or unwilling to stop an unlawful cyber attack coming from its nation, then the servers or equipment enabling the attack are targetable themselves, irrespective of the home country's declared neutrality.[159] An intent-based strategy, which would state that if a state unintentionally facilitates a cyber attack then it would not be held liable, could help alleviate this problem. But what the term "unintentionally" means would have to be clarified in relation to the "unable or unwilling" concern of victim states.[160]

D. COUNTERMEASURES

In the realm of cyber warfare, there are many actions that states and non-state actors can take that will not qualify as an armed conflict under current international law of jus ad bellum but still violate Article 2(4)'s prohibition against the use of force.[161] This means that the victim state could not respond to such a low-level attack with an action in self-defense under Article 51 of the United Nations charter.[162] So what could a state that was targeted by such an attack do?

154. *Id.* at 576.
155. Hathaway, *supra* note 36, at 855 (citing George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L., 1079, 1141–42 (2000) (discussing neutrality and information warfare)).
156. Gervais, *supra* note 2, at 576.
157. *Id.* at 576–77.
158. *Id.* at 577.
159. Hathaway, *supra* note 36, at 855.
160. Gervais, *supra* note 2, at 576-77.
161. *Id.* at 554.
162. *Id.*

There a multiple options for a victim state in this situation. One option is for the victim state to use retorsions, which are unfriendly but lawful actions that a state perpetrates against another state, a common one being a victim state denying access from the aggressor state's servers.[163] This option can become cumbersome when a state is dealing with zombie computers located in many countries across the globe because no state can realistically shut down its servers to multiple countries around the globe.[164] Countermeasures, which are "a form of unilateral, non-forcible self-help employed by an injured state in response to internationally wrongful acts by another state," are a more aggressive approach.[165] Countermeasures are meant to force the aggressor state to come into compliance with its international obligations to not use force on another state and are not meant for retributive purposes or to punish.[166] The legal source of these countermeasures comes from the International Law Commission Draft Articles on Responsibility on States for Internationally Wrongful Acts, which allows a state to cease legal obligations towards the aggressor state to bring an end to the illegal acts or to win reparations due to the act.[167] In order for a victim state to lawfully use countermeasures against an aggressor state, it must first call on the aggressor to cease its illegal forceful actions and/or make reparations.[168] If this first attempt is unsuccessful, the victim state can then utilize a countermeasure known as an active defense (for example, launching a distributed denial-of-service attack at the aggressor state in order to shut down the server or systems that are allowing the attack to occur).[169] Of course, in order for a state to utilize these active defenses against another state, there must have been an international wrongful act directed towards the victim state and it must be attributable to the aggressor state.[170] If the state is responding to a series of attacks, then the state may be able to go beyond the proportionate response to one attack by treating the cumulative damage of the series of attacks as the threshold for its response.[171]

Because of the characteristics of a cyber attack, some argue that the proportional requirement is easily met because a state would use a cyber attack in response to whatever action was launched against it.[172] Such arguments further go on to say that the chance of collateral damage done by a cyber attack going past its intended target are lessened from the fact that nations, which have a duty to protect their own civilians from anticipated attacks, are "vigorously trying to prevent" viruses spreading from beyond their target, making the chance of such collateral damage minute.[173] This means that there would be little unnecessary suffering after such a response was launched. But some believe that countermeasures could be more dangerous when applied to the cyber warfare context. The warning requirement of Article 52, requiring a state to request from the aggressor state to desist from its activity, can be overruled by language in Article 52(2), which states

163. *Id.* at 555.
164. *See id.* at 556.
165. Hinkle, *supra* note 145, at 14.
166. *Id.* at 15.
167. *Id.* at 14.
168. Gervais, *supra* note 2, at 555.
169. *Id.* at 556.
170. Hinkle, *supra* note 145, at 16.
171. Gervais, *supra* note 2, at 557.
172. Melnitzky, *supra* note 42, at 561.
173. *Id.* at 562.

"[n]otwithstanding paragraph 1(b), the injured state may take such urgent countermeasures as are necessary to preserve its rights."[174] This provision is to enable a victim state to respond against its aggressor without giving the aggressor state time to "immunize itself from countermeasures," which frustrates the purpose of notification.[175] Also, the International Court of Justice allows for emergency scenarios that permit an injured state to have a level of discretion in determining whether, and to what extent, countermeasures would be utilized by it.[176] This "emergency scenario" doctrine, when applied to cyber attacks, could become frequently utilized by victim states because a cyber attack, by its nature, is unexpected and has the ability to cause mass damage if it inflicts harm beyond its objective, as described above.[177]

It has been said that active defenses, because of the well-established law of reciprocity, would be unlikely to be considered unlawful force and would have a low chance of unnecessary suffering from the aggressor country. The U.S. Department of Defense stated, "[i[f the cyber provocation is not considered to be an armed attack, a similar response will also presumably not be considered to be an armed attack."[178] Because the active defenses would attack other computers, the principal of distinction is also considered to be met with relative ease as compared to other forms of reciprocity.[179] But one must remember that, because the active defense would be in response to an unexpected cyber-attack against the victim state, the response from the aggrieved state could cause unanticipated collateral damage to the aggressor state. This is because, as stated above, unless substantial research and planning is done in order to execute a cyber-attack, the chances for that attack spreading to other civilian networks and systems are increased.[180] For example, the attacks on Estonia resulted in zero civilian causalities themselves, but if Estonia had launched a countermeasure that disabled systems in Russia, those countermeasures—due to the lack of planning and preparation—could spread past the intended target networks and lead to injuries of civilians, which would be a worse consequence than the original attack such countermeasures were in response to.[181] These consequences would only be exacerbated by the fact that when a smaller country, such as Estonia, launches a countermeasure against a much larger country, like Russia, the chance that said attack would spread past the intended target is greater because the larger country has more networks and systems that could potentially be affected.[182]

174. U.N. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, *in* Report of the Int'l Law Comm'n art. 52(3), 53d sess, Apr. 23–June 1 & July 2–Aug. 10, 2001, U.N. Doc. A/56/10; GAOR, 56th Sess., Supp. No. 10 (2001) [hereinafter Draft Articles]; Hinkle, *supra* note 145, at 18.

175. *Id.* (quoting Draft Articles, *supra* note 174, art. 52, cmt. ¶ 6).

176. *Id.* (citing OMER YOUSIF ELAGAB, THE LEGALITY OF NON-FORCIBLE COUNTER-MEASURES IN INTERNATIONAL LAW 50 (1988)).

177. *See* Jeremy Richmond, Note, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842, 846–47 (2012).

178. Hinkle, *supra* note 145, at 19–20 (quoting Office of Gen. Counsel, Dept. of Def., An Assessment of International Legal Issues In Information Operations 19 (1999).

179. Melnitzky, *supra* note 42, at 561.

180. *See* Hinkle, *supra* note 145, at 20–21.

181. *Id.*

182. *Id.*

IV. Treaties and Other Steps Towards a Legal Framework

As seen above, there are many characteristics that make choosing an existing legal framework under which to govern cyber warfare problematic. As will be seen below, several treaties and agreements already in existence could apply to certain aspects of cyber warfare, but these are piecemeal and do not apply to all parts of cyber warfare. This section will analyze some existing accords, both bilateral and multilateral, and discuss what steps have already been taken to begin addressing the regulation of international cyber warfare.

A. Applicable Existing Treaties

Several international treaties exist that cover certain aspects of international cyber warfare, although none cover this area of warfare entirely. Telecommunication law, which is derived from the International Telecommunication Convention, could play a role in international cyber warfare.[183] Radio regulations standardize the operation of telecommunication networks and services. Regulation 18 of the Convention provides that no country may transmit false or misleading signals, which refers not to the information contained in the message but to the transmitter itself.[184] Also, Article 19(2) of the Telecommunication Convention allows for a state to cut off private telecommunications that are contrary to the home state's laws.[185] It should be noted that these provisions from the Telecommunications Convention have typically been suspended between two belligerents involved in an armed conflict.[186]

There have been comparisons of cyber space to outer space, but some have noted there is a key difference between the two stemming from what is readily observable.[187] In outer space, no country can put nuclear weapons into celestial orbit, and this rule is enforceable because, if a nation were to put a nuclear weapon into space, many countries would soon be aware of this through monitoring equipment; in cyber warfare, it is only the effects of the attack that are observable.[188] Also of note concerning space is that Article IX of the Outer Space Treaty makes it illegal for a country to interfere with the exploration of outer space, but a nation may destroy a satellite in orbit if that satellite is being used for military purposes.[189] This raises issues of dual-use objectives because, in the United States, 60 percent of military communications through satellite are provided by private entities.[190] Nonetheless, the existing outer space treaties do not seem to practically apply to the issues of cyber warfare.[191]

183. Schaap, *supra* note 12, at 164.
184. *Id.* at 165–66 (citing Lawrence T. Greenberg, Seymour E. Goodman & Kevin J. Soo Hoo, Information Warfare and International Law, 41, n.41 (1998)).
185. *Id.* at 165 (citing International Telecommunications Convention, Nairobi, Nov. 6, 1982, 32 U.S.T. 3821).
186. *Id.* at 166.
187. Raboin, *supra* note 9, at 625.
188. *Id.* at 626 (citing Scott J. Shackeford, *From Nuclear War to Net War, Analogizing Cyber Attacks in International Law*, 27 Berkeley J. Int'l L. 192, 220 (2009)).
189. Schaap, *supra* note 12, at 162.
190. *Id.*
191. *See id.*

International Aviation law, such as the Convention on International Civil Aviation, tangentially relates to cyber warfare. Annex 17 of this Convention prohibits the use of weapons against civil aircraft, but this same Convention's Article 89 suspends its applicability during wartime.[192] Additionally, the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Article I, prohibits interference with a plane's operating system if such interference would render the plane incapable of flight.[193] This treaty also prohibits disrupting or destroying the navigation facilities that allow for flight if said interference would endanger any aircraft in flight, which could have an effect on the targets that nations consider when planning a cyber attack.[194]

Another source of cyber regulation stems from the European Union. In 2001, the European Union created the European Union Council Convention on Cybercrime, which then adopted a Cybercrime Treaty, and although the treaty was created under the guidance of the European Union, it has been signed by forty-one nations, including the United States.[195] But this treaty governs only cybercrime, and it specifically does not apply to actions taken with authority from the respective governing nations, thus making it inapplicable to cyber warfare.[196] Nonetheless, this treaty shows that the global community is interested and willing to take action to address issues involving international regulation of cyberspace.[197]

B. Possible Courses of Action

Given the issues involving the scope and practicality of existing treaties and agreements, as well as the political barriers that exist between nations concerning issues of censorship, it is easy to see how formulating and adopting a treaty to govern cyber warfare is a challenge for the international community. This comment now turns to what countries are doing, and what can be done, to address regulating international cyber warfare.

As can been seen from this comment, the breadth and pace at which cyber warfare has developed shows that only an international solution can solve the problem of regulating such weapons. The United States Department of Defense has said that "cyberspace is a network of networks that includes thousands of ISPs [internet service providers] across the globe; no single state or organization can maintain effective cyber defenses on its own."[198] But because of political differences—notably between the United States, China, and Russia—concerning political censorship, bilateral efforts seem to be a more suitable route for the time being. The United States has signed a Memorandum of Understanding with India on the issue of cyber attacks and has added an extension to the existing Australia,

192. *Id.* at 167.

193. *Id.* at 168 (citing Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Sept. 23, 1971, 24 U.S.T. 564).

194. *Id.*

195. Raboin, *supra* note 9, at 633.

196. *Id.*

197. *Id.*

198. Hathaway, *supra* note 36, at 880 (quoting U.S. Dep't of Def., Department of Defense Strategy for Operating in Cyberspace 9 (2011)).

New Zealand, and United States Security Treaty.[199] This extension allows for cooperation between the United States and Australia to share information and technology with each other in the event of a large-scale cyber attack.[200]

Given the amount of cyber crime, cyber espionage, and other cyber operations that originate from Russia and China, some have mentioned that any treaty that lacks their membership as signatories would be *sine qua non* because without these two nations any gains in regulating cyber activity would be negated.[201] But there are other approaches that sidestep the Russia-China problem. One idea is to form bilateral partnerships with other nations, while also including the International Criminal Police Organization (INTERPOL) and other domestic police bodies, which would be helpful because many cyber attacks have a criminal component in their execution.[202] Another suggestion is to utilize the more than 250 Cyber Emergency Response Teams that exist in the United States and connect them with the NATO Cyber Emergency Response Team based in Estonia to create a Multinational Cyber Emergency Response Team, which would locate and attribute the source of cyber attacks through collaboration and pooling of resources and intelligence.[203]

There have been some positive developments on the international front concerning an international, multilateral treaty on cyber warfare. In July 2010, fifteen countries submitted recommendations to the United Nations Secretary General as "an initial step towards building an international framework for security and stability that these technologies require."[204] These steps included the following: (1) confidence building and exchange of national views on the use of cyber information technologies in conflict, (2) information exchange on national securities strategies and technologies and best practices, (3) further dialogue among countries, and (4) finding possibilities to elaborate common terms and definitions.[205] Importantly, the recommendations were put together by countries including the United States, Russia, and China, which is a significant step toward one day having an international treaty.[206] One author has suggested that the United States, specifically the President's administration, should release a white paper defining how it would address specific attacks because this would encourage Russia and China to do the same.[207] Whether China and Russia would actually release their own white papers is unclear, but such a move by the United States would at least show that one of the world's cyber powers is willing to use collaboration to address the issue of regulating cyber warfare.

Some scholars believe that, whatever the actual product turns out to be, there are certain steps that must be taken in order to pass an international treaty governing cyber

199. Kirsch, *supra* note 7, at 641 (citing Press Release, Dep't of Homeland Sec., United States and India Sign Cybersecurity Agreement (July 19 2011), *available at* http://www.dhs.gov/ynews/releases/20110719-us-india-cybersecurity-agreement.shtm).

200. *Id.* at 641–42.

201. *See id.* at 640.

202. Shackelford, *supra* note 33, at 27.

203. *Id.*

204. Hathaway, *supra* note 36, at 860 – 61 (quoting U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Foreword ¶¶ 3, 5, U.N. Doc. A/65/201 (July 30, 2010)).

205. *Id.*

206. *Id.*

207. Shackelford, *supra* note 33, at 27.

warfare. A preliminary step would be to, as stated above, agree on definitions for the terminology interwoven in the cyber warfare vernacular, such as cyber-attack and cyber space (a difficult step due to the political differences described elsewhere in this comment).[208] An example of this process is seen in the OECD Bribery Convention, which provides its signatories with a definition of bribery that the signatories incorporate in their own domestic national legislation governing bribery.[209] Even though cyber warfare is an international issue, domestic law may play an important part in its overall regulation. The United States has released a proposal called the National Strategy for Trusted Identities in Cyberspace (NSTIC).[210] This proposal seeks to establish an Identity Ecosystem, allowing Americans to obtain credentials from companies similar to an ATM card. NSTIC represents one of the first attempts for the United States to address the issue of anonymity on the Internet.[211]

V. Conclusion

Technology has enabled information systems to become ubiquitous in the daily life of hundreds of millions of people. From traffic lights to water utility systems and from nuclear power plants to city power grids, computers and the technology behind them have led to an interconnected world that allows for instant communications, breakthroughs in medical treatments, and many other beneficial consequences to the modern world. But these benefits and breakthroughs have come paired with serious dangers that the information age has created. In a world where a single computer can bring a portion of a city's infrastructure to a halt, the potential dangers of cyber warfare "can no longer be swept under the proverbial rug."[212] As more and more nations realize the crippling effects that cyber weapons can have on their target information systems, as well as their relatively cheap costs when compared to traditional kinetic weapons, such weapons will be used more often, not less. Computers and technology will only improve as time progresses, which is why the legal gray area of cyber warfare should be clarified in order to help nations understand and comply with international rules that will limit the potential harm that cyber weapons can have.

In order for an applicable legal regime to be crafted in some fashion, there must first be an agreement between nations about what constitutes a cyber attack. Western nations that value a freedom of exchange of ideas online should find common ground with more authoritarian nations who define a cyber attack to include an information war. Considering that these nations make up some of the most influential and militarily powerful countries in the world, not until a mutual definition has been established will progress toward an international framework to govern cyber warfare be seen.

Once a definition has been crafted for a cyber attack, there still remain other questions that need to be solved. One such question is how to determine if a cyber attack has occurred. The definition mentioned above by Michael Schmitt has received some notoriety; but there needs to be a consensus among nations so that there is a definitive answer to

208. Hathaway, *supra* note 36, at 881881 (citing SCO Agreement, *supra* note 92).
209. *Id.*
210. Melnitzky, *supra* note 42, at 548.
211. *Id.* at 548–49.
212. Kirsch, *supra* note 7, at 646.

when a cyber attack has occurred and how much (and what type of damage) must occur in order for it to be labeled as such. Furthermore, the difficulties arising with both the jus ad bellum and jus in bello frameworks—due to the difficult process of attribution involving a cyber attack and the unknown consequences that a cyber attack can have—seem to necessitate some new framework coming into existence, whether it be a treaty or some other codified document. Addressing the attribution problem will take international cooperation and possibly a network of some sort that allows nations to pool together their resources and portions of their databases in order to pinpoint to a certain extent where a cyber attack originated and which nation or nations were responsible for its perpetration.

When coupled with the threat of cyber espionage, the dangers are clear that, with technology becoming a more important part of nations' citizenry's daily lives, the pace at which the technology has developed has far surpassed the pace at which the public is aware of the potential risks involved in utilizing that technology in our most important infrastructures and utilities. If the international community is to avert serious loss of property and potential loss of life, there should be a governing framework to hold law-breaking nations accountable and help govern cyber weapons use. It cannot be forgotten that the Hague Conventions, Geneva Conventions, and U.N. Charter were crafted in a different era with vastly different weapons. It may well be time for the international community to address cyber warfare and the technology that it has spawned so that what has been such a boon to the modern world does not become its bane.