


10-15-2011

## Corresponding Evolution: International Law and the Emergence of Cyber Warfare

Bradley Raboin

Follow this and additional works at: <http://digitalcommons.pepperdine.edu/naalj>

 Part of the [Computer Law Commons](#), [International Law Commons](#), and the [Internet Law Commons](#)

---

### Recommended Citation

Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. Nat'l Ass'n Admin. L. Judiciary Iss. 2 (2011)

Available at: <http://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5>

This Comment is brought to you for free and open access by the School of Law at Pepperdine Digital Commons. It has been accepted for inclusion in Journal of the National Association of Administrative Law Judiciary by an authorized administrator of Pepperdine Digital Commons. For more information, please contact [Kevin.Miller3@pepperdine.edu](mailto:Kevin.Miller3@pepperdine.edu).

# Corresponding Evolution: International Law and the Emergence of Cyber Warfare

By Bradley Raboin

## TABLE OF CONTENTS

I. INTRODUCTION.....	603
II. THE EMERGENCE OF CYBER WARFARE.....	607
A. <i>Defining Cyber Warfare</i> .....	607
B. <i>The Weapons of Cyber Warfare</i> .....	609
1. Denial-of-Service.....	611
2. Malicious Programs.....	612
3. Logic Bombs.....	614
4. IP Spoofing.....	614
5. Trojan Horses.....	615
C. <i>Modern Proliferation: Instances of Cyber Warfare in Our Contemporary World</i> .....	616
1. Estonia.....	616
2. Georgia.....	619
3. Iran.....	621
III. CYBER WARFARE AND INTERNATIONAL LAW.....	624
A. <i>The Applicability of Current International Laws to Cyber Warfare</i> .....	624
B. <i>Inadequacies of Current International Laws</i> .....	640
1. Attribution Problem.....	640
2. Jurisdiction Problem.....	647
3. “Use of Force” Problem.....	653
IV. THE FUTURE OF CYBER WARFARE AND INTERNATIONAL LAW.....	658
A. <i>Evolution</i> .....	659
B. <i>Consistency</i> .....	661
C. <i>International Agreements</i> .....	662
V. CONCLUSION.....	666

## I. INTRODUCTION

Warfare has always been an evolving concept. Throughout history, it has constantly been shaped and altered by the exigencies of nations and the moral sentiments of the global community. Yet, the paramount force behind this continual military evolution is not economic, social, or moral; rather, the greatest controlling factor has been the ever-changing limitations of wartime technology. As United States Air Force Lieutenant-Colonel and Communications Officer Donald Ryan has observed, “[t]he history of war can be characterized as an imaginative use of technology to nullify the advantages of mass.”<sup>1</sup> For centuries, nations have searched for and sought ways to utilize technological advancements to overcome material deficiencies.<sup>2</sup> The recent advent of the information age, and the willingness of nations to utilize emerging computer technologies for military purposes, may have finally ended that search. Now, with merely a computer and an Internet connection, an entire nation’s infrastructure, both military and civilian, may be critically affected.<sup>3</sup>

---

<sup>1</sup> See Donald E. Ryan, Jr., *Implications of Information-Based Warfare*, JOINT FORCES QUARTERLY, Autumn/Winter 1994-95, at 114. As Ryan observed in his article, the entire development of historical warfare has coincided and evolved parallel to the technological developments that serve to make warfare possible in increasingly efficient ways. *Id.* Ryan continues by specifically noting the inherent relationship between technological development and the corresponding evolution of wartime methodologies and instruments: “[t]he introduction of the crossbow resulted in thicker armor. That, in turn, led to innovations such as the English longbow and gunpowder, to pierce armor.” *Id.*

<sup>2</sup> *Id.* Continuing with Ryan’s reasoning, nearly every military advancement in history has sought to overcome the power of numbers. Machine guns, tanks, and planes made the value of actual numerical infantry far less significant. In turn, missiles and bombs lessened the value of numerous guns, tanks, and planes. Finally, the modern development of nuclear weapons, unmanned aircraft, and intercontinental missile capacity has made one military weapon capable of more destruction than entire squadrons of conventional military personnel.

<sup>3</sup> See Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKLEY J. INT’L L. 192, 193-94 (2009). Shackelford notes that a professionally coordinated cyber-attack “could destroy a nation’s economy and deprive much of it’s population of basic services, including electricity, water, sanitation, and even police and fire protection . . . ” *Id.* Many commentators believe that a worst-case scenario cyber-attack could produce catastrophic effects equivalent to the destruction and devastation of nuclear

According to some commentators, the emergence of cyber warfare is more than just another evolutionary step in the development of wartime strategy and methodology; instead, they argue that it represents a fundamental transformation in the very nature of the concept of war itself.<sup>4</sup> The notion that cyber warfare will alter the inherent nature of war is ultimately rooted in the conceptual idea that cyber warfare does not merely change the weaponry of modern wars, but that it represents a radical shift in the nature of the wartime battlefield.<sup>5</sup> Whereas every historical evolution of warfare has occurred within the common sphere of the physical, tangible world, cyber warfare redefines the central wartime battlefield.<sup>6</sup> Yet, the consequences of actions within this new cyber warfare battlefield are unique because although they occur in the intangible domain of computer networks and information streams, the effects of the actions taken within that domain have very “real” effects in the physical world of our everyday reality.<sup>7</sup> It is in this new warfare realm, most commonly referred to as “cyberspace,” that

---

weaponry. See, e.g., *Doomsday Fears of Terror Cyber-Attacks*, BBC NEWS (October 11, 2001), <http://news.bbc.co.uk/2/hisience/nature/1593018.stm>.

<sup>4</sup> See e.g., John Arquilla & David Ronfeldt, *CyberWar is Coming!*, COMPARATIVE STRATEGY, Vol 12, No. 2, Spring, 1993, at 31, available at <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA485253>.

<sup>5</sup> See Natasha Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 296-97 (2008).

<sup>6</sup> See Arquilla, *supra* note 4, at 32. Arquilla and Ronfeldt argue that cyber warfare does more than change the way in which future battles will be fought on a mechanical level; rather, they conclude, “[t]he post-modern battlefield stands to be fundamentally altered by the information technology revolution, at both the strategic and tactical levels.” *Id.*

<sup>7</sup> Although cyberspace remains a conceptual location, it is also inherently reliant upon physical infrastructures and its effects are readily felt in the physical world—“[c]yberspace is a place, a battlefield, where individuals acting on their own or in concert with a country, nation-state, or terrorist organization may cause costly and devastating damage . . . .” Solce *supra* note 5, at 300. The real-world effects of cyberspace actions were evident in a test conducted by the Department of Energy’s Idaho National Laboratory in 2007. See James D. Zirin, *Abdicating on a ‘cyber czar’?* LA TIMES (Oct. 14, 2009), <http://articles.latimes.com/2009/oct/14/opinion/oe-zirin14>. In the experimental test, researchers were able to hack into a power plant’s central systems and “were able to cause [the] generator to shake, smoke, and shut down with a few keystrokes.” *Id.*

many believe the keys to the future of modern warfare lie.<sup>8</sup>

As states have hectically scurried to gain dominance over this newest form of military technology, they have also increasingly recognized the need for international limitations and controls on the use and dissemination of such potentially dangerous technology. The United States (“U.S.”), responding to the mass increases in threats to its own internal cyber-security<sup>9</sup>, has responded with the creation of various military and governmental cyber-security agencies<sup>10</sup> and most recently with proposed legislation directly addressing the critical importance of cyberspace security.<sup>11</sup>

---

<sup>8</sup> Dr. Lani Kauss, Director of the Air Force Cyberspace Task Force, observed in 2006, “[C]yberspace is neither a mission nor an operation . . . [it] is a strategic, operational, and tactical warfighting domain.” C. Todd Lopez, *Senior Leaders Discuss Fighting in Cyberspace*, INTERCOM, Nov. 2006, at 18–19, available at <http://public.afca.af.mil/shared/media/document/AFD-061220-041.pdf>.

<sup>9</sup> The increases in cyber originating attacks on the United States’ internal and governmental infrastructure has been alarmingly consistent; in 1994, the U.S. experienced only 250 reported cases of disruptive cyber-attacks against information networks. See Barry Kellman & Stephen Dycus, *International Security*, 42 INT’L LAW 799, 811 (2000). Only four years later, in 1998, that number had risen to nearly 6,000 and in 1999, the number of reported cyber attacks against U.S. government infrastructure had reached over 18,000. *Id.*

<sup>10</sup> The U.S. has created numerous agencies to deal with the emerging threats and military possibilities of cyber warfare; it has also issued several inter-governmental reports on the topic. A select few of these, and hardly an exhaustive list, follow: the July 1996 President’s Commission on Critical Infrastructure Protection (PCCIP), the 1998 Presidential Decision Directive No. 63 (PDD-63), the FBI INFRAGARD program, the 2001 Executive Order 13228 on Homeland Security, the 2001 USA Patriot Act, the 2002 National Strategy for Homeland Security, the Homeland Security Act of 2002, the 2002 Cyber Security Research and Development Act, the 2003 National Strategy to Secure Cyberspace, the 2004 National Cyber Alert System (NCAS), the 2006 creation of the 67th Network Warfare Wing of the Air Force, and the 2009 formation of the US Cyber Command and USCERT as well as the White House Cyberspace Policy Review. See generally Solce, *supra* note 5, at 293-94. See also John Moteff, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*, CONG.

RESEARCH SERV, <http://www.fas.org/irp/crs/RL32357.pdf> (last visited Oct. 19, 2010).

<sup>11</sup> Most recently, Senator Joe Lieberman proposed a Congressional Bill entitled “Protecting Cyberspace as a National Asset of 2010.” The primary focus of the bill is both the protection of critical national infrastructure from cyber-attacks abroad and the creation of emergency powers, vested in the President, designed

Meanwhile, the Russian government has voiced adamant support for an international treaty regulating and limiting the use of cyber warfare technologies while concurrently working diligently to advance their own cyber technologies.<sup>12</sup> Domestic movements in other advanced states, including the United Kingdom and China, to strengthen and expand internal cyber-security and cyber-capabilities further evidence a growing global awareness of the importance of cyber warfare.<sup>13</sup> Finally, even less nationalistic international organizations have begun to make cyberspace issues a priority on their own security agendas.<sup>14</sup>

The purpose of this Comment is to consider how cyber warfare is currently addressed by international laws and the degree to which

---

specifically to allow for quick responses to major cyber-attacks (the specifics of the proposed Bill will be considered later in this comment). See Donny Shaw, *Lieberman Cybersecurity Bill Would Give DHS Broad Emergency Powers Over the Internet*, OPEN-CONGRESS BLOG (June 14, 2010), <http://www.opencongress.org/articles/view/1917-Lieberman-Cybersecurity-Bill-Would-Give-DHS-Broad-Emergency-Powers-Over-the-Internet>.

<sup>12</sup> See *infra* notes 120, 262 (describing the Russian military approach to cyber warfare operations and recent Russian suggestions of an international treaty agreement to limit the use and proliferation of cyber warfare generally).

<sup>13</sup> Within the past few years, several other states have begun to address the issue of cyber warfare and cyber-security directly through directives, legislation, and domestic measures aimed at developing and protecting national cyberspace autonomy. In 2009, the UK issued an internal Cabinet Office document entitled “Cyber Security Strategy of the United Kingdom—Safety, Security, and Resilience in Cyberspace.” See Stuart Malawer, *Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance*, VIRGINIA LAWYER, INTERNATIONAL PRACTICE SECTION, Vol. 58, February 2010, at 29. Several other states have also made cyber-security and cyber warfare capabilities an increasingly important area of their military and governmental agendas (particularly, the development of cyber warfare strategy and capabilities in China and Russia, which will be discussed later in this comment). See Solce, *supra* note 5, at 287-99.

<sup>14</sup> In 2001, the European Union created a “Convention on Cybercrime” in an effort to begin addressing, on an unprecedented scale, the problems and threats of cyberspace activities. See Council of Europe, Convention on Cybercrime, Additional Protocol/ Explanatory Reports, Nov, 23, 2001, C.E.T.S 185, available at <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>. Additionally, in 2010, Hamadoun Tourè, U.N. International Telecommunications Union Secretary General, stated that he felt an international treaty seeking to prevent cyber warfare was needed. AFP, *UN Chief calls for treaty to prevent cyber war*, GOOGLE NEWS (Jan. 30, 2010), <http://www.google.com/hostednews/afp/article/AleqM5h8Uvk-jpSvCWT-bqYSglW>.

those laws remain both applicable and effective. The analysis proceeds in three Parts: Part I discusses the historical development of cyber warfare and its increasing usage in modern conflicts,. Part II considers the applicability of current international laws to the realm of cyber warfare, and Part III considers broad changes needed within the international law paradigm to allow for the effective regulation of cyber warfare.

## II. THE EMERGENCY OF CYBER WARFARE

### A. Defining Cyber Warfare

Any investigation into the meaning of cyber warfare must begin with considering cyberspace, the newly realized computer and information domain in which such warfare occurs. The term “cyberspace” was first used by William Gibson in his 1984 novel *Nueromancer*, which detailed the story of a computer hacker hired by a mysterious employer to work on the ultimate computer network hack job.<sup>15</sup> In this original context, the term was used to refer to “a shared virtual environment whose inhabitants, objects, and spaces comprise data that is visualized, heard and touched.”<sup>16</sup> Obviously, this literary definition has become altered over the course of time as the concept of cyberspace materialized into a modern reality. Today, cyberspace is most commonly associated with notions of the Internet, the World Wide Web, and globally connected computer systems and operating networks.<sup>17</sup> However, cyberspace has also become

---

<sup>15</sup> WILLIAM GIBSON OFFICIAL WEBSITE, <http://www.williamgibsonbooks.com> (last visited Nov. 11, 2010).

<sup>16</sup> MICHAEL A. SINKS, *CYBER WARFARE AND INTERNATIONAL LAW* 3 (Air Command and Staff College, April 2008).

<sup>17</sup> *See id.* Modern commentators have also sought to provide more simplistic definitions of cyberspace; one such plain language attempted definition reads, “[c]yberspace is not a physical place—it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web.” THOMAS WINGFIELD, *THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE* 17 (2000).

increasingly defined in a military context by a variety of governmental agencies and bodies.<sup>18</sup>

Within the United States, the definitions of cyberspace differ from one government department to another. The Department of Defense has termed cyberspace to mean 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.”<sup>19</sup> Meanwhile, in a 2001 Congressional Research Service (“CRS”) report, cyberspace was redefined, this time as the “total interconnectedness of human beings through computers and telecommunication without regard to physical geography.”<sup>20</sup> Finally, the National Military Strategy for Cyberspace Operations proposed the following definition: “[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.”<sup>21</sup>

This inability to settle upon a definition of cyberspace, even within the departments of a nation as advanced as the U.S., remains equally applicable to the more specific notion of cyber warfare.<sup>22</sup> Again, within the U.S., definitions of cyber warfare also differ from one government department to another. The Department of Defense has defined cyber operations as “the employment of cyber

---

<sup>18</sup> See SINKS, *supra* note 16, at 3.

<sup>19</sup> JOINT CHIEFS OF STAFF, JOINT PUBLICATION 1-02, DEP’T OF DEF. DICT. OF MILITARY & ASSOC’D TERMS 141 (2001), *available at* [http://www.dtic.mil/doctrine/jel/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf).

<sup>20</sup> STEVEN A. HILDRETH, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS NO. RL30735, CYBERWARFARE 11 (2001) [hereinafter 2001 CRS Report].

<sup>21</sup> Staff Sergeant C. Todd Lopez, *Fighting in Cyberspace means Cyber Dominance*, A.F. PRINT NEWS, Feb. 28, 2007. In 2006, the Joint Chiefs of Staff of the U.S. Armed Forces officially adopted this as the definition that would be utilized generally by the U.S. military. See Michael W. Wynne, Sec’y of the Air Force, Remarks as Delivered to the C4ISR Integration Conference: Cyberspace as a Domain in Which the Air Force Flies and Fights (Nov. 2, 2006), *available at* <http://www.af.mil/library/speeches/speech.asp?id=283> (last visited Oct 20, 2010).

<sup>22</sup> See Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 125-126 (2009).



capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace.”<sup>23</sup> In the 2001 CRS Report, a slightly more generalized definition of cyber warfare was provided: “[c]yberwarfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary’s ability to do the same.”<sup>24</sup>

Ultimately, cyber warfare, regardless of the specific definition used, has come to symbolize a state sponsored use of weapons functioning within the cyberspace domain to create problematic and destructive real world effects. The lack of workable, universally accepted definitions of cyberspace and cyber warfare only further exacerbates any attempt to analyze international regulation of activities, such as cyber warfare, occurring within the cyberspace domain.<sup>25</sup>

### *B. The Weapons of Cyber Warfare*

While it was formerly the case that cyber warfare weaponry continued to function primarily to immobilize enemy forces on the battlefield, this is no longer the case.<sup>26</sup> As cyber weaponry has

---

<sup>23</sup> JOINT PUB., *supra* note 19, at 141. The Department of Defense has appeared to remain committed to the position that cyber warfare and “network warfare operations” are essentially the same and should be addressed accordingly. *Id.*

<sup>24</sup> See Hildreth, *supra* note 20, at 1. Many commentators have sought to break cyber warfare operations into two distinct categories: offensive and defensive. See e.g., Iftach Ian Amit, *Cyber[crime-war]*, SECURITY AND INNOVATION GROUP (2010) at 2-5, [www.securityandinnovation.com](http://www.securityandinnovation.com). The basic argument is simply that cyber warfare is actually best viewed as two separate kinds of actions: “on the defense side, the aim of cyber warfare is to protect infrastructure, military capabilities, and civilian institutions. On the offence side, the aim of cyber warfare is to target an adversary’s critical infrastructure, alter their view of the battlefield (both kinetic and virtual), and affect their population (propaganda).” *Id.* at 3.

<sup>25</sup> See Wolfgang McGavran, *Intended Consequences: Regulating Cyber Attacks*, 12 TUL. J. TECH. & INTELL. PROP. 259, 271 (2009).

<sup>26</sup> See Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT’L L.J. 272, 283-84 (Winter 1996). As Kanuck predicted in his 1996 comment on the then newly burgeoning field of cyber warfare, the aims of such cyber based attacks is not likely to be confined to purely

become increasingly used against both military and civilian targets, it remains important to understand that cyber weapons actually come in two distinct forms.<sup>27</sup> The first is the actual delivery method weapon: this is the standard device actually used as the portal through which the cyber attack is coordinated and the cyber weaponry constructed.<sup>28</sup> The second type of cyber weaponry is the cyberspace component.<sup>29</sup> These intangible weapons are potentially comprised of computer programs, network viruses, and digital command operations, and function solely in the cyberspace domain.<sup>30</sup> Since the primary

---

military targets as the technology of cyber weapons and the increasing regularity of their use expand. *Id.* at 284. Indeed, he notes, “[cyber warfare] extrapolation to a much wider warspace is frighteningly plausible and probable. Strategic nodal analysis in the twenty-first century will most likely point to financial databases, government records, air traffic control systems, communications networks, or automated public utilities as the ideal targets of full-scale aggression.” *Id.* In the end, Kanuck observes, “attacking an enemy’s information networks may go beyond incapacitating its armed forces; it may serve as the best means of achieving victory.” *Id.* This understanding of cyber weaponry has two critical implications: first, it indicates that cyber warfare is likely to become a general military strategy seeking as its ultimate aim final wartime victory, not merely the rendering of enemy military forces inoperable. Second, it becomes increasingly clear that when such an aim becomes the primary goal of cyber warfare operations, civilian and military targets become equally susceptible to attack to achieve that goal. These predictions regarding the critical role of cyber warfare in the future of military operations were also supported by Arquilla and Ronfeldt, who anticipated that cyber warfare would “be to the 21st century what *Blitzkrieg* was to the 20th century.” Arquilla, *supra* note 4, at 31.

<sup>27</sup> See generally McGavran, *supra* note 25, at 261.

<sup>28</sup> See *id.* The point here is that it takes devices existing within the physical world of everyday reality, such as computers, modems, and connection cables to build and deploy a cyber attack. One way to prevent such attacks would be the destruction of these material devices that are at the root of the cyberspace domain.

<sup>29</sup> See *id.*

<sup>30</sup> See *id.* Again, the key is to remember that there is a critical distinction between the cyberspace domain weapons and the actual physical weapons, far more innocuous in their appearance simply because of their ability to do so many other innocent tasks (certainly, a computer is not thought of in the same way as a machine gun, despite the fact that, in the proper hands, the computer may be a far more effective weapon capable of killing many more people) used to employ the cyberspace domain weaponry. This difference between the weaponry of cyber warfare may seem somewhat irrelevant when the effects of the weaponry are ultimately the same, but the distinction nonetheless creates complex legal issues that are explored in more detail subsequently.

weapons—those used as the delivery method—are present in almost every aspect of our daily lives, it is the second kind of cyber weaponry, functioning only within the cyberspace domain, that have become the focus of State development in the cyber warfare context.<sup>31</sup> Although constantly evolving, the most common types of cyber domain weapons, including their basic functions, capabilities, and uses, are outlined below.

### 1. Denial-of-Service

A denial-of-service (“DoS”) attack is defined as an “assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted”.<sup>32</sup> Generally, DoS attacks work by crippling a website or computer network resource and making it unusable by overwhelming the resource with a massive amount of information requests, resulting in an inability to respond to legitimate information and data requests.<sup>33</sup>

---

<sup>31</sup> A simple example may be illustrative: a state conducting cyber warfare operations requires two weapons to carry out its attack. First, it requires the delivery weapon (likely a computer and internet connection); second, it also requires some cyberspace weaponry to be transported across the cyberspace domain and intended to affect the ability of an enemy’s functioning within the cyberspace domain. Since it is not difficult to acquire primary delivery weapons – computers are available globally and expense is not a likely deterrent to a state conducting cyber warfare operations – it is the secondary weapons, operating within cyberspace alone, that are preciously sought after by state governments interested in employing cyber warfare. These cyberspace domain weapons, therefore, are the key to the conducting of cyber warfare operations generally.

<sup>32</sup> See *TechEncyclopedia, Denial of Service Attack*, TECHWEB.COM, <http://www.techweb.com/encyclopedia/> (search “Denial of Service Attack”; then follow “Look Up” hyperlink) (last visited Oct. 6, 2010). Generally, there seems to be basic agreement amongst international cyber warfare commentators that these types of attacks are the most common form of cyber warfare weaponry because of their simplicity and overall effectiveness in disrupting computer network functions. See generally Mindi McDowell, *Understanding Denial of Service Attacks*, U.S. COMPUTER EMERGENCY READINESS TEAM (2004), <http://www.us-cert.gov/cas/tips/ST04-015.html>.

<sup>33</sup> See McDowell, *supra* note 32. See also *Managing the Threat of Denial-of-Service Attacks*, CERT COORDINATION CENTER, (2001), [http://www.cert.org/archive/pdf/Managing\\_DoS.pdf](http://www.cert.org/archive/pdf/Managing_DoS.pdf). According to the CERT, a DoS attack is intended to hinder the operation of a computer network service by

A distributed-denial-of-service (DDoS) attack operates similarly to a standard DoS attack, but involves the coordination and use of numerous pre-infected computers working in unison to disable a single, targeted computer network or service.<sup>34</sup> Specifically, “an aggressor utilizes thousands of infected computers—known as zombies or bots—to concurrently attack a single system.”<sup>35</sup> DDoS attacks remain an attractive and effective cyber warfare weapon because they exponentially increase the power of standard DoS attacks and are available at relatively low cost.<sup>36</sup> Consequently, according to one commentator, a state could “fund an entire cyber warfare campaign for the cost of replacing a tank tread [and] would be foolish not to.”<sup>37</sup>

## 2. Malicious Programs

Malicious programs, or malware, typically operate by “disrupting normal computer functions, or by opening a back door for a remote attacker to take control of the computer.”<sup>38</sup> Viruses, the

---

“explicit[ly] attempt[ing] . . . to prevent legitimate users of a computer-related service from using that service.” *Id.*

<sup>34</sup> See Schaap, *supra* note 22, at 134.

<sup>35</sup> *Id.*

<sup>36</sup> See McGavran, *supra* note 25, at 262. See also John Markoff, *Cyber Attack Preceded Invasion*, CHI. TRIB. (Aug. 13, 2008), <http://archives.chicagotribune.com/2008/aug/13/business/chi-cyber-war>. DDoS attacks also remain a highly attractive cyber warfare option because they originate from multiple computers located in several locations and thus, are increasingly difficult to trace. See Kevin Coleman, *Department of Cyber Defense, An Organization who's time has come!*, TECHNOLYTICS, 2 (Nov. 2007), [http://www.technolytics.com/Dept\\_of\\_Cyber\\_Defense.pdf](http://www.technolytics.com/Dept_of_Cyber_Defense.pdf).

<sup>37</sup> See McGavran, *supra* note 25, at 262-63.

<sup>38</sup> See Schaap, *supra* note 22, at 135. See generally Clay Wilson, Cong. Research Serv. Rep. For Cong. No. RL32114, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress 15*, 21 (Oct. 17, 2003), available at <http://www.fas.org/irp/crs/RL32114.pdf>. One of the primary appeals of malicious software is that it can be configured to either immediately disable an infected computer, or it may operate on a time delay, disabling the infected computer only after being remotely prompted to carry out its disabling commands. *Id.* at 35. Further, malicious programs may also operate to disable the infected computer directly or they may take over the infected computer and cause it to issue commands disabling or disrupting other computer networks. *Id.*

most common form of malicious programming, may function to delete certain computer files or make such files unusable.<sup>39</sup> Specifically, a virus attaches itself to a computer program or file and spreads from one computer to another, moving across computer networks by way of self-replication.<sup>40</sup> Additionally, a virus will typically carry a “payload”—a side effect of the virus that normally functions to corrupt or destroy computer data on the infected computer.<sup>41</sup> Viruses typically have the ability to remain discretely present within an infected computer, only becoming destructive when a user runs or opens the software to which the malicious program has been attached.<sup>42</sup>

The other common form of malicious programming, a worm, functions similarly by spreading from one computer to another and eventually infecting an entire computer network.<sup>43</sup> However, a worm differs from a virus in that it is both capable of traveling across a computer system without aid from individual computer users and it is capable of directly replicating itself thousands of times within a single computer.<sup>44</sup> Worms tend to consume massive amounts of memory, and as a result, infected computers, and the networks they operate on, often become unresponsive.<sup>45</sup> With recent cyber

---

<sup>39</sup> See *The Tech Terms Computer Dictionary, Malware*, TECHTERMS.COM, <http://www.techterms.com/definition/malware> (last visited Oct. 24, 2010).

<sup>40</sup> *Introduction to Computer Viruses*, SOPHOS.COM (May 26, 1998), [http://www.sophos.com/en-us/press-office/press-releases/1998/05/va\\_virusesintro.aspx](http://www.sophos.com/en-us/press-office/press-releases/1998/05/va_virusesintro.aspx).

<sup>41</sup> *Id.*

<sup>42</sup> See Vangie Beal, *The Difference Between a Virus, Worm, and Trojan Horse*, WEBOPEDIA.COM (June 29, 2010), <http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp>. The concept that malicious software may exist on a computer benignly until activated by the computer user is known generally as an attachment to an executable file. *Id.*

<sup>43</sup> *Id.*

<sup>44</sup> *Id.* Unlike a virus, which both requires a computer user to actively open or start the software containing the malicious program and the virus to spread to other computers to replicate itself, a worm is able to activate on its own and replicate on a single computer. *Id.* These key features make the worm a more sophisticated and dangerous form of computer virus, as one computer infected with a worm may subsequently send out thousands of self-replicated copies to other computers operating on the same network. *Id.*

<sup>45</sup> *Id.*

advances, worms may now allow individuals to tunnel into computer systems and even remotely control the infected computer.<sup>46</sup>

### 3. Logic Bombs

Logic bombs, a more advanced type of malicious programming, only execute their destructive effects when triggered by particular events occurring at a pre-determined time.<sup>47</sup> A logic bomb can sit dormant for long periods of time unsuspected and then be activated, making its effects far more likely to be wide-spread than if its' malicious impact was readily apparent.<sup>48</sup> Once activated, a logic bomb may cause severe damage to the infected computer, rendering it entirely unusable, deleting specific data, or even functioning to activate a more complex DoS attack.<sup>49</sup>

### 4. IP Spoofing

Also known as IP address forgery, IP spoofing is a kind of hijacking technique that allows the hacking user to operate a

---

<sup>46</sup> *Id.* Another critical and more general recent development has been the emergence of polymorphic malware, which allows the malicious software to alter its signature randomly every time it replicates and spreads to another computer. *See generally* Glossary, *Polymorphic Malware*, INTERNETSECURITYZONE.COM, [http://www.internetsecurityzone.com/Glossary/Polymorphic\\_Malware](http://www.internetsecurityzone.com/Glossary/Polymorphic_Malware) (last visited Oct. 26, 2010). The emergence of polymorphic malware allows worm and virus malware to avoid detection by anti-malware programs designed to recognize malware by its specific signature and characteristics, while simultaneously not affecting the ability of the malicious program to disrupt the functions of the infected computers. *Id.*

<sup>47</sup> *See* Coleman, *supra* note 36. *See also* *What is a logic bomb?*, TECH-FAQ.COM, <http://tech-faq.com/logic-bomb.shtml> (last visited Oct. 28, 2010).

<sup>48</sup> *See* David Hoffman, *CIA Slipped Bugs to Soviets*, THE WASHINGTON POST (Feb. 26, 2004), [http://www.industrialdefender.com/general\\_downloads/incidents/1982.06\\_trans\\_si\\_berian\\_gas\\_pipeline\\_explosion.pdf](http://www.industrialdefender.com/general_downloads/incidents/1982.06_trans_si_berian_gas_pipeline_explosion.pdf). As Hoffman discusses in his article, this type of cyber warfare technology has been readily available and was allegedly utilized as far back as the Cold War Era by the CIA to destroy a Soviet natural gas pipeline. *Id.*

<sup>49</sup> *See* Coleman, *supra* note 36.

computer while appearing as a trusted host.<sup>50</sup> By thus concealing his true identity, the hacker can gain access to computer networks and network resources.<sup>51</sup> When hijacking a network Internet browser, any computer using the browser upon entering a URL is taken to a fraudulent webpage mirroring the entered site page, but created by the hijacker.<sup>52</sup> The moment the user interacts with any of the content of the fraudulent webpage, the hijacking user gains the ability to access sensitive network information or the computer's fundamental programming features.<sup>53</sup>

## 5. Trojan Horses

Trojan horses, as the name implies, operate as a kind of malicious software based on fooling targeted computers into believing that the malicious program will actually perform a useful or desired function.<sup>54</sup> Instead, the Trojan horse acquires unauthorized access to the infected computer.<sup>55</sup> Subsequently, the Trojan horse programming allows a remote user to access the infected computer and may also cause the infected computer to serve as a resource in later DoS attacks.<sup>56</sup>

These key weapons of cyber warfare are becoming increasingly accessible to an ever-growing number of states.<sup>57</sup> Recent studies have

---

<sup>50</sup> See *IP Spoofing*, (IP address forgery or a host file hijack), SEARCHSECURITY.COM, <http://searchsecurity.techtarget.com/definition/IP-spoofing> (last visited Oct. 28, 2010).

<sup>51</sup> See *id.*

<sup>52</sup> *Id.*

<sup>53</sup> *Id.*

<sup>54</sup> See, e.g., *Targeted Trojan Email Attacks*, U.S. COMPUTER EMERGENCY CENTER (July 8, 2005), <http://www.us-cert.gov/cas/techalerts/TA05-189A.html>.

<sup>55</sup> *Id.*

<sup>56</sup> See McDowell, *supra* note 32. Trojan horses are key cyber warfare weapons because they both allow a remote user to acquire access to an infected computer at any time after infection and also to use the infected computer in later DoS attacks requiring several computers to jam other network services, or computer programs operating on different servers. *Id.*

<sup>57</sup> See generally Kevin Coleman, *The Cyber Arms Race has Begun*, CSO ONLINE (Jan. 28, 2008), <http://www.csoonline.com/exclusives/column.html?CID=33496>.

determined that, given the modest costs involved in conducting basic cyber warfare operations, nearly 140 states have operational cyber warfare programs.<sup>58</sup> The availability of cyber warfare weaponry, and the potentially devastating effects that such weapons may have on an enemy's critical infrastructures during global conflict, further indicate the paramount importance of understanding the legal implications of cyber warfare. The increased willingness to engage in cyber warfare operations, examples of which form the basis of the following Part of this comment, make clear the immediate need for such consideration.<sup>59</sup>

### *C. Modern Proliferation: Instances of Cyber Warfare in Our Contemporary World*

#### 1. Estonia

In April of 2007, one of the world's most Internet-dependent nations, Estonia, came under severe and crippling cyber attack.<sup>60</sup> The DDoS attack ultimately left the nation in cyber shambles: only hours after the attack, the web sites of Estonia's leading banks, newspapers, and major government agencies had crashed, thrusting the nation into cyberspace isolation.<sup>61</sup>

---

<sup>58</sup> *Id.*

<sup>59</sup> See *infra* note 277 (Discussing the importance of regulating cyber warfare operation now, while it remains in its infantile stages of development and prior to becoming a permanent and critical fixture of states' military strategy).

<sup>60</sup> See Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED MAG (Aug. 21, 2007), [http://www.wired.com/politics/security/magazine/15-09/ff\\_estonia?currentPage=all](http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all).

Estonians use the Internet, and Internet based services, for nearly every aspect of their daily lives; Estonians manage their personal banking primarily over the Internet, and Estonians can even vote in national elections online. See Sutton Meagher, Comment, *When Personal Computers are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights*, 23 Am. U. Int'l L. Rev. 349, 356 (2008). This massive reliance on the Internet for everyday living in Estonia has even led some commentators to refer to Estonia as "E-stonia". See, e.g., Indranjit Basu, *Estonia becomes E-stonia*, DIGITAL COMMUNITIES (Apr. 9, 2008), <http://www.govtech.com/dc/articles/284564>.

<sup>61</sup> See Davis, *supra* note 60. See also Johnny Ryan, *Growing Dangers: Emerging and Developing Security Threats*, NATO REV. (Winter 2007),



Some believe, and Estonia publicly indicated its belief, that Russia was responsible for the attacks.<sup>62</sup> However, the attacks

---

<http://www.nato.int/docu/review/2007/issue4/english/analysis2.html>. The DDoS attacks targeted and paralyzed the most critical Estonian web sites and were particularly aimed at the web sites of the president, parliament, political ministries and parties, major news outlets, and Estonia's two major banks. *Id.* The DDoS attacks worked by overloading the Estonian web sites with so much request information that the servers backed up to the point of shutting down altogether. *Id.* According to the Estonian Defense Minister, the sites, normally visited around 1,000 times per day, were under cyber bombardment of nearly 2,000 visits and requests per second. *See* Steven L. Meyers, *Estonia Accuses Russia of Computer Attacks*, N.Y. TIMES (May 18, 2007), <http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html>17h.. The DDoS attack was, in fact, a combination of several simultaneously occurring DDoS attacks, and at the time of the attack nearly 130 identifiably different DDoS attacks were targeting and disrupting Estonian Internet infrastructures. *See* Sean Kerner, *Estonia Under Russian Cyber Attack?*, INTERNETNEWS.COM, (May 18, 2007), <http://www.internetnews.com/security/article.php/3678606/Estonia+Under+Russia+n+Cyber+Attack.htm>. Internet traffic increased dramatically during the attack, and the units of actual data being transmitted on Estonian servers increased from 20,000 to over 4 million units per second during the course of the DDoS attacks. *Id.*

<sup>62</sup> *See A Cyber Riot: Estonia and Russia*, THE ECONOMIST, May 12, 2007, available at <http://www.economist.com/node/9163598>. Russia denied, and continues to deny, all involvement in the attacks. *Id.* However, several of the original domains for the initial attacks were traced by security officials to Russian servers, some of which were actually registered directly to the Russian government and then President Putin. *See* Meyers, *supra* note 61. Even after Estonia reported the attacks to the EU and NATO, the Kremlin continued to adamantly deny responsibility for the attacks. *Id.* Many continue to maintain, however, that the DDoS attack was Russian retaliation for Estonian officials relocating a Soviet-era bronze statute, called the Soldier of Tallinn, from the Estonian capitol to an international military cemetery outside the city. *See A Cyber Riot*, THE ECONOMIST, May 12, 2007. Ethnic Russians, who comprise nearly one fourth of the Estonian population, and the Russian Government objected to the movement, which they viewed as an insult and marginalization of Estonia's Russian historic heritage. *Id.* The Russian government even called the actions "blasphemous" and the Estonian authorities were faced with riots by some of the ethnic Russian population. *Id.* Still others have contended that the attack was an attempt by Russia to test both the West's preparedness for such a cyber attack, as well as NATO's commitment to its newest and smallest members (Estonia had become a member of NATO in 2004). *See* Anne Applebaum, *For Estonia and NATO, A New Kind of War*, WASH. POST, May 22, 2007, at A15, available at <http://www.nato.int/structur/countries.htm>. After Estonia asked for cyber assistance from NATO, and shortly after NATO cyber experts arrived in Estonia, the attacks stopped in their entirety. *See Cyber*

originated from several other nations, and the nature of the DDoS attacks themselves made tracing the ultimate source impossible.<sup>63</sup> Ultimately, the attack on Estonia demonstrated “several disturbing realities.”<sup>64</sup> It displayed the extremity of the attribution problem in cyber attacks, the ease with which devastating cyber attacks may be employed, and the real world destruction that may be caused by attacks carried out solely in the cyberspace domain.<sup>65</sup>

---

*War as the Ultimate Weapon*, STRATEGYWORLD.COM, (Jan. 5, 2008), <http://www.strategypage.com/htm/w/htiw/articles/20080105.aspx> .

<sup>63</sup> See *Frontline: Cyberwar!*, (PBS television broadcast Apr. 24, 2003), available at <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwarfar/>. The DDoS servers responsible for the attacks originated from several locations, including the United States, Egypt, South America, and Russia. See Davis, *supra* note 60; see also Shackelford, *supra* note 3, at 203. The ability to identify the source of DDoS attacks is always practically impossible because of the fact that the actual attacks are not necessarily, or even normally, carried out by the attacker. See Schaap, *supra* note 22, at 134. In a typical DDoS attack, as seen in the attacks against Estonia, a central controlling computer system will often initiate the attack, which will actually be carried out, unbeknownst to the computer users, by other infected computer systems located all around the globe. *Id.* The resulting anonymity of the initial computer user, who initiates the attack but may not even actually participate in the attack itself, is one of the most attractive characteristics of a DDoS attack. *Id.* The anonymity afforded by use of DDoS attack was on full display nearly a decade earlier than the attack on Estonia when, in 1998, the “Solar Sunrise” attacks on United States Department of Defense computer systems occurred. See Christopher Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT’L L. 825, 839-840 (2001). Computers registered and located within the United Arab Emirates carried out the DDoS attacks in this case; however, it was a young Israeli and two high schools students from California, and not the UAE, who had initiated the attacks. See JOHNATHAN ZITTRAIN, *THE FUTURE OF THE INTERNET AND HOW TO STOP IT* 37-45 (2008); see also *Solar Sunrise*, GLOBALSECURITY.ORG, <http://www.globalsecurity.org/military/ops/solar-sunrise.htm> (last visited Oct. 25, 2010). The teenagers took advantage of the “global integration of the Internet” to hide the origin of the true source of the attacks while manipulating the DDoS attack locations to make it appear as though the attacks had originated from the UAE. See Shackelford, *supra* note 3, at 204. If high school students are able to sufficiently hide the true origins of their simple DDoS attack designs, imagine the difficulty in tracing highly specialized cyber warfare professionals.

<sup>64</sup> McGavran, *supra* note 25, at 265.

<sup>65</sup> *Id.*

## 2. Georgia

In 2008, Georgia, responding to separatist actions, launched surprise aerial and ground attacks against the revolutionary forces located in the provinces of South Ossetia and Abkhazia.<sup>66</sup> Shortly thereafter, a simple, yet crippling DDoS attack hit several of Georgia's government and media websites.<sup>67</sup> These initial cyber attacks were traced to commanding servers in Russia.<sup>68</sup> Although there remains no direct evidence of Russian government involvement, the subsequent actions make some degree of Russian State involvement seem far more likely.<sup>69</sup> Only a short while after the

---

<sup>66</sup> See McGavran, *supra* note 25, at 265. McGavran also notes that much of the international community, including NATO and the U.S., criticized this offensive military action by Georgia. *Id.* at n. 47. Nevertheless, he does not seem to indicate that these criticisms were in any way a condolence of the subsequent Russian reprisals taken against Georgia. *Id.* at 265.

<sup>67</sup> See Jeremy Kirk, *Estonia, Poland Help Georgia Fight Cyber Attacks*, CIO (Aug. 12, 2008), [http://www.cio.com/article/443314/Estonia\\_Poland\\_Help\\_Georgia\\_Fight\\_Cyber\\_Attacks](http://www.cio.com/article/443314/Estonia_Poland_Help_Georgia_Fight_Cyber_Attacks). The attacks specifically included hijacking and defacing government sites such as the official website of Georgian President Mikheil Saakashvili. *Id.* On the President's website, the site appearance had been altered and anyone visiting the site was prompted to a photo gallery displaying President Saakashvili's picture juxtaposed next to images of Adolf Hitler. *Id.* Although the DDoS attack was very similar to the cyber attack on Estonia only a year before, the effects of the attacks in Georgia were far less. *Id.* However, Kirk notes, it is critical that the reason for this lesser effect is not that the cyber attack method was less effective, but merely that Georgia is not nearly as reliant upon Internet infrastructure as the more advanced Estonian state. *Id.* Perhaps more critically, Georgian military IT systems were affected by these attacks. See Brian Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, WASH. POST (Oct. 16, 2008), [http://voices.washingtonpost.com/securityfix/2008/10/report\\_russian\\_hackers\\_forums\\_f.html](http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hackers_forums_f.html). The Georgian air defense systems were heavily affected and Georgian military command and control operations were, for some time, operated solely through U.S. government and unsecured Google accounts. *Id.*

<sup>68</sup> See Kirk, *supra* note 67.

<sup>69</sup> See *id.*; Iftach Ian Amit, *Cybercrime/War: Linking State Governed Cyber Warfare with Online Criminal Groups*, SECURITY AND INNOVATION, <http://www.securityandinnovation.com> (last visited Oct. 12, 2010). Amit argues that professionally hired criminal groups, centered in Russia and employed as freelance cyber warfare mercenaries, were responsible for the actions against Georgia. *Id.* Although a fascinating notion, the fact remains, as Kirk notes in his

initial cyber attacks on Georgian websites, Russian army, navy, and air forces formed the heart of a kinetic military offensive against the territorial sovereignty of the Georgian State.<sup>70</sup> The ability to coincide cyber attacks with conventional military offensives makes for an efficiently devastating combination and, in the current state of international legal uncertainty surrounding the state-sponsored use of cyber attacks, they may become more and more prevalent as a general military strategy.<sup>71</sup>

---

article on the cyber attacks in Georgia, that the Russian government has adamantly denied responsibility for the attacks and the lack of direct evidence linking the cyber attacks and Russian state sponsorship are the more legally persuasive arguments. *See* Kirk, *supra* note 67. Nonetheless, it has been further noted that Russian state involvement in the attacks seemed highly likely because of the high level of preparation and advanced reconnaissance employed in executing the attacks. *See* Krebs, *supra* note 67.

<sup>70</sup> *See* Markoff, *supra* note 36. Markoff notes that the initial attacks on the Georgia government and media sites began roughly one month before the actual Russian military offensive and the beginning of the Georgian War. *Id.* He suggests that these may have served as preliminary attacks to test their efficiency, and expected full-scale usage during the impending, actual conflict. *Id.* After the Russian military offensive against Georgia ended, the cyber attacks against the Georgian sites continued for some time before finally dying down. *Id.* Even then, it has been argued that the eventual ability of Georgia to overcome the ongoing cyber attacks against its official web sites was likely due, in large part, to the extensive assistance given by the far more Internet savvy Estonian and Polish states to the Georgian authorities in mitigating the damage of the attacks and creating more secure server space for the targeted web sites. *See* Kirk, *supra* note 67; *see also* Eneken Tuck Et Al., *Cyber Attacks Against Georgia: Legal Lessons Identified 4*, COOP. CYBER DEF. CTR. OF EXCELLENCE (2008), <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf>.

<sup>71</sup> *See* Siobhan Gorman, *Cyberattacks on Georgian Web Sites are Reigniting a Washington Debate*, WALL ST. J. (Aug. 14, 2008), [http://online.wsj.com/article/SB121867946115739465.html?mod=googlenews\\_wsj](http://online.wsj.com/article/SB121867946115739465.html?mod=googlenews_wsj). The general reason for this trend may simply be that states generally, with the lack of clear and precise international legal standards, do not consider such cyber attacks to be warfare weapons and hence, are permissible forms of wartime strategy. *Id.* As Scott Borg, the director of the U.S. Cyber Consequences Unit, has stated, “we are in a world where governments have not decided whether the tools of cyberattacks are weapons [and] [w]e don’t have any really clear international understandings about these matters.” *Id.*

### 3. Iran

In 2009, two events relating to the volatile Iranian state further evidenced the power, utility, and growing use of cyber warfare in modern military strategy. First, following the 2009 Iranian elections, there erupted what FOX News termed a “full-on guerrilla cyberwar” between the Iranian government and dissatisfied domestic movements protesting the national elections.<sup>72</sup> In response to what many Iranians felt was an unfair election, the movements began coordinating demonstrations and undertaking efforts to bring down key government web sites.<sup>73</sup> The internal forces working to subvert the Iranian government were coordinating their activities through Twitter, a U.S.-based online communications and posting web application.<sup>74</sup> Despite the requests of the Iranian government to cease its functioning within Iran, Twitter took affirmative steps to remain active and usable by the Iranian population.<sup>75</sup> It remains unclear

---

<sup>72</sup> *Crisis in Iran Sparks Global Guerilla Cyberwar*, FOX NEWS (June 16, 2009), <http://www.foxnews.com/story/0,2933,526627,00.html>.

<sup>73</sup> *See id.* Although this appears to be merely domestic discord being channeled into online action (which, in and of itself would be a valid area of concern—the concept of internal cyber civil war between nationals and their government), the events following the Iranian election also illustrate the extent to which one nation can subtly utilize cyber warfare tactics against another. *See id.* Here, the real cyberbattles were between the Iranian government and dissatisfied segments of their own population; yet it was the means used to fight those battles that allowed for passive strategic intervention by other interested nations. *See id.*

<sup>74</sup> *See id.*

<sup>75</sup> *Id.* In an effort to combat national protest coordination and online propaganda against the results of the national elections, the Iranian government began an extensive censorship program of online materials. *See id.* Consequently, many Twitter users and bloggers outside Iran began to post and tweet information on how to avoid such censorship and some even changed their own network settings to mirror those in Iranian settings in an effort to confuse Iranian officials working to block domestic online postings. *Id.* Some Twitter users even posted instructions on how to disable official Iranian government web sites. *Id.*; *see also* Noah Sachtman, *Web Attacks Expand in Iran’s Cyber Battle (Updated Again)*, DANGER ROOM, WIRED.COM, (June 16, 2009, 4:06 PM), <http://www.wired.com/dangerroom/2009/06/web-attacks-expand-in-irans-cyber-battle/> (noting that since its inception, and with assistance from international bloggers and tweeters (specifically those based in the U.S.) (the internal cyber opposition has begun a full-scale assault on Iranian media outlets as a way to maintain Iranian opposition communications and disrupt a small amount of official

whether the decision to remain operable came solely from Twitter, or if the decision was backed by U.S. government officials..<sup>76</sup>

Second, in 2010, Iran's two major nuclear power and research facilities at Bushehr and Natanz were hit with what FOX News called the "most sophisticated cyberweapon ever created."<sup>77</sup> The weapon, dubbed Stuxnet, operates as a cybermissile equipped with a warhead designed specifically to penetrate advanced security systems and take control of general computer system controls.<sup>78</sup> Although Iran initially denied that any attack had taken place, it has since admitted that the Stuxnet weapon was a massive disruption to the development of its

---

government web sites. This assault includes systematically targeted DDoS attacks on numerous Iranian government sites). After a top Iranian crisis tweeter posted that twitter had become the sole means of internal communications and reporting of news in Iran, Twitter, recognizing its critical importance to these domestic protests, went so far as to inconvenience millions of American users and rescheduled an important network update to allow Twitter to remain active in Iran. See *Crisis in Iran Sparks Global Guerilla Cyberwar*, *supra* note 72. Using the Twitter access, Iranians were ultimately able to maintain internal communications and reporting, and, as well as posting video clips on the officially blocked You-tube site and kept the international community informed as to internal Iranian activities. *Id.*

<sup>76</sup> See *Crisis in Iran Sparks Global Guerilla Cyberwar*, *supra* note 72. It was widely reported that Twitter had been contacted by the U.S. State Department, who asked that they not shut down their systems in Iran. *Id.* Whether this official request occurred or not, the facts are quite clear that the U.S. government did not take any steps to prevent continued Twitter functioning in Iran. See *id.* As such, this example displays a more passive form of cyber strategy used by one nation (the U.S., where Twitter was operating to maintain its functioning capabilities overseas despite the censorship of the Iranian government) against another. Furthermore, by not preventing the postings and provision of information to Iranians by private citizens within the U.S., the U.S. government, again in a purely passive form, may have been getting exactly what it wanted (namely, to provide the Iranian people with the tools and knowledge to circumvent and frustrate efforts by the Iranian government to quell internal domestic discord within their own population).

<sup>77</sup> Ed Barnes, *Stuxnet Worm Still Out of Control at Iran's Nuclear Sites*, *Experts Say*, FOX News (Dec. 9, 2010), <http://www.foxnews.com/scitech/2010/12/09/despite-iranian-claims-stuxnet-worm-causing-nuclear-havoc/>.

<sup>78</sup> See *id.* In this case, the Stuxnet weapon worked to bypass Iranian cyber security programs, assume control of critical systems, and evade detection. *Id.* The program, a highly specialized and advanced form of malicious programming, took over the control systems of the centrifuge in the uranium-processing center in Natanz and disabled the massive nuclear reactor turbine at the Bushehr facility. *Id.*

nuclear program.<sup>79</sup> Iran publicly blamed the U.S. and Israel for the attacks, and has since increased its own efforts to expand the capabilities of its national cyber warfare operations.<sup>80</sup> The Stuxnet attacks on Iran further evidence the utility of cyber warfare operations,<sup>81</sup> the growing willingness to use such attacks, and the

---

<sup>79</sup> See Babak Dehghanpisheh, *Going Cyber Against Nuke Program*, THE DAILY BEAST (Oct. 4, 2010), <http://www.thedailybeast.com/newsweek/2010/10/04/stuxnet-worm-latest-attack-in-growing-cyberwar.html>. The damage inflicted by the Stuxnet program has remained an area of dispute, but Symantec, a major anti-virus software company, has estimated that over 60,000 Iranian operations computers have been infected. *Id.* Further, Ali Akbar Salehi, the head of Iran's Atomic Energy Organization, reported that, as a result of the attack, the nuclear operations at the Bushehr plant have been delayed at least two months. *Id.* Others have indicated that the increased assistance sought by Iran from external software advisors, presumably on how to remove the Stuxnet worm from their systems, indicates just how much damage has been done. See Barnes, *supra* note 77. One leading software advising firm in the U.S. has reported that since the Stuxnet attacks, Iran has supplanted the U.S. as leading traffic requesting information on how to eliminate such malicious programs as the Stuxnet virus. *Id.* In the end, many commentators have concluded that Iran simply does not have the technological advancement and capabilities to overcome such a coordinated and sophisticated cyberattack. *Id.* Ralph Langer, a German cyber expert who has studied the effect of Stuxnet in Iran extensively said that Iran, realistically, would need to "throw out every personal computer involved with the nuclear program and start over, but they can't do that. Moreover, they are completely dependent on outside companies for the construction and maintenance of their nuclear facilities." *Id.* According to Langer, this lack of technological knowledge combined with a lack of domestic production of computer technology may mean that it could be years before Iran's nuclear facilities are functioning normally again. *Id.*

<sup>80</sup> See Barnes, *supra* note 77. The accusations against the U.S. and Israel have been largely unverified, although most agree that the scale, sophistication, and complexity of the Stuxnet attack make it highly likely that a foreign government with advanced cyberwarfare capabilities created the virus. *Id.* After the internal, guerilla-style cyberwarfare that followed the disputed elections in Iran in 2009, Iran launched the Iranian Cyber Army. *Id.* Linked with the Revolutionary Guard's division of the Iranian military forces, this newest branch of the Iranian military has, according to a Revolutionary Guard spokesman, the goal of "conquer[ing] virtual space." *Id.*

<sup>81</sup> See *id.* Analyst Ralph Langer has also addressed the useful advantages demonstrated by the Stuxnet attack, noting that "[w]e didn't see a full-blown war, [and] we didn't see fatalities." *Id.* Further, Langer observes, the attractiveness of cyberattacks such as Stuxnet are also financial: "Stuxnet may have cost somewhere between five and 10 million dollars [to create], that's cheap compared to an air strike or war in the region." *Id.*

extreme uncertainty and difficulty in ascertaining the origins of those attacks.<sup>82</sup>

### III. CYBER WARFARE AND INTERNATIONAL LAW

#### A. *The Applicability of Current International Laws to Cyber Warfare*

At present, international law has yet to fully comprehend the legal ramifications of cyber warfare.<sup>83</sup> As such, international law typically only applies to cyber warfare activities by analogy.<sup>84</sup> The

---

<sup>82</sup> *Id.* While, as Langer points out, the financial benefits of attacks such as Stuxnet are certainly advantages considered by foreign governments considering launching cyberattacks abroad, it is likely that the anonymity afforded by such attacks is the primary draw for foreign governments seeking to inflict mass damage to other nations' Internet-based infrastructures, essentially without consequence because they are unable to be verified as the actual source of that attack. *See Opening Up the Stuxnet Worm*, CYBERANSWERS (Jan. 6, 2011), <http://cyberanswers.org/?p=617>. Security researchers have, in large part, been left "scratching their heads trying to determine the origin of the Stuxnet worm." *Id.* Although many, including Roel Schouwenberg, the senior antivirus researcher at Kaspersky Labs, believe that the sophistication and organization behind both the Stuxnet worm itself and its targets indicate a high probability of foreign state government involvement, there is simply no hard evidence to make such a connection. *Id.* As a result, foreign governments may be able to deliver catastrophic attacks on other states' cyberspace infrastructures and computer-based networks without incriminating themselves.

<sup>83</sup> *See* Scott Shackelford, *Estonia Three Years Later: A progress Report on Combating Cyber Attacks*, 13 No. 8 J. INTERNET L. 23, 26 (2010). Much of the difficulty in establishing an effective legal regime to deal with modern cyber warfare issues arises from the complexity and constantly evolving nature of the technology at the heart of cyber warfare, the general inaccessibility (and perhaps even lack of knowledge of existence altogether) of such technology, and the crucial lack of consistency in the international community regarding what cyber warfare really even entails. *See* Shackelford, *supra* note 3, at 198-99; *see also* Schaap, *supra* note 22 at 125-27; *see generally* Sinks, *supra* note 16, at iii. Consequently, most commentators' views reflect the essential belief that the current international legal framework is, at best, severely underdeveloped. *See* Shackelford, *supra* at 26.

<sup>84</sup> *See* McGavran, *supra* note 25, at 269; Shackelford, *supra* note 3, at 215; *see generally*, Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1037 (2007). Further, and perhaps more alarmingly, it seems that modern and technologically advanced states, including the U.S., are not seeking to take much action to modernize international laws to address the emerging development of cyber warfare (although, it must be noted that many states, as will be considered later in this comment, have



most common attempts to analogize cyber warfare to current international laws have been limited to comparisons between full-scale cyber warfare and nuclear attacks.<sup>85</sup> Attempts have also been made to address cyber warfare through analogy to already-existing international laws and treaties regarding outer space, air space, land, and the sea.<sup>86</sup> However, the analogy between cyber warfare and the international laws governing air, land, and sea are inadequate in terms of their nature and applicability.<sup>87</sup> While violations of air, land, and sea laws may be readily observed and hence prevented, cyberspace is not restricted by the constraints of the physical world.<sup>88</sup> Given the inherent differences between the domains they seek to regulate, international laws currently applicable to these areas are simply not a practical way to address the legality of cyber warfare.<sup>89</sup>

---

shown significant drive to legislate at the domestic level to address the growing capacity for, and use of, weapons of cyber warfare). See McGavran, *supra* note 25, at 269.

<sup>85</sup> Although many commentators have attempted to provide such an analogy-based argument, one of the most complete is that found in Scott Shackelford's *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*. See Shackelford, *supra* note 3, at 217-19. See also Rex Hughes, *Towards a Global Regime for Cyber Warfare*, NATO COOPERATIVE CYBER DEFENSE CENTRE OF EXCELLENCE, [http://www.ccdcoe.org/publications/virtualbattlefield/07\\_HUGHES%20Cyber%20Regime.pdf](http://www.ccdcoe.org/publications/virtualbattlefield/07_HUGHES%20Cyber%20Regime.pdf) (last visited Dec. 11, 2010). According to Shackelford's analysis, the worst results of a full-scale cyber warfare attack are comparable only to the resulting devastation of a full-scale nuclear attack. See Shackelford, *supra* note 3, at 215.

<sup>86</sup> See Shackelford, *supra* note 3, at 219-27. While Shackelford and others have also attempted to relate the international legal treatment of other areas, such as space, air, land, and sea, to cyber warfare, those international laws are based on a domain so distinct from cyberspace (the sole domain in which cyber warfare operates) as to render analogies between the two nearly impossible.

<sup>87</sup> Analogies relating international laws applicable to air, land, and sea fail to adequately address the critical problem with cyber warfare: that cyber warfare ultimately operates in cyberspace, a non-physical domain not subject to conventional forms of legal regulation and compliance monitoring.

<sup>88</sup> See Sinks, *supra* note 16, at 6-7. Although cyber warfare necessarily involves actions occurring across other physical boundaries, or what Sinks calls other linear domains, international laws applicable to those domains (like air, sea, and land) simply function on basic assumptions not applicable to cyber warfare. *Id.* at 7.

<sup>89</sup> *Id.* at 8.

Outer space, while the closest physical analogy to cyberspace, remains a purely physical place.<sup>90</sup> Outer space is readily observable, and hence capable of oversight in a way not possible in the intangible cyberspace domain.<sup>91</sup> International laws limit the use of outer space for military purposes by not allowing weapons of mass destruction, particularly nuclear weapons, to be placed in celestial orbit.<sup>92</sup> These international legal limitations are enforceable because states currently possess the technology to monitor compliance with such rules and regulations: if a state attempts to launch a nuclear weapon into orbit, it would be practically impossible to hide this act from the international community. Yet, in cyberspace, actions are not subject to such readily observable simplicity. Indeed, as we have seen in the cyber attacks on Estonia, it is the effects of cyber warfare, not its actual implementation, which remain visible to the international world. Although there are convincing scientific arguments relating cyberspace to outer space,<sup>93</sup> the principal difference between them—the fact that cyberspace is initiated and results in tangible world effects, while outer space operates at all times in a purely physical, and hence physically observable, world—renders legal application through analogy between the two both impractical and inefficient. In considering international legal restrictions on outer space and cyberspace, the fact remains that a differing basis lies at the heart of each domain. As such, cyberspace must be subject to regulation from

---

<sup>90</sup> See *Outer space*, WIKIPEDIA, [http://en.wikipedia.org/wiki/Outer\\_space](http://en.wikipedia.org/wiki/Outer_space) (last visited Jan. 5, 2010). Although generally defined as a void, outer space is not empty; it contains low densities of physically observable particles. *Id.*

<sup>91</sup> As Shackelford notes, outer space international law does not permit sovereignty claims in space. See Shackelford, *supra* note 3, at 219.

<sup>92</sup> See *id.*

<sup>93</sup> See Rebecca Bryant, *What Kind of Space is Cyberspace?*, MINERVA - AN INTERNET JOURNAL OF PHILOSOPHY, VOL. 5, 2001, <http://www.ul.ie/~philos/vol5/cyberspace.html> (last visited Nov. 29, 2010). Bryant argues that cyberspace and outer space are intimately connected in that they share four primary components that define their existence; namely, each is fundamentally structured around place, distance, size, and route. *Id.* However, despite these theoretical similarities, she concludes that cyberspace cannot be subsumed under a theory of physical space. *Id.* Bryant notes that although cyberspace is intimately connected to the physical world (insofar as cyberspace depends on computer and network structures created and operating within the physical world), it is this intimate connection between the two that also leads to their most basic difference: “physical space, if it exists, depends on nothing at all.” *Id.*

a legal paradigm that accounts for and addresses this ultimate difference.<sup>94</sup>

Meanwhile, analogies between nuclear war and cyber warfare remain, in large part, based upon the similarity in the real world, tangible consequences of each type of warfare.<sup>95</sup> However, the fact that nuclear and cyber warfare have similar consequences in terms of damages and injury does not inexorably lead to the subsequent conclusion that the international laws applicable to nuclear war should also be applied to cyber warfare.<sup>96</sup> In fact, the general ambiguity and uncertainty surrounding the international legality of nuclear warfare seems to suggest the exact opposite; namely, that the existing international legal paradigm is completely inadequate to effectively deal with key issues inherently raised by cyber warfare.<sup>97</sup>

---

<sup>94</sup> It seems that the obvious problem is that no other domain addressed by any legal paradigm will possibly be able to account for this distinction between the physical world and cyberspace, and indeed, this is true. Consequently, as this Comment will conclude, cyber warfare requires a completely new and revolutionary legal approach, hence rendering all attempts at legal analogy inadequate. *See infra* notes 162, 211, 238 (commentators views that a new international legal paradigm may be required to address the legal issues created by cyber warfare operations).

<sup>95</sup> *See* Shackelford, *supra* note 3, at 216. He argues that the kinetic effects of a large-scale cyber warfare attack can be understood only with reference to the historically observable effects of nuclear weaponry and “[a]n all-out [cyber warfare] attack could disable or destroy *all* critical infrastructures, leave the victim nation completely helpless and terrorize its population.” *Id.* at 218. Furthermore, Shackelford argues that cyber warfare and nuclear war similarly do not discriminate between civilians and combatants, and their use is almost inevitably guaranteed to result in some degree of collateral damage. *Id.* at 217-18.

<sup>96</sup> *See Hearing for the Future of Cyber Attack Attribution: Before the H. Science and Technology Subcomm. on Technology & Innovation, 110th Cong. Sess. 1 (2010)*. In this Congressional Hearing, the ramifications of full-scale cyber warfare were distinguished from nuclear war in that while the use of nuclear weapons is prevented by the mutually-assured destruction and deterrence factors, these do not apply in regulation of cyber warfare. *Id.*

<sup>97</sup> *See* Shackelford, *supra* note 3, at 216. While Shackelford is correct to point out that cyber warfare is a concept not specifically addressed by international law (on either a treaty or customary basis), that fact is not a legitimate reason for treating cyber warfare and nuclear war as analogous under international law. As Shackelford admits, the current international law legal regime is, to this day, ambiguous regarding the use of nuclear weapons. *Id.* at 217-18. The fact remains that, more than half a century after their first emergence, nuclear weapons continue to hold an unclear status under international law. *See id.* at 217. The fact that

In the end, the analogy is inadequate by its very nature.<sup>98</sup> As such, these attempts to address perhaps the greatest threat to international security since the development of the atomic bomb<sup>99</sup> require more consideration in order to be truly effective.<sup>100</sup>

---

nuclear weapons remain an unclear concept under international law after such a long time seems to indicate that the international legal community's approach to nuclear weapons has proven to be utterly inadequate. Since their international introduction in 1945 and their first and only wartime uses during World War II, nuclear weapons have perplexed international legal scholars. *See id.* at 217-18. Shackelford notes that the International Court of Justice [ICJ] did attempt to address the international legality of nuclear weapons in the 1996 *Legality of Nuclear Weapons* case, but the opinion was muddled at best. *Id.* The case resulted in an even split (7-7) amongst the court justices and was ultimately decided by the President's tie breaking vote. *See* Commander Robert Green, *Judgment Day at World Court: Nuclear Weapons States Brought to Book*, <http://www.cs.umbc.edu/~nicholas/676/files/197.html> (last visited Sept. 9, 2011). This case indicated that although the use of nuclear weapons would generally be contrary to international law, the court was unable to determine whether nuclear weapons may be permissible in cases of extreme self-defense where the very existence of a state is in jeopardy. *Id.* Ultimately, the inability of international law to adequately define the status of nuclear weapons is not a legitimate reason for seeking to analogize them to cyber warfare. If anything, international law and its inability to deal with nuclear weapons indicates that new international legal strategies need to be employed when dealing with cyber warfare to avoid the same legal ambiguity that remains such a problem with nuclear warfare.

<sup>98</sup> *See infra* notes 158-60 (discussing the specific problems with seeking to use analogy as a legal tool).

<sup>99</sup> *See* Paul Woodward, *Stuxnet: The Trinity Test of Cyber warfare*, WAR IN CONTEXT (Sept. 23, 2010), <http://warincontext.org/2010/09/23/stuxnet-the-trinity-test-of-cyberwarfare/>. Woodward believes that the recent Stuxnet attacks in Iran were the first major cyber warfare action taken on an international level between states. *Id.* He further states that this attack is as critical as the first nuclear weapons test conducted by the United States, code-named "Trinity," although he ultimately believes that it is more likely that Israel, and not the United States, was directly responsible for the attack. *Id.* Woodward calls Stuxnet a "cyber missile" and implies that the damage caused by such a weapon could trigger "Chernobyl-like catastrophe, or the entire destruction of [a nation's] conventional energy grid." *Id.* Further, Woodward notes that many feel that the relationship between the Stuxnet cyber weapon and nuclear weapons extends further to the basic mechanisms by which each devastating weapon self-regulates and prohibits its use; namely, through deterrence. *Id.* However, Woodward instead views Stuxnet as indicative of a show of global strength by Israel (who Woodward believes is ultimately behind the attack) both of their advanced cyber warfare capabilities and, critically, their willingness to utilize such capabilities. *Id.* Woodward finally believes that the weapons of cyberwarfare are even more problematic than nuclear weapons because

In the past decade, attempts to legally regulate cyber warfare operations have become increasingly common as individual nations recognize both the undeniable proliferation of cyber warfare technology and the immediacy of the threat posed by such proliferation.<sup>101</sup> There have been numerous domestic attempts to address various aspects of cyber warfare within prominent states functioning as global leaders in cyber warfare development and technology.<sup>102</sup>

Within the U.S., domestic responses to cyber warfare threats have been steadily increasing since the mid-1990s and Department of Defense funding for cyber warfare related intelligence nearly doubled from 1998 to 2001.<sup>103</sup> The origins of the U.S. cyber warfare regulation began as far back as 1988 when the government formed

---

of their ease of proliferation and use amongst several state and private actors. *Id.*; see generally Sir Robert Fry, *Fighting Wars in Cyberspace*, WALL STREET J. (July 21, 2010), <http://online.wsj.com/article/SB10001424052748703724104575379343636553602.html>. Fry, a former Deputy Commanding General of coalition forces in Iraq and currently chairman of a business consultancy, believes that cyber warfare is, on the whole, an even greater threat to global security than nuclear weapons. *Id.* He notes that cyber warfare, much like nuclear weapons, is ultimately capable of causing “instantaneous failure of the systems that animate and sustain modern life . . . [a]t a stroke, computer systems, power grids, industrial production and financial markets could fail, with untold consequences for civil governance and social cohesion: an electronic Pearl Harbor and all without a conventional shot being fired.” *Id.* Such a devastating cyber warfare attack is not “academic hypothesis,” Fry warns, but a very real possibility, especially given the ease with which cyber weaponry can proliferate. *Id.* Ultimately, Fry concludes, “[c]yber operations are the next weapons of mass effect, or, as more than one wag has put it, ‘weapons of mass disruption.’ Whereas nuclear weapons have been used twice in human history, cyber weapons are employed daily.” *Id.*

<sup>100</sup> See Fry, *supra* note 99. Although Fry does concede that cyber warfare may, similarly to nuclear proliferation and use, remain subject to principles of deterrence, he ultimately believes that this form of self-regulation is inadequate. *Id.* In order to address the novel and devastating potential of cyber warfare, Fry concludes, there is “an existential need to create some form of regulatory system that allows more than implicit deterrence. This will not be easy.” *Id.*

<sup>101</sup> See McGavran, *supra* note 25, at 268-69.

<sup>102</sup> See Shackelford, *supra* note 83, at 23.

<sup>103</sup> See generally Anthony H. Cordesman, *Defending America – Redefining the Conceptual Borders of Homeland Defense: Terrorism, Asymmetric Warfare, And Nuclear Weapons*, CSIS PUBLICATIONS (Feb. 14, 2001), <http://csis.org/files/media/csis/pubs/terrorasymw&nucl.pdf>.

the first cyber emergency response team (“CERT”) at Carnegie Mellon University.<sup>104</sup> CERT was formed in response to a growing number of cyber based attacks on government networks and computer infrastructures.<sup>105</sup> In its first year of operation, CERT investigated six cases of computer security invasions.<sup>106</sup> Presently, the successor to CERT, the U.S. Cyber Emergency Response Team (“USCERT”) operates as a department of Homeland Security and handles well over 50,000 such investigations annually.<sup>107</sup> The U.S. Air Force took over much of the nations’ cyber warfare operations in 2005, and the Air Force mission statement was even altered to reflect the addition of cyberspace as an Air Force battlefield.<sup>108</sup> In 2009, the U.S. launched the next phase of its cyber defense scheme, the U.S. Cyber Command (CYBERCOM), which was created to unify various government departments and agencies dealing with national cyber warfare strategy.<sup>109</sup> Subsequently, President Obama appointed a permanent cyber czar to deal with national cyber warfare policies on a more cohesive scale.<sup>110</sup> However, many feel that this newly created post remains heavy on responsibility but fairly light in terms of actual authority.<sup>111</sup> Most recently, U.S. Senator Joe Lieberman introduced a piece of cyber security legislation that would grant the President broad powers of control over the national Internet infrastructure in

---

<sup>104</sup> See Shackelford, *supra* note 83, at 23.

<sup>105</sup> See *id.*

<sup>106</sup> See *id.*

<sup>107</sup> See *About Us*, United States Computer Emergency Readiness Team (US-CERT), <http://www.us-cert.gov/aboutus.html> (last visited Dec. 12, 2010). See also Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, CERT COORDINATION CENTER 5 (Nov. 2002), <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408853&Location=U2&doc=GetTRDoc.pdf>.

<sup>108</sup> See Staff Sgt. C. Todd Lopez, *Cyber Summit begins at Pentagon Nov. 16*, AIR FORCE PRINT NEWS (Nov. 15, 2006), <http://www.af.mil/news/story.asp?id=123032005>.

<sup>109</sup> See U.S. Cyber Command Factsheet, UNITED STATES STRATEGIC COMMAND, [http://www.stratcom.mil/factsheets/Cyber\\_Command](http://www.stratcom.mil/factsheets/Cyber_Command) (last visited Jan. 14, 2010).

<sup>110</sup> See Ellen Nakashima, *Obama to name Howard Schmidt as cybersecurity coordinator*, WASH. POST (Dec. 22, 2009), <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html>.

<sup>111</sup> See *id.*

cases of cyber attack emergencies.<sup>112</sup> Although various privacy concerns regarding the proposed bill have been raised, such proposals evidence the increasing willingness of domestic legislatures to directly address cyber warfare issues within their domain.<sup>113</sup> Finally, in July of 2010, the U.S. House of Representatives held a hearing to consider the implications of cyber warfare in terms of state attribution and the potential role of deterrence in preventing cyber warfare.<sup>114</sup>

The U.S. is not the only global power to recently address cyber warfare issues on a domestic scale. In China, cyber warfare has been a primary military concern and goal for several years. As far back as 1999 the PLA Daily, the official media outlet of the People's Liberation Army of China, reported, "[i]nternet warfare is of equal significance to land, sea, and air power and requires its own military branch."<sup>115</sup> Reports by various U.S. intelligence agencies have likewise concluded that the Chinese military is both expanding its cyber warfare capabilities and simultaneously exploring offensive cyber warfare strategies and weaponry.<sup>116</sup> Over the years, there have been several claims that China has attacked U.S. based targets via cyber warfare weaponry, although the vast majority remain

---

<sup>112</sup> See PROTECTING CYBERSPACE AS A NATIONAL ASSET ACT OF 2010, S. 3480, 111TH CONG. (2010), available at <http://www.opencongress.org/bill/111-s3480/text>. See also Donny Shaw, *Lieberman Cybersecurity Bill Would Give DHS Broad Emergency Powers Over the Internet*, OPENCONGRESS BLOG (June 14, 2010), <http://www.opencongress.org/articles/view/1917-Lieberman-Cybersecurity-Bill-Would-Give-DHS-Broad-Emergency-Powers-Over-the-Internet>.

<sup>113</sup> See *Protecting Cyberspace as a National Asset Act of 2010*, supra note 112; see also Shaw, supra note 112.

<sup>114</sup> See *Hearing on Planning for the Future of Cyber Attack Attribution: Before the H. Sci. and Tech. Subcomm. on Tech. and Innovation*, 110th Cong. Sess. 1 (July 15, 2010), available at <http://science.house.gov/hearing/subcommittee-technology-and-innovation-hearing-cyber-attack-attribution>.

<sup>115</sup> See Kevin B. Alexander, *Warfighting in Cyberspace*, JOINT FORCES Q., July 31, 2007, at 58-59, available at <http://www.military.com/forums/0,15240,143898,00.html>. See also Schaap, supra note 22, at 132-33.

<sup>116</sup> See U.S. DEPT. OF DEF. ANNUAL REPORT TO CONGRESS: MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 21 (2007), available at <http://www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf>; Kevin Coleman, *China's Cyber Forces*, DEFENSE TECH.ORG (May 8, 2008), <http://defensetech.org/2008/05/08/chinas-cyber-forces/#more-2831>.

unconfirmed, and China has denied any responsibility for such attacks.<sup>117</sup>

Additionally, Russia has established itself as a leader in cyber warfare technology, and has become dedicated to utilizing cyber warfare strategy to increase the effectiveness of more traditional forms of military prowess.<sup>118</sup> Russia, like China, has been accused of involvement in several global instances of cyber attacks, but they have denied any such actions and no definitive proof of their participation has been established.<sup>119</sup> Russia's domestic approach to cyber warfare has been split between several government and military agencies seeking to protect critical Russian cyberspace infrastructure while concurrently developing offensive cyber warfare strategies to attack the vulnerable infrastructures of enemies of the State.<sup>120</sup> Despite these various domestic efforts, the concept of cyber warfare generally is, by its nature, a global issue that may only be effectively addressed at the international level.<sup>121</sup>

Global responses to cyber warfare remain in their infancy; yet, there has been an increasing trend amongst international organizations to address this growing issue.<sup>122</sup> In particular, three

---

<sup>117</sup> See Siobhan Gorman, *Electricity Grid in US Penetrated by Spies*, WALL STREET J. (Apr. 8, 2009), <http://online.wsj.com/article/SB123914805204099085.html>.

<sup>118</sup> See Kevin Coleman, *Russia's Cyber Forces*, DEFENSETECH.ORG (May 27, 2008), [http://www.defensetech.org/archives/cat\\_cyberwarfare.html](http://www.defensetech.org/archives/cat_cyberwarfare.html); see also Schaap, *supra* note 22, at 133.

<sup>119</sup> See Shackelford, *supra* note 83, at 24-5.

<sup>120</sup> See Timothy L.I. Thomas, *Russia's Information Warfare Structure: Understanding the Roles of the Security Council, Fapsi, the State Technical Commission and the Military*, 7 EUR. SEC. 156 (Spring 1998), available at <http://www.tandfonline.com/doi/abs/10.1080/09662839808407354#preview>; see also Shackelford, *supra* note 83, at 25.

<sup>121</sup> Warfare, in its most basic global understanding, is defined as "a contest between two or more independent nations [sic] carried on by authority of their respective governments." *War*, THE 'LECTRIC LAW LIBRARY, <http://www.lectlaw.com/def2/w038.htm> (last visited Jan. 12, 2010). Although domestic consideration of cyber warfare issues is important, international law requires a more globally applicable approach to cyber warfare to which the entire global community can derive an understanding of cyber warfare's legality and limitations.

<sup>122</sup> See Shackelford, *supra* note 3, at 243-44; see also Malawer, *supra* note 13, at 28.



international agencies have officially addressed cyber warfare, to varying degrees, over the past few years.<sup>123</sup>

First, in 2001, the European Union (EU) sought to address the growing problems of cyberspace crimes and illegal Internet activities through the EU Council Convention on Cybercrime.<sup>124</sup> Although created under the initiative of the European Union, the convention in Budapest, which resulted in the extensive Cybercrime treaty, was signed by forty-one nations, including the U.S., Canada, and Japan.<sup>125</sup> Not only was this treaty the first international agreement directly addressing cyberspace-related global legal issues, but it specifically stressed the importance of reconciling domestic policies and establishing a globally unified regime of international cooperation to deal with cyberspace crimes.<sup>126</sup> However, the EU Convention does not apply to cyber warfare, and, in fact, its criminal liability for cyberspace crimes specifically does not extend to actions undertaken in accordance with lawful government authority.<sup>127</sup> Although the primary aim of the EU Convention on Cybercrime is criminal activity online, and not cyber warfare, it nonetheless remains a valuable indication of the willingness of the world's global powers to cooperate in modifying and expanding the application of international law to issues of legal regulation in cyberspace.<sup>128</sup> It remains critically important that global nations and organizations such as the EU and U.S. start to work together to address issues

---

<sup>123</sup> See Shackelford, *supra* note 3, at 243-44; see also Malawer, *supra* note 13, at 28.

<sup>124</sup> See Council of Europe, Convention on Cybercrime, Additional Protocol/ Explanatory Reports, Nov, 23, 2001, C.E.T.S 185, available at <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>.

<sup>125</sup> See Ira Piltz, *Internet law- European Union's Convention on Cyber crime (ets no. 185):Cybercrime: First International Treaty on Crimes Committed via the Internet*, COMPUTER CRIME RESEARCH CENTER (Jan. 22, 2008), <http://www.crime-research.org/news/22.01.2008/3144/>.

<sup>126</sup> See *id.*; Tom Espiner, *US joins European cybercrime convention*, ZDNET UK BLOG (Oct. 2, 2006, 1:30 PM), <http://www.zdnet.co.uk/news/security-management/2006/10/02/us-joins-european-cybercrime-convention-39283761/>.

<sup>127</sup> See Schaap, *supra* note 22, at 171-72.

<sup>128</sup> See Alain Megias, *European Union Policies Regarding Cybercrime*, INTERNET BUSINESS LAW SERVICES (Jan. 22, 2011), <http://www.i-policy.org/2011/01/european-union-policies-regarding-cybercrime.html>.

which deal with the cyberspace domain and which have not, up to this point, been explicitly addressed by international laws.<sup>129</sup> The formation of such treaty agreements not only creates binding international legal obligations upon signatory states, but if acceded to by enough of the global community, could also become binding customary international law.<sup>130</sup>

Second, in 2002 and again in 2007, the North Atlantic Treaty Organization (NATO) held summits in which the implications of cyber warfare were a primary concern.<sup>131</sup> In 2002, NATO held a summit in Prague where it first began to consider the importance of cyber defense.<sup>132</sup> Although the Prague summit began NATO discussions of cyber warfare and its potential impact on the global community, it was after the 2007 cyber attack on Estonia that the need to expand on the 2002 summit became readily apparent.<sup>133</sup> After numerous cyber attacks crippled their electronic infrastructures, Estonia, a NATO member, officially requested NATO assistance in defense of its digital assets.<sup>134</sup> NATO responded by sending cyber specialists to Estonia, but did not accomplish much in terms of aiding Estonia or regulating the Internet-based weapons being used against them.<sup>135</sup> Ultimately, some have concluded that the NATO response, or lack thereof, “illustrated the lack of a coherent NATO cyber doctrine and strategy.”<sup>136</sup> Following the attacks on Estonia, NATO held another summit, this time in Bucharest a year later, to reconsider the growing problem of cyber warfare.<sup>137</sup> The Bucharest summit dealt with how the alliance should specifically respond to cyber

---

<sup>129</sup> *Id.*

<sup>130</sup> See DAVID HARRIS, CASES AND MATERIALS ON INTERNATIONAL LAW 38-40 (Sweet and Maxwell, 7th ed. 1998).

<sup>131</sup> See *Defending against cyber attacks*, NATO/OTAN (Jun. 24, 2011), [http://www.nato.int/issues/cyber\\_defence/index.html](http://www.nato.int/issues/cyber_defence/index.html).

<sup>132</sup> *Id.*

<sup>133</sup> See Shackelford, *supra* note 83, at 25-26.

<sup>134</sup> See Rex B. Hughes, *NATO and Cyber Defense: Mission Accomplished?*, NATO/OTAN (Apr. 2009), <http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf>.

<sup>135</sup> See Shackelford, *supra* note 83, at 25.

<sup>136</sup> See *id.*; Hughes, *supra* note 134, at 10-11.

<sup>137</sup> See Shackelford, *supra* note 83, at 25.

warfare and § 47 of the Bucharest Summit Declaration stated, "NATO remains committed to strengthening key alliance information systems against cyber attacks."<sup>138</sup>

As a result of this summit, NATO developed a Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia to address defending against and countering advanced cyber attacks.<sup>139</sup> Also, the Bucharest summit resulted in the creation of the Cyber Defense Management Authority in Brussels.<sup>140</sup> This authority represents a centralized NATO cyber defense strategy and seeks to merge national and private sector cyber defense elements.<sup>141</sup> The essential NATO cyber warfare defense strategy remains under the control of the North Atlantic Council and, at present, it seems that cyber warfare would only activate NATO treaty Article 4, requiring NATO members to consult one another to determine a response to a cyber attack against NATO members.<sup>142</sup> This also means that Article 5 of the NATO treaty would not be applicable to instances of cyber attack against a NATO member; hence, other NATO treaty nations would not be required under the treaty obligations to assist the attacked nation in combating against such cyber warfare.<sup>143</sup> Thus, although NATO has begun to concretely address the issues raised by the increasing threat of cyber warfare, several additional steps are still required before NATO can sufficiently deal with countering and

---

<sup>138</sup> See Bucharest Summit Declaration, Section 47, North Atlantic Treaty Organization, April 3, 2008, available at [http://www.nato.int/cps/en/natolive/official\\_texts\\_8443.htm](http://www.nato.int/cps/en/natolive/official_texts_8443.htm).

<sup>139</sup> See Shackelford, *supra* note 83, at 25; see also *NATO Opens New Centre of Excellence on Cyber Defense*, NATO NEWS (May 20, 2008), <http://www.nato.int/docu/update/2008/05-may/e0514a.html>.

<sup>140</sup> See Ian Grant, *NATO Sets Up Cyber Defense Management Authority in Brussels*, ComputerWeekly.com BLOG (Apr. 4, 2008, 4:22pm), <http://www.computerweekly.com/Articles/2008/04/04/230143/nato-sets-up-cyber-defense-management-authority-in-brussels.htm>.

<sup>141</sup> See *id.* See also Shackelford, *supra* note 83, at 25.

<sup>142</sup> See Grant, *supra* note 140; see also Shackelford, *supra* note 83, at 25. See also *Defending against cyber attacks*, NATO NEWS (Jan. 29, 2009), [http://www.nato.int/cps/en/natolive/topics\\_49193.htm](http://www.nato.int/cps/en/natolive/topics_49193.htm).

<sup>143</sup> See *NATO agrees on common approach to cyber defense*, EURACTIV.COM (Apr. 4, 2008), <http://www.euractiv.com/infosociety/nato-agrees-common-approach-cyber-defence/article-171377>.

addressing cyber warfare.<sup>144</sup> Furthermore, although NATO policy may be unofficially indicative of the stance of a large portion of the international community, it does not ultimately reflect general international law. Hence, even if NATO were to explicitly address cyber warfare activities, it is doubtful that such organizational doctrine would evince international law on that subject.<sup>145</sup>

Finally, just last year, the U.N. began to take a definite, albeit unofficial, recognition of the pressing concerns associated with cyber warfare proliferation.<sup>146</sup> While the official U.N. policy regarding cyber warfare remains unclear, most commentators maintain that cyber warfare may be somewhat susceptible to treatment under established U.N. Charter provisions, and there has been an increasing tendency for individual agencies and high-level U.N. officials to voice their concerns with the growing cyber warfare issue.<sup>147</sup> In January of last year, the U.N. International Telecommunications Union Secretary General, Hamadoun Touré, spoke at the World Economic Forum debate, noting that “cyber war would be worse than a tsunami—a catastrophe.”<sup>148</sup> Touré then proposed that an international treaty should be formed to prevent the outbreak of such a war.<sup>149</sup> The treaty should, according to Touré, center around a global agreement that nations would not utilize cyber warfare as a first strike weapon.<sup>150</sup> Others, such as former director of US intelligence John Negroponte, have expressed severe reservations regarding the creation of such a cyber warfare treaty.<sup>151</sup> Still others have called for a global alliance or agency to address the issues of cyber warfare, including Microsoft chief research and strategy officer Craig Mundie, who has advocated for the creation of a World Health

---

<sup>144</sup> See Shackelford, *supra* note 83, at 25.

<sup>145</sup> See *id.*

<sup>146</sup> See AFP, *UN Chief Calls for Treaty to Prevent Cyber War*, GOOGLE NEWS (Jan. 30, 2010), <http://www.google.com/hostednews/afp/article/ALeqM5h8Uvk-jpSvCWT-bqYSg1Ws4I4yAA>.

<sup>147</sup> See *id.*

<sup>148</sup> *Id.*

<sup>149</sup> *Id.*

<sup>150</sup> *Id.*

<sup>151</sup> *Id.*

Organization for the Internet.<sup>152</sup> Mundie went so far as to suggest that a “driver’s license” for Internet users may be a useful step towards securing the cyberspace domain and preventing illegal and destructive online incidents.<sup>153</sup>

While the recent statements from Touré have not been confirmed as indicative of any official U.N. policy or stance, they are nonetheless compelling evidence that the U.N. has begun to consider cyber warfare as a legitimate global issue worthy of consideration. In the meantime, it seems that the current U.N. Charter provisions might continue to be imperfectly applied to some instances of cyber warfare.<sup>154</sup> In fact, Walter Gary Sharp, the editor of the United Nations Peace Operations, recently stated in his book, *Cyberspace and the Use of Force*, that traditional international law explicitly covers cyber warfare.<sup>155</sup> Sharp concluded that cyber warfare activities fall within the armed attack category, and hence should remain subject to customary international law and U.N. Charter provisions dealing with such use of illegal force.<sup>156</sup>

While these attempts to address the international legality of cyber warfare are a positive step in the right direction, they remain fundamentally flawed in that each attempt ultimately operates within

---

<sup>152</sup> *Id.*

<sup>153</sup> *Id.* See also Brian D. Hill, *UN agency calls for global cyber warfare treaty, ‘driver’s license’ for Web users*, U.S.W.G.O. (Feb. 1, 2010), [uswgo.com/un-agency-calls-for-global-cyberwarfare-treaty-drivers-license-for-web-users.htm](http://uswgo.com/un-agency-calls-for-global-cyberwarfare-treaty-drivers-license-for-web-users.htm).

<sup>154</sup> See, e.g., Shackelford, *supra* note 3, at 244-47 (arguing that U.N. resolutions and the U.N. Charter generally may remain applicable to some instances of cyber warfare); Dondi S. West, *A Survey and Examination of the Adequacy of the Laws Related to Cyber Warfare*, <https://www.defcon.org/images/defcon-18/dc-18-presentations/West/DEFCON-18-West-Laws-Cyber-Warfare-WP.pdf> (last visited Oct. 25, 2010) (a presentation arguing that the current rules of international law, embodied within the U.N. Charter, are sufficient to address the emerging issues of cyber warfare); Schaap, *supra* note 22, at 148-50 (arguing that customary international laws of war, combined with the U.N. Charter provisions on “use of force,” may apply to cyber warfare).

<sup>155</sup> WALTER GARY SHARP, SR., *CYBERSPACE AND THE USE OF FORCE* 234-35 (Aegis Research Corp. 1999).

<sup>156</sup> *Id.*; see also Sinks, *supra* note 16, at 22-23.

the confines of an international legal structure that is ill-equipped to deal with the advanced issues raised by questions of cyber warfare.<sup>157</sup>

In the end, the proposed use of analogy to govern the legality of cyber warfare is a problematic proposition at best and, at worst, a very dangerous suggestion.<sup>158</sup> While the use of analogy has remained

---

<sup>157</sup> Despite the inadequacy of the current global attempts of the international community to address issues of cyber warfare legality, as this comment argues, the fact nonetheless remains that attempts such as those mentioned in this section do evidence the fact that key international organizations are treating these cyber warfare issues as a present concern. As U.S. General Wesley Clark recently warned, cyber warfare is such an irregular and unfamiliar form of military attack that it may be “tempting for policymakers to view cyber warfare as an abstract future threat.” Wesley K. Clark & Peter L. Levin, *Securing the Information Highway: How to Enhance the United States’ Electronic Defenses*, Foreign Affairs, Nov.-Dec. 2009, at 2. Nonetheless, as will be argued in this comment in more detail in the subsequent sections, the fact remains that global leaders considering the legality of cyber warfare must also recognize that the existing international law paradigm is inherently inadequate to address cyber warfare because it remains based on presumptions that simply do not hold true for the unique area of cyber warfare operations. See Amit, *supra* note 24, at 7 (noting that it is obvious that conventional understandings of combat and battlefield simply do not pertain to considerations of cyber warfare).

<sup>158</sup> The concept of analogy generally has always been a problematic idea. Since its first use by the Greeks in mathematical formulations, the concept of analogy has been thought of primarily as a cognitive function used for transferring a meaning from one subject to another target subject. See *Analogy*, WIKIPEDIA, <http://en.wikipedia.org/wiki/Analogy> (last visited Dec. 10, 2010). By its nature, analogy is merely a comparison of two dissimilar things; it is a cognitive tool designed to relate two objects in a way that our minds can adequately comprehend. *Id.* The value of analogy, however, has been questioned since its first use; great philosophers such as Plato, though using analogy in many of their discourses, continually warned against its inherent inadequacy. Amelie Frost Benedikt, *Runaway Statues: Platonic Lessons on the Limits of an Analogy*, PAIDEIA PROJECT ON-LINE, <http://www.bu.edu/wcp/Papers/Anci/AnciBene.htm> (last visited Oct. 10, 2010). Plato used analogy in nearly all of his famous dialogues; it was in the *Meno* that Plato both utilized and distanced himself from his interlocutor’s use of analogy to understand the relationship between knowledge and opinion. *Id.* Although Plato recognized that analogy is a useful and indispensable tool in philosophic discourse, he simultaneously understood that analogy remains limited in its ability and practical usefulness, and so reminded his readers not to overzealously follow or apply the concept. *Id.* In the end, the use of analogy, in any context, remains a difficult thing; as Plato observed rightly so long ago, we must be wise in understanding when it applies, when it does not, and to what degree its applicability should be accepted.

a commonly accepted form of judicial reasoning,<sup>159</sup> it is ultimately little more than a self-regulating legal tool used to resolve disputes for which no actual, independent rules of law have formed.<sup>160</sup> Furthermore, global attempts to operate within the framework of existing international law have proven insufficient in addressing the legality of cyber warfare.<sup>161</sup> Instead of futilely attempting to analogize the current international legal paradigm to accommodate cyber warfare, a more active role needs to be adopted by the international community.<sup>162</sup> The critical first step in taking such a proactive approach to establishing the international legality of cyber warfare must be the formation of a definite understanding of the most fundamental legal issues raised by the emergence of cyber warfare.<sup>163</sup> Only by identifying and understanding the inability of current

---

<sup>159</sup> See GIORGIO DEL VECCHIO, GENERAL PRINCIPLES OF LAW 12 (1986).

<sup>160</sup> *Id.* at 14-15. As del Vecchio notes, analogy, in its legal use, remains limited insofar as it only applies when there is substantial similarity between the instant case and the cases to which the legal rule of law being analogized applies. *Id.* at 15. Ultimately, he concludes, the law has regulated the use of analogy because, as a general matter of law and of logic, jurisprudence has come to realize that despite the value of analogies in solving cases, the simple fact remains that often analogy alone remains insufficient to actually solve the instant case. *Id.* at 14.

<sup>161</sup> See Steven A. Hildreth, *Cyberwarfare*, CONG. RESEARCH SERV., RL30735 9 (June 19, 2001), available at <http://www.dtic.mil/cgibin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA398642>. Hildreth concludes that, given the pervasive uncertainty associated with attempting to define cyber warfare operations within the present international law paradigm, "there is little likelihood that the international community will soon generate a coherent body of information operations law." *Id.*

<sup>162</sup> See Shackelford, *supra* note 3, at 246. Although the basis of Shackelford's article is the analogizing of current international laws and treaties to cyber warfare operations, even he ultimately concedes that these analogies are not a "panacea" for the numerous and complex issues associated with the emergence of cyber warfare. *Id.* In the end, Shackelford recognizes that cyber warfare ultimately will require the "creation of a [new] legal regime" to deal explicitly with cyber warfare. *Id.* It is exactly the creation of such a newly formed international legal paradigm, specifically addressing the three primary problems with the former international law regime, which constitutes the final part of this comment.

<sup>163</sup> *Id.* See also Kanuck, *supra* note 26, at 286-87. As Kanuck observes, cyber warfare has done more than merely alter our perceptions of what constitutes military activity and armed attack; it has fundamentally and forever altered and redefined the battlefield in which military operations occur. *Id.* Consequently, international laws applicable to such military activities need not be based on our prior conceptions of what limitations defined that battlefield. *Id.*

international law to deal with cyber warfare can the global community begin to formulate new and effective legal solutions to effectively address the revolutionary legal issues posed by cyber warfare.<sup>164</sup>

### *B. Inadequacies of Current International Laws*

Presently, international law is unable to deal with three key legal issues raised by cyber warfare: the problems of attribution, jurisdiction, and “use of force.” These paramount considerations are problematic in the cyber warfare context because they make clear the fundamental flaw in attempting to apply current international law to cyber warfare: international law naturally assumes it can be made applicable to any type of military strategy, however, the reality is that cyber warfare cannot be adequately addressed by the existing paradigm and structure of international law.<sup>165</sup>

#### 1. Attribution Problem

The most commonly identified challenge that cyber warfare poses for the present international legal regime is the concept of attribution.<sup>166</sup> The concept of attribution—the question of whose acts are attributable to a sovereign national State—is a critical question in

---

<sup>164</sup> *Id.* at 287-88.

<sup>165</sup> *See id.* at 283. The idea that the presently existing international legal regime is inherently insufficient to cope with issues raised by modernized cyber warfare operations has been argued to be based solely on the fact that cyber warfare operations involve the melding of military target and military information into one entity. *Id.* This argument is simply stating that international law is predicated on the belief that such law addresses the means of military strategy employed by global powers; when, as in cyber warfare, the means employed and the ends sought are the same (namely the destruction of information), the traditional concept of war becomes inapplicable, and international law ceases to be of any real value. *Id.*

<sup>166</sup> Sean M. Condon, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. L.J. & TECH. 403, 414 (2007); *see also* Shackelford, *supra* note 3, at 233; Steven Fox, *Cyber Warfare and Attribution*, CSO (July 16, 2009, 9:03 PM), [http://blogs.csoonline.com/cyber\\_warfare\\_and\\_attribution](http://blogs.csoonline.com/cyber_warfare_and_attribution); Kevin Coleman, *The Challenge of Attribution in Cyber War; Bring on the Lawyers*, DEFENSE TECH (Sept. 7, 2010), <http://defensetech.org/2010/09/07/the-challenge-of-attribution-in-cyber-war/>; Sinks, *supra* note 16, at 2.



present international law for two reasons. First, identifying the source of an attack allows the victim to make an appropriate response against that party without threatening innocent collateral damage, and second, the right of reprisal and self-defense of a State that is the victim of a cyber attack largely depend on whether the identity of the attacker can be definitively determined.<sup>167</sup>

The recent events surrounding the controversial 2009 Iranian elections, discussed earlier in this comment, provide a better context for considering the real world problems of attribution in cyber warfare operations.<sup>168</sup> According to Matthew Burton, a former U.S. intelligence analyst who has since joined those providing valuable cyber knowledge to the Iranian opposition, “[we have] turned our collective power and outrage into a serious weapon that we could use at our will . . . [w]e practiced distributed, citizen-based warfare.”<sup>169</sup> Are the actions of national citizens online, in efforts to assist foreigners rebelling against their local governments, attributable to the nation in which those providing the assistance reside?<sup>170</sup> Are the actions attributable to the nation in which those providing assistance are maintaining their computer operations and server information? Are the actions attributable to all the nations through which those

---

<sup>167</sup> See Condon, *supra* note 166, at 414.

<sup>168</sup> Noah Shachtman, *Web Attacks Expand in Iran's Cyber Battle*, WIRED (June 16, 2009, 4:06 PM), <http://www.wired.com/dangerroom/tag/media-war/>. See *supra* notes 75-76 (detailing the potential involvement of other States, and the documented involvement of private parties operating outside Iran, in the internal cyber battles between the Iranian government and local factions who remained dissatisfied with the national elections); see also *supra* note 70.

<sup>169</sup> *Crisis in Iran Sparks Global Guerilla Cyberwar*, *supra* note 72.

<sup>170</sup> See *id.* In the Iranian elections scenario, private individuals and bloggers from across the globe posted information to assist elements within Iran to dodge censorship. *Id.* Other international bloggers have sought to assist local Iranians opposed to the recent elections by altering their server location in order to interfere with local Iranian attempts to subdue online propaganda within Iran; there has even been a report that one American blogger posted instructions on how to disable official Iranian websites. *Id.* Would such acts by a party operating within the U.S. be attributable to the U.S. government? If it were, severe implications would arise for both Iran – which would likely hold the U.S. government directly responsible for such acts as, at the very least, attempts to disrupt internal order and, at worst, acts of war – and the U.S. – who would likely, in order to avoid Iranian reprisals and international sanctions, need to strictly regulate private citizen access to the Internet and ability to post such materials.

providing the assistance need to have their cyberspace information travel? These are the complex, and often dizzying, questions and issues related to the relationship between cyber warfare operations and State attribution that require consideration from an legal regime.

Traditionally, attribution under the present international law regime is subsumed into the more generalized category of state responsibility.<sup>171</sup> According to the International Law Commission (ILC) Draft Articles on State Responsibility, the actions of a non-state organization may be attributed to the State in a variety of circumstances.<sup>172</sup> However, it is the concept of attribution established under Article 8 of the ILC Draft Articles that poses the most critical consideration for cyber warfare operations by private individuals.<sup>173</sup> Under this article, a State may be held liable for the cyber warfare activities of private individuals and organizations if it can be shown that the person or persons were acting on behalf of the State

---

<sup>171</sup> See generally Harris, *supra* note 130, at 484. Within this large area of state responsibility, Harris considers whether the actions of individuals and non-government agencies and organizations are attributable to the state government (and hence that state government can be held internationally accountable for the consequences of those actions, under international law, as though the acts were their own) in terms of what he calls "imputability." *Id.* at 499.

<sup>172</sup> *Id.* Under Article 5 of the ILC Draft Articles, the conduct of any state organ, having that status under internal, domestic law, shall entail responsibility of the state generally if they are acting within their capacity as such at the time of the action in question. *Id.* Further, under Article 6, a state organ's acts will be attributable to the state regardless of what area of the state it is involved in, and without regard to how superior or subordinate its role in the state generally is. *Id.* Lastly, under Article 7, organizations and agencies serving as either territorial governments or which are not formally part of the state government structure, but are nonetheless empowered by law to exercise aspects of governmental authority, shall also entail state responsibility. *Id.*

<sup>173</sup> See *id.* at 500. Article 8 states as follows:

The conduct of a person or a group shall also be considered as an act of the State under international law if

(a) it is established that such person or group of persons was in fact acting on behalf of that State; or

(b) such person or group of persons was in fact exercising elements of the governmental authority in the absence of the official authorities and in circumstances which justified the exercise of those elements of authority. *Id.*

government.<sup>174</sup> In the cyber warfare context, this remains both an impractical and dangerous method for determining attribution. The ease with which cyber warfare activities can be carried out,<sup>175</sup> combined with the inability to generally prove, with any sense of definiteness, the ultimate source of a cyber attack, makes this method of attribution severely insufficient.<sup>176</sup>

Ultimately, present international law seeks to address state responsibility and imputability (or attribution) either by making States strictly liable for internationally unlawful conduct originating from within its borders and organizations,<sup>177</sup> or by considering whether a State is subjectively liable for intentionally breaching established international laws.<sup>178</sup> Regardless of which approach is

---

<sup>174</sup> The notion of state imputability becomes even more expansive when taking into account International Court of Justice (ICJ) case law and international arbitration rulings interpreting state responsibility and attribution. Specifically, in both *Caire Claim* and *Youmans Claim*, it was held that state responsibility would extend to state actors even when those actors were acting beyond the scope of their state given authority. *See id.* at 492, 507. In the *Caire Claim* case, an international claims commission concluded that the actions of Mexican military personnel would be attributed to the Mexican government, despite evidence indicating that the military officers were acting contrary to orders. *Id.* at 493-94. Likewise, in *Youmans Claim*, another international claims commission interpreting international law held the Mexican government responsible for the actions of its domestic police when they killed American citizens while attempting to quell a local mob that had surrounded the home where the American citizens were residing. *Id.* at 507-08.

<sup>175</sup> The number of both individuals and states capable of initiating some form of cyber attack are problematic. *See, e.g.,* Schaap, *supra* note 22, at 134 (estimating that over 140 nations have operational cyber warfare programs in development); Coleman, *supra* note 57.

<sup>176</sup> The fact ultimately remains that this present understanding of attribution and state responsibility is fundamentally based on the belief that, following an attack, the source of the attack would be readily discernable. Cyber warfare, on the other hand, is an attractive military strategy precisely because it is so difficult to trace to a definite source. *See* Lipson, *supra* note 107.

<sup>177</sup> *See* Harris, *supra* note 130, at 491. This theory of state responsibility is what Harris terms the risk or objective theory of state responsibility. *See id.* This theory requires only that an action of the state be contrary to established international laws, regardless of the intent behind the action. *Id.*

<sup>178</sup> *Id.* Harris calls this state responsibility theory the fault or subjective theory. *Id.* Unlike the risk theory, state responsibility under this theory requires both an unlawful action under international law and a subjective intent or negligence on the part of the state being held responsible for the breach. *Id.*

used,<sup>179</sup> these theories provide little guidance when the source of the attack is unknown, as is typically the case in cyber warfare operations, or at least incapable of definite verification.<sup>180</sup> Some have argued that this State responsibility problem is primarily an evidentiary issue, and that by allowing for a standard of *beyond a reasonable doubt* to prove a State's involvement with cyber warfare operations, the problem can be effectively remedied.<sup>181</sup> While such

---

<sup>179</sup> *Id.* International judicial and arbitration practices provide equal support for the use of either theory of state responsibility, although state practice sheds little light on which is the more favored approach. *See id.*

<sup>180</sup> *See* Sinks, *supra* note 16, at 2. In general, one of the major advantages of cyber warfare is the ability to conduct such operations with practical complete anonymity. *Id.* The recent cyber attack on Estonia serves as a useful example of the fact that cyber warfare, by its nature, is conducive to covert state military action that can remain covert when the state carrying out the cyber attack ensures that the attack cannot be directly traced back to it. *See* Shackelford, *supra* note 83, at 24-25. As Shackelford notes, the attacks on Estonia were largely believed to be the work, to some degree, of the Russian military. *Id.* Even more telling are the subsequent cyber attacks on Georgia in 2008, which interestingly coincided with a conventional Russian military operation against that state. *See* McGavran, *supra* note 25, at 265-66. Although this may seem to further evidence Russian governmental involvement in the cyber attacks, others argue that the cyber bombardment of Georgian Internet infrastructures continued well after the Russian military operations, and hence were likely not Russian in origin. *See* Vasanth Sridharan, *Russia Calls Off Attack on Georgia—Cyber Attack Continues*, BUSINESS INSIDER (Aug. 12, 2008), <http://www.businessinsider.com/2008/8/russia-calls-off-attack-on-georgia-cyber-attack-continues>. Both the arguments for and against Russian government involvement in the cyber attacks on Estonia and Georgia have legitimate merit, evidencing the primary problem with attempting to use current theories of state responsibility to address attribution in cyber warfare. The established understandings of international law do not need to be merely reconsidered and adapted to fit into the cyber warfare regime; rather, these outmoded international legal concepts must be abandoned in the cyber warfare context altogether. *See infra* note 273 (further arguing that a re-evaluation of much of the international legal paradigm will likely be required to deal with the legality of cyber warfare operations).

<sup>181</sup> *See* Scott Shackelford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, SOCIAL SCIENCE RESEARCH NETWORK (Jan. 12, 2010), <http://ssrn.com/abstract=1535351>. Shackelford notes that state responsibility has generally been applied in cases where a state government exercises a sufficient degree of control over another person or entity. *Id.* at 5. Two tests have developed to determine whether such control exists. *Id.* The first of these tests, called the operational control standard and developed by the ICJ in the *Nicaragua* case, requires that non-state actors must act under the

an approach is noble in conception, it could easily result in instances in which a State is held liable for the conduct of entities engaging in cyber attacks without that State's support or knowledge.<sup>182</sup> Elite cyber warfare specialists can not only hide their origin, but alter their apparent location in order to implicate a State that is, in reality, no way involved in the cyber attacks.<sup>183</sup> In the end, the potential

---

complete control of the state in order to hold that state responsible for the non-state actor conduct. *Id.* The second test, called the overall control standard and developed by the ICTY in the *Tadic* case, requires only that a state have an effective degree of control over the conduct of non-state actors to hold their conduct attributable to the state generally. *Id.* In subsequent cases, the ICJ has defined the ICTY overall control standard to require only evidence proving beyond a reasonable doubt (as opposed to beyond any doubt, as required by the complete control standard in the *Nicaragua* case) that the non-state actor conduct was actually under state control to find state responsibility under international law. *Id.* Shackelford notes that, in the cyber warfare context, the ICTY overall control standard remains preferable because it permits a lower and more realistic burden of proof to relate a state government to state-sponsored, or even state-directed, attacks carried out exclusively by non-state actors. *Id.*; *but see infra* notes 183-84 (explaining general policy reasons why requiring such a lower burden of proof in implicating state responsibility for the conduct of non-state actors may be a dangerous proposition).

<sup>182</sup> See Congressional Documents, *supra* note 96, at 3.

<sup>183</sup> See *id.* at 4. According to reports made by the U.S. Congress, it was noted that the Internet remains inherently trusting in nature and, as such, it does not typically provide any mechanisms to prevent information from being falsified. *Id.* The ability to alter the apparent origin of a cyber attack has been utilized in Iran, where Internet bloggers have switched their computer settings, in an effort to confuse and impede government attempts to regulate and censor domestic Internet traffic and postings, to make it appear as though they are operating from within Iran. See *Crisis in Iran Sparks Global Guerilla Cyberwar*, *supra* note 72; see also AFP, *supra* note 14 (Craig Mundie, the Chief Research and Strategy Officer at Microsoft, said that he believes there are at least ten global states capable of sophisticated, large-scale cyber warfare attacks, and these states could make the attacks "appear to come from anywhere"). In particular, DoS attacks, which, as described earlier in this comment, function by employing the services of thousands of unknowing computers to simultaneously disable a specific network or computer server system, allow for this kind of manipulation. See Schaap, *supra* note 22, at 134; Congressional Documents, *supra* note 96, at 4. By utilizing computers located primarily, or even exclusively, within a single state, it would be easy for an advanced cyber attacker to initiate a DoS attack from one remote location and then make it appear as though the attack was actually coming from a state where these infected computers, unbeknownst to either the individual computer users or the localized state government, are actually located. See Congressional Documents,

consequences of a misguided accusation, and subsequent kinetic military reprisals for a mistakenly presumed act of cyber warfare, seem to outweigh the risk that State governments may illegally engage in competing actions of small-scale cyber warfare against one another.<sup>184</sup>

---

*supra* note 96, at 4. It would not be unreasonable to imagine the disastrous consequences of such a scenario: a China based server infects millions of U.S. based computers, through which a massive DoS attack is launched against Russia. *See supra* note 63 (recall the “Solar Sunrise” attacks in which a young Israeli and two high school students in the U.S. made a DDoS attack on Department of Defense systems appear to have originated from the UAE). Naturally, the origin of the DoS attack will appear to be American and certainly the consequences of such an attack could be globally catastrophic; Russia has already made it clear that it would consider nuclear reprisals to cyber warfare attacks to be completely justified under current international laws. Schaap, *supra* note 22, at 123; *see also* Timothy Thomas, *Russian Views on Information Based Warfare*, AIRPOWER J. (1996), available

at <http://www.airpower.au.af.mil/airchronicles/apj/apj96/spec96/thomas.html>. Under the overall control standard advocated by Shackelford and the ICJ, the preceding hypothetical may very well justify, on grounds beyond a reasonable doubt, that the cyber attacks originated from the U.S. and Russian retaliation would be justified. *See supra* note 181 (detailing the overall control standard requiring attribution proof beyond a reasonable doubt). This result simply is not tolerable. When states have publicly declared that they are willing to use nuclear weapons to respond to cyber warfare operations conducted against them, caution must be the primary concern and the most stringent burdens of proof must be required before a state is permitted to hold another state responsible for cyber warfare activities. *See infra* note 184.

<sup>184</sup> Although Shackelford notes that a more stringent evidentiary showing will likely have the effect of depriving states that are victims of cyber attacks of just compensation and reparations, it nonetheless seems that this may be a small price to pay compared with the potentially catastrophic consequences of allowing too relaxed of a standard to govern state attribution. *See* Shackelford, *supra* note 181, at 8. Furthermore, attribution issues may be less problematic for full-scale cyber warfare operations simply because there are a limited number of states capable of such large scale operations; yet, this must be considered in light of the fact that many states have little to lose in terms of cyber attack retaliation. *See* Congressional Documents, *supra* note 96, at 2. If major states cannot deter cyber warfare operations, and they cannot achieve much in cyberspace-based retaliation, then they are left only with the possibility to respond with conventional, kinetic based warfare. *Id.* This, again, cannot be condoned or permitted under any form of international law. Ultimately, the major problem with the use of either the operation control or overall control standards for determining state responsibility in international law is that both have been born from an international legal paradigm insufficient to deal with cyber warfare. As this comment will conclude, it is only by

## 2. Jurisdiction Problem

The second major shortcoming of current international law, making such laws ultimately inapplicable to legal issues raised by cyber warfare, is jurisdiction. In traditional international law, jurisdiction was based on the notion of state sovereignty.<sup>185</sup> It was this notion that each sovereign state has the inherent right to regulate and control its own territory that formed the basis of legal jurisdiction.<sup>186</sup> Obviously, state jurisdiction is key to any cyber warfare analysis, as it controls which state has the right, under international law, to prosecute<sup>187</sup> and seek remedy against cyber warfare aggressors.<sup>188</sup>

In considering international legal jurisdiction and cyber warfare, the first inquiry that must be made is whether a state can claim actual jurisdiction over cyberspace based on any traditional

---

re-evaluating and rejecting the current international legal regime that effective solutions to regulate cyber warfare can emerge. *See infra* notes 198, 210, 272 (outlining the general problems with traditional international laws application to cyber warfare in terms of territory, jurisdiction, and the need to reform those principles).

<sup>185</sup> *See Kanuck, supra* note 26, at 275. State jurisdiction developed, under customary international law, in what is commonly termed the “Westphalian system;” under this 1648 treaty system, the international community was comprised of individually sovereign states that regulated their activities with one another under the theory of *pacta sunt servanda*. *Id.* This international order was based on an understanding that the fundamental element of state sovereignty was that each state was subject to the laws and jurisdictions of one another whenever they ventured into territory claimed by another sovereign state. *Id.*; *see also* RICHARD CRAWFORD PUGH & OSCAR SCHACTER, *INTERNATIONAL LAW: CASES AND MATERIALS* xxiv (3d ed. 1993).

<sup>186</sup> *See Kanuck, supra* note 26, at 275-76. State jurisdiction is also commonly defined as “the power of a state under international law to govern persons and property by its municipal law.” Harris, *supra* note 130, at 264. Accordingly, state jurisdiction is primarily concerned not with the content of a state’s laws, but with “identify[ing] the persons and property within the permissible range of a state’s law and its procedures for enforcing that law.” *Id.*

<sup>187</sup> In addition to the right of a state to seek remedies and reparations for acts of cyber warfare under international law, an equally important factor is that often, jurisdiction also controls a state’s rights of retaliation, self-defense, and reprisal under international law. *See Sinks, supra* note 16, at 15.

<sup>188</sup> *See id.*

territorial principles.<sup>189</sup> There are five standard ways through which a state, under traditional international law principles, may acquire territory, and hence, concurrently acquire jurisdiction over that territory.<sup>190</sup> The five methods — conquest, prescription, cession, natural forces, and occupation —<sup>191</sup> all, for varying reasons, remain inappropriate in application to the cyberspace domain.<sup>192</sup> The acquisition of territory through conquest has, over the course of the past century, become illegitimate under customary international law.<sup>193</sup> Meanwhile, prescription, cession, and natural forces all remain inapplicable because they are predicated on factors that simply do not exist in the cyberspace domain.<sup>194</sup> Territorial acquisition through prescription is premised on the understanding that sovereignty has passed from one sovereign to another through either the passage of time or adverse possession of the disputed territory.<sup>195</sup> In the case of cyberspace jurisdiction, where the problem is the original acquisition of sovereignty, territorial prescription provides little guidance.<sup>196</sup> Cession is based on the ability of one state to voluntarily pass its sovereignty to another state.<sup>197</sup> Again,

---

<sup>189</sup> See WALTER B. WRISTON, *THE TWILIGHT OF SOVEREIGNTY* xii (1992). Traditionally, it has been an accepted concept of international law that “sovereignty has always been, in part, based on the idea of territoriality.” *Id.* at 7. The extent of a state’s jurisdictional reach has typically been directly related to, and even defined by, its geographic borders. *Id.*

<sup>190</sup> See Harris, *supra* note 130, at 190-229. Harris provides a comprehensive overview of the five primary ways international law has historically recognized the acquisition of territory. *Id.*

<sup>191</sup> See *id.*

<sup>192</sup> See Kanuck, *supra* note 26, at 288.

<sup>193</sup> See Harris, *supra* note 130, at 218. Although conquest was formerly one of the most common forms of acquiring territory — and hence, acquiring jurisdiction over that territory — it became unlawful under customary international law during the early twentieth century. *Id.* The 1928 Briand-Kellogg Pact denouncing “use of force” to acquire territory under international law was further codified in Article 2(4) of the U.N. Charter. *Id.* Additionally, under the Stimson doctrine of non-recognition, it has also become customary international law that states have an active duty to refrain from recognizing as legitimate any territorial acquisitions made through conquest. *Id.* at 218-19.

<sup>194</sup> See *id.* at 211-29.

<sup>195</sup> *Id.* at 211-13.

<sup>196</sup> See Shackelford, *supra* note 3, at 213.

<sup>197</sup> Harris, *supra* note 130, at 227.



unfortunately, this mode of territorial acquisition is of little help when, as is the case with cyberspace, the problem is determining who, if anyone, has an original claim to cyberspace territorial jurisdiction.<sup>198</sup> Finally, the natural forces territorial principles also fail to directly apply to cyberspace because they are limited in application to physical land.<sup>199</sup> Cyberspace, as its own territorial domain, is not subject to the standard notion that naturally occurring forces may alter territorial boundaries.<sup>200</sup>

Finally, occupation, while potentially applicable to cyberspace,<sup>201</sup> remains inappropriate for both policy and practicality reasons.<sup>202</sup> Thus, in order to determine jurisdiction over cyberspace,

---

<sup>198</sup> Shackelford, *supra* note 3, at 213.

<sup>199</sup> Harris, *supra* note 130, at 229.

<sup>200</sup> *See id.*

<sup>201</sup> Some have argued that current international treaty agreements regarding territory, namely the Antarctic Treaty System and 1967 U.N. Outer Space Treaty, might also serve as a template for declaring cyberspace a domain over which no claims of state sovereignty may be made. *See* Shackelford, *supra* note 3, at 211-13. In this sense, the jurisdiction over cyberspace activities would be resolved by simply not allowing any sovereignty claims at all. *Id.* at 213. However, this type of treatment would hardly result in any international legal process for dealing with legitimate acts of cyber warfare. *Id.* at 211-16.

<sup>202</sup> *See id.* at 213. Concepts of traditional occupation of territory are simply not applicable to cyberspace; as Shackelford observes, "unlike the physical world, cyberspace is an abstract reality of ideas, information, and logic." *Id.* The cyberspace domain operates on the condition that, although accessed through computer systems located within a defined territory, it exists across all physical territorial boundaries without obstruction. *Id.* at 212-13. Ultimately, cyberspace destroys the traditional mode of occupational territory because it erodes the assumed connection between territory and sovereignty. *Id.* Shackelford suggests using the "common heritage of mankind" principle to regulate state sovereignty over the cyberspace domain; as he observes, a key element of such an approach would be the non-militaristic nature of cyberspace. *Id.* at 213. However, the fact is that most states technologically capable of exploiting cyberspace for military purposes have already begun to do so. *Id.* Although noble in concept, it remains highly unlikely that, given the massive amounts of time and money expended on such cyber warfare strategies and military development, states would simply abandon those efforts for the common good of global access to the cyberspace domain.

and the cyber warfare operations occurring in that domain, a new understanding of territory must be reached.<sup>203</sup>

The second necessary inquiry regarding the jurisdiction problem is whether any of the traditional jurisdiction principles already existing and applicable under the present international law regime can also be applied to cyber warfare operations.<sup>204</sup> In considering the five traditional modes of acquiring criminal jurisdiction for international crimes — territorial, active nationality, protective security, passive nationality, and universality — it becomes apparent that several of these theories may be helpful in deciding jurisdiction over cyber warfare operations.<sup>205</sup> Although the active and passive nationality principles remain potentially applicable to instances of non-state actor cyber attacks,<sup>206</sup> it is the territorial, protective security, and universality principles that would create a far

---

<sup>203</sup> This new understanding is one of the primary considerations that must be dealt with during, as this comment concludes, a necessary reformulation of the international legal paradigm designed specifically to cater to the issue of cyber warfare operations. See *infra* notes 238, 242, 249.

<sup>204</sup> See Harris, *supra* note 130, at 264. This inquiry is principally limited to a consideration of the traditional international legal principles of jurisdiction as related to criminal jurisdiction. Civil jurisdiction over other sovereign states is, under current international law, limited to only a requirement of a substantial connection between the victim and accused parties. *Id.*; see also F.A. Mann, *The Doctrine of Jurisdiction in International Law*, 111 RECUEIL DES Cours 1 (Vol. 1 1964).

<sup>205</sup> Sinks, *supra* note 16, at 15. Indeed, arguments have already been made advancing the possibility of adopting a jurisdictional scheme applicable to cyber warfare based on the territorial, nationality, and protective security principles. *Id.*

<sup>206</sup> See Harris, *supra* note 130, at 265, 279, 298. The active nationality principle would allow the state representing the nationality of the guilty party to acquire jurisdiction over them; the passive personality principle would allow the state representing the nationality of the victim to acquire jurisdiction. *Id.* However, because each of these jurisdictional theories is predicated on the nationality of a single citizen, either victim or liable party, it seems inappropriate to use them in the context of state-sponsored cyber warfare operations. Another major problem with the use of any of the criminal jurisdiction principles in the context of state sponsored cyber warfare is that, under traditional international law, states are *not* subject to criminal jurisdiction, only individuals are. See *id.* at 309 (traditional notions of state immunity do not allow for one state to be tried in another states courts absent consent).

more efficient basis for determining jurisdiction over state-attributed cyber warfare.<sup>207</sup>

The territorial principle allows jurisdiction by either the state in which the crime occurs, the objective territorial principle, or where the effects of the crime are felt, the subjective territorial principle.<sup>208</sup> Although it is difficult to trace and determine the origin of cyber attacks, there is nonetheless a physical location constituting the site from which the cyberspace-based attacks are actually launched.<sup>209</sup> The protective security principle<sup>210</sup> would also apply to cyber warfare operations because large-scale cyber attacks certainly threaten the national interests of the state-victim of such attacks.<sup>211</sup> Finally, the jurisdiction over cyber warfare attacks could also be determined using the universality principle<sup>212</sup> if the attacks were of such a nature as to constitute a breach of customary international law.<sup>213</sup>

While currently existing criminal jurisdiction principles could be applied to acts of cyber warfare, such application would still necessitate a severe alteration of the existing international legal paradigm.<sup>214</sup> However, although the application of the universality

---

<sup>207</sup> See Sinks, *supra* note 16, at 15-17.

<sup>208</sup> See Harris, *supra* note 130, at 278.

<sup>209</sup> See Sinks, *supra* note 16, at 16-17.

<sup>210</sup> Harris, *supra* note 130, at 288. Harris defines the protective security principle as allowing a state whose national security is endangered by the unlawful action to acquire jurisdiction. *Id.* The primary requirement for asserting such jurisdiction is merely that there is a sufficient "linking point" between the one over whom jurisdiction is sought and the national security interests of the state seeking jurisdiction over them. *Id.* at 286.

<sup>211</sup> Sinks, *supra* note 16, at 15-16.

<sup>212</sup> Harris, *supra* note 130, at 288-89. The universality principle is defined as the ability to acquire jurisdiction based solely on the nature of the crime committed. *Id.*

<sup>213</sup> *Id.* When peremptory norms of international law, rights that states cannot, under any circumstances violate or deviate from, are breached, any state within the recognized international community retains the right to acquire jurisdiction over the guilty party. *Id.* Common examples of such peremptory norms are war crimes and piracy. *Id.* This principle, along with the protective security principle, was invoked by Israel in order to acquire jurisdiction over the head of the Nazi Gestapo during the Holocaust. *Id.* at 280.

<sup>214</sup> Each of these principles of jurisdiction is normally used to allow one state to acquire jurisdiction over *individuals* of a differing nationality; normally, sovereign states are not subject to the jurisdiction of other states without their

principle would require such significant re-evaluation — an argument that will ultimately be endorsed in part three of this comment —<sup>215</sup> the current territorial principle may also remain applicable when used in an effects-based context.<sup>216</sup> Under this theory, jurisdiction for cyber warfare attacks could be based on the location where the effects of the attack are felt.<sup>217</sup> Although this may help resolve the issue of jurisdiction, it would do little more than transfer the burden of identifying the culprit behind the attack to a victim-state that, because of that attack, is likely to be even less equipped to trace the origin of the cyber-based strike.<sup>218</sup> Ultimately, the problems of jurisdiction, like those of attribution, seem to lead inexorably to the

---

consent. *See id.* at 307-08. This state immunity concept gives states immunity from the jurisdiction of other states so long as they are acting within the general scope of public, state-related activities (the modern formation of restrictive immunity). *Id.* As such, in order to acquire jurisdiction over another sovereign state for liability for cyber warfare operations, a new legal precedent permitting the trial of a state for criminal penalties under international law would need to be formed. Another, perhaps more realistic, option would be to extend the jurisdictional reach of international tribunals, or the creation of a new international tribunal dealing exclusively with monitoring compliance with international cyber warfare law and endowed with global power to enforce decisions regarding liability for breaches of those laws. *See infra* note 267 and accompanying text (Shackelford proposes a global force pooling resources and working to prevent, identify, and punish cyber warfare aggressors).

<sup>215</sup> The need for a large scale overhaul of the existing international legal structure is not intended to make the current regime applicable to cyber warfare; rather, it requires the creation of a new branch of international law, founded on traditional principles but discarding those principles completely when necessary, to effectively cohere to the revolutionary requirements of cyber warfare legality. *See* Kanuck, *supra* note 26, at 288; Sinks, *supra* note 16, at 16-17; Shackelford, *supra* note 3, at 214.

<sup>216</sup> *See* Shackelford, *supra* note 3, at 211-12; Kanuck, *supra* note 26, at 286-87.

<sup>217</sup> *See id.*; *see also* Pugh & Schacter, *supra* note 185, at 1049. Although this doctrine holds some promise for establishing jurisdiction over acts of cyber warfare, it remains plagued by the same attribution problem that haunts all traditional, international legal jurisdictional methods. *See* Kanuck, *supra* note 26, at 287. Ultimately, “[a]ny comprehensive regulatory structure based on physical location thus seems grossly inadequate.” *Id.*

<sup>218</sup> *See* Shackelford, *supra* note 3, at 214. The interconnectivity of the attribution problem and the jurisdiction problem are evident; while the ability of a state to have a valid jurisdictional claim over a cyberspace attacker is critical, such an ability is rendered utterly useless unless that attacker can be identified. *Id.*

same conclusion: cyberspace and cyber warfare operations transcend the most fundamental assumptions underlying traditional international law and, as such, it is only through the creation of a new international legal paradigm that effective solutions can emerge.<sup>219</sup>

### 3. “Use of Force” Problem

Perhaps the most critical problem with seeking to apply the current international legal regime to cyber warfare is the general uncertainty surrounding what constitutes “use of force,”<sup>220</sup> and, accordingly, what self-defense responses remain permissible reactions under international law.<sup>221</sup>

Under current, customary international law, codified in the U.N. Charter Article 2(4),<sup>222</sup> defining an act as a “use of force” is

---

<sup>219</sup> See Kanuck, *supra* note 26, at 288 (“Even in the most abstract sense, the notion of territory [and its corollary on possessory rights] can only imperfectly account for the information realm. Cyberspace and information alike transcend physical boundaries, thereby requiring a legal paradigm that looks beyond merely the locus of events.”). As will be proposed in part three of this comment, cyber warfare is a unique and problematic international legal issue and will inevitably require “a reformulation of those [traditional, international, and legal] concepts to accommodate the imminent transnational society that will function predominantly in the borderless realm of cyberspace.” *Id.* at 286.

<sup>220</sup> See e.g., Sinks, *supra* note 16, at 18-19; 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, 446 (2009); West, *supra* note 154, at 17.

<sup>221</sup> See McGavran, *supra* note 25, at 268. Both the attribution and jurisdiction problems are most critical for response purposes: a state besieged by a large scale cyber warfare attack will likely not want to seek international legal sanctions against the attacking state, but rather it will want to know, under international law, to what degree may they respond to such an attack. *See id.*

<sup>222</sup> Current international law reflects the U.N. Charter 2(4), which states the following: “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.” U.N. Charter art. 2, para 4, available at <http://www.un.org/en/documents/charter/chapter1.shtml> (last visited Oct. 29, 2010). It has been argued that the phrase “any other manner inconsistent with the Purposes of the United Nations” does permit the “use of force” when such action would be consistent with the preservation of international peace, harmony, and principles of the inherent right to self determination, as formative goals of the U.N. generally. *See* Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), UNIV. OF MINN. HUMAN RIGHTS LIBRARY,

important for two reasons. First, if an act is defined as a “use of force”, it is presumptively illegal under both customary international law and the U.N. Charter.<sup>223</sup> Second, if an action is defined as a “use of force” under these provisions, retaliation by the victim state may be expressly permitted by those same provisions.<sup>224</sup> While the importance of defining an act of cyber warfare as “use of force,” and hence illegal under international law, is apparent,<sup>225</sup> the attribution issue also makes cyber warfare problematic in terms of self-defense.<sup>226</sup>

---

<http://www1.umn.edu/humanrts/instreet/GAres3314.html> (last visited Oct. 29, 2010).

<sup>223</sup> See *id.*; see also McGavran, *supra* note 25, at 269 (recognition of an act as a “use of force” under the U.N. Charter is a threshold issue in considering international legality).

<sup>224</sup> Article 51 of the U.N. Charter permits a sovereign state to respond to “use of force” against it; it reads as follows:

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

U.N. Charter art. 51, available at <http://www.un.org/en/documents/charter/chapter7.shtml> (last visited Oct 29, 2010).

<sup>225</sup> The ability to define a cyber warfare operation as a “use of force” would, of course, make the action illegal under the U.N. Charter and hence, at the very least, would entitle the victim state to the support of much of the international community. See *Definition of Aggression*, *supra* note 222. More importantly, international treaties purporting to advance collective action against a state that aggressively acts against one of its members would likely become effective if a cyber attack were defined as a “use of force.” See McGavran, *supra* note 25, at 270-71.

<sup>226</sup> See Shackelford, *supra* note 3, at 237 (in order for U.N. article 51 on self-defense to become legitimately applicable, the state using that force would need to be identified in order for any kind of retaliation to be justified). However, when confronted with a true instance of cyber attack on a member state, the U.N. was “conspicuously silent;” after the 2008 cyber assault against Estonia, the U.N.

However, the ability to use force in an international setting is not merely restricted by the U.N. Charter to self-defense measures under article 51; rather, the U.N. Security Council, pursuant to Chapter 7 of the Charter, is also authorized to use force to ensure international peace and security.<sup>227</sup>

Ultimately, fitting cyber warfare into the customary scheme of “use of force” as defined in the U.N. Charter is both problematic and uncertain.<sup>228</sup> While the traditional methods of determining whether an assault falls within the U.N. definition of aggression<sup>229</sup> and “use of force” have remained questionable,<sup>230</sup> a far more appropriate and effective results-based analysis has begun to emerge.<sup>231</sup>

---

did little to respond to or identify the status of such an attack under the U.N. Charter. *Id.* at 238. Such inaction ultimately only served to “[belie] the continuing legal uncertainty of cyber attacks in the international system.” *Id.* at 236-37; *see also* Schaap, *supra* note 22, at 146-47 (further noting that NATO also did not seem to consider the attacks on Estonia a “use of force” sufficient to invoke collective self-defense provisions of the NATO treaty, instead considering the acts to be more akin to cyber crime or terrorism).

<sup>227</sup> U.N. Charter art. 43-44, *available at* <http://www.un.org/en/documents/charter/chapter7.shtml>. Chapter 7 of the U.N. Charter expressly authorizes the U.N. Security Council to use means involving armed forces to secure international peace and security. *Id.* The U.N. Security Council famously authorized the “use of force” under chapter 7 of Security Council Resolution 678 when it requested that “all necessary means” be used to enforce its decisions against the resistance of the Iraqi state. Harris, *supra* note 130, at 960-61.

<sup>228</sup> *Compare* Sinks, *supra* note 16, at 18 (noting that some elites simply do not feel that cyber attacks can be adequately defined under the conventional “force” or “aggression” definitions of the U.N. Charter) *with* Schaap, *supra* note 22, at 147 (recognizing that a cyber attack which causes physical damage may be treated under the U.N. Charter as a “use of force”).

<sup>229</sup> *See* Definition of Aggression, *supra* note 222. The U.N. General Assembly officially addressed and defined aggression in 1974 when it introduced Resolution 3314 (XXIX); the resolution, in Article 1, defines aggression generally as “the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations . . . .” *Id.*

<sup>230</sup> *See* McGavran, *supra* note 25, at 269-70. Three emerging theories that have been developed and applied to the consideration of whether cyber warfare fits into the traditional “use of force” definition are the instrumentality, target-based, and consequentiality approaches. *Id.* Under the instrumentality approach, cyber warfare would be treated as outside of the “use of force” definition because such attacks differ from conventional, kinetic military assaults. *Id.* The target-based approach would consider cyber warfare as a “use of force,” as defined under the

As opposed to the traditional mode of determining “use of force” based on the nature of the assault, considering the effects of a cyber warfare attack is a better method for determining the international legal status of such incidents.<sup>232</sup> Under the former mode, many types of cyber warfare attacks would not be considered internationally unlawful, despite the fact that they may produce real world, kinetic damage equal to or surpassing the destruction wrought by conventional military weaponry.<sup>233</sup> The latter approach, meanwhile, is based on considering whether the effects of cyber attack are sufficiently similar to damage caused by conventional kinetic military assaults.<sup>234</sup> Such an approach allows for flexibility

---

U.N. Charter, whenever it penetrates a state’s critical infrastructure. *Id.* Finally, the consequentiality approach would consider cyber attacks to be a “use of force” if the attack produces damages equivalent to traditional military attacks. *Id.* However, each of these theories, considered individually, has been considered inadequate as either under- or over-inclusive in their consideration of what cyber warfare attacks would qualify as a “use of force.” *Id.*; see generally Hollis, *supra* note 84, at 1040-41 (Hollis provides a more detailed analysis of each of these theories and a discussion of why each proves “inadequate in the modern context”); Shackelford, *supra* note 83, at 26 (it remains unclear when a cyber attack would actually rise to the level of an armed attack under international law). *But see* Sharp, *supra* note 155, at 234. Sharp argues that the currently existing international legal structure sufficiently encompasses cyber warfare; he feels that the vast majority of cyber warfare operations would fall within the present definition of “use of force” and hence be unlawful under international law. *Id.* Nevertheless, Sharp does concede that such a conclusion would be primarily rooted in considering the effects, not the general mode, of the cyber attack. *Id.*

<sup>231</sup> See Kanuck, *supra* note 26, at 288-89; see also Sinks, *supra* note 16, at 18-19.

<sup>232</sup> Kanuck, *supra* note 26, at 289.

<sup>233</sup> *Id.* The Judge Advocate General for International Law of the United States Navy stated that although information manipulation may at some point qualify as “use of force”, that threshold has not yet been adequately defined. David L. Pierce, *Address at the Judge Advocate General Information Warfare Convention* (June 8, 1995). As a result of the varying theories used to place cyber warfare attacks in the “use of force” sphere, there is a continual risk that legitimate and destructive attacks would not be considered a “use of force” due to the cyberspace nature of those attacks. McGavran, *supra* note 25, at 270-71; see also Kanuck, *supra* note 26, at 289 (cyber warfare operations which interfered with a state’s financial systems or power grids would likely not qualify as “aggression” and hence would not be a use of force despite their “crippling effects”).

<sup>234</sup> See Sinks, *supra* note 16, at 19. Sinks notes that cyber warfare has evolved to a level of technological advancement whereby a kinetic attacks can be



and could serve as an appropriate mix of the theories already advanced in determining what cyber warfare actions should constitute a “use of force.”

Michael Schmitt, the Dean of International Law at the George C. Marshall Center, has advanced a theory similar to this effects-based notion.<sup>235</sup> Schmitt’s proposed theory combines both the effects of the cyber attack and the intent behind the attack.<sup>236</sup> Thus, any cyber attack that does actually cause, or may foreseeably cause, widespread injury, destruction, or death may be considered a “use of force” under the existing legal paradigm.<sup>237</sup> This theory to determine when cyber warfare qualifies as a “use of force” would not only allow for more destructive forms of cyber warfare assault, regardless of the type of weaponry utilized,<sup>238</sup> to be appropriately deemed internationally unlawful, but it also would greatly assist states in determining what cyber warfare responses would be legitimate under Article 51 self-defense.<sup>239</sup>

---

carried out completely in the absence of any kinetic weaponry, via cyber warfare. *Id.* Regardless, some commentators maintain the belief that certain instances of cyber warfare would clearly qualify as a “use of force” under the U.N. Charter and customary international law. *See* Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT’L L. & POL. 57, 80-81 (2001). Cyber attacks that preclude or are carried out in tandem with conventional military operations would, according to these commentators, qualify as a cyber warfare “use of force.” *Id.*

<sup>235</sup> *See* Schaap, *supra* note 22, at 147-48.

<sup>236</sup> *Id.*

<sup>237</sup> *Id.*; *see also* Sinks, *supra* note 16, at 20-22. Many have argued that cyber warfare operations require such an “expansion of the definition on the ‘use of force’” because a failure to do so would result in many destructive cyber warfare operations simply falling outside of the current definition, and hence not being considered illegal under traditional international laws. *Id.* at 20; *see also* Barkham, *supra* note 234, at 58.

<sup>238</sup> *See* Schaap, *supra* note 22, at 147-48. The weapons of cyber warfare are often seemingly benign, or at least fairly harmless, when considered individually; it is often only in the aggregate, such as with DDoS attacks, that the full destructive power of such weaponry becomes apparent. *See id.* Evaluating whether a cyber warfare attack qualifies as a “use of force” by considering both the intent and the consequences of the attack account for this oft forgotten fact.

<sup>239</sup> *Id.*; *see also* Sinks, *supra* note 16, at 20 (“International scholars recommend, ‘clearer rules of what kinds of information warfare actions constitute an armed attack,’ which drives permissible responses of self-defense”). Whether, in

In the end, the ability to identify a cyber warfare assault as a “use of force” will both inform the legality of that assault under international law and address the limits of internationally lawful self-defense responses to such an assault.<sup>240</sup> While there are indications that the international community has begun to recognize that a consequence-based consideration of cyber warfare operations is needed to adequately determine whether cyber warfare qualifies as a “use of force,”<sup>241</sup> it is only through a combination of a result-oriented approach with an additional intent consideration that cyber warfare can be effectively defined under international law.

#### IV. THE FUTURE OF CYBER WARFARE AND INTERNATIONAL LAW

Cyber warfare operations require a new and revolutionary reconsideration of many of the most fundamental principles underlying current international law.<sup>242</sup> Specifically, the present international legal regime must adapt in three primary ways. First, the critical concepts of attribution, jurisdiction, and “use of force” must be reexamined and altered to meet the exigencies created by the proliferation of cyber warfare operations. Second, consistent definitions of cyber warfare must be formed which either fit cyber warfare into existing international legal modes, or, more likely, a new area of international law must be developed to consider the issues

---

response to an attributed cyber attack, Article 51 on self-defense would permit the use of conventional, kinetic military response (bombing the location from which the cyber attack originated, for example) is an important question which, although beyond the scope of the “use of force” discussion here, will be yet another critical consideration for the international legal community. *See id.*

<sup>240</sup> *See* Schaap, *supra* note 22, at 148-49.

<sup>241</sup> *See* Sinks, *supra* note 16, at 21 (in the international community, there is a “growing recognition that an assertion of jurisdiction over offences abroad having an intended and substantial effect within a state may be justified”). By looking at the consequences of a cyber warfare assault, and concurrently considering the intentions behind that assault, international law will be better able to conclude whether the assault should be considered a “use of force,” and thus illegal under international law.

<sup>242</sup> *See* Kanuck, *supra* note 26, at 290 (arguing that certain existing international laws, inapplicable to cyber warfare, must be “exchanged for a new paradigm that addresses the deleterious activities of nation-states in a global sense”).

raised by non-traditional, cyber-based warfare activities. Lastly, international agreements must be formed immediately to limit and define cyber warfare while it is still in its infancy as a global concept and military strategy.

### A. Evolution

In order for international law to effectively address the issues raised by cyber warfare operations, the traditional international legal regime must adapt to the core factor driving the development of cyber warfare: technology.<sup>243</sup> Throughout history, the international legal regime has adapted to technological advances, indicating that it both can, and must, continue to adapt and evolve alongside the ever-changing realm of technology.<sup>244</sup>

Critical to the evolution of international laws are the necessary alterations to traditional understandings of attribution, jurisdiction, and “use of force.” While traditional international law assumes that attribution of State military operations will be fairly straightforward, cyber warfare has made evident that this assumption is not always true.<sup>245</sup> Rather, new theories of attribution must be developed by the international community to address the difficulty in tracing cyber-based attacks.<sup>246</sup> Further, until such a globally supported notion can be developed, a more strict attribution requirement should be maintained in order to avoid the potentially catastrophic consequences of full-scale cyber warfare based on anything less than absolutely certain State attribution.<sup>247</sup>

---

243 Harris, *supra* note 130, at 16.

244 *Id.* Harris observes that international law has always been forced to change in correlation to the advances of science. *Id.* Specifically, Harris recalls that international law had to be altered to accommodate the nuances of territorial definitions when outer space and the deep-sea bed became legitimate areas of global exploitation. *Id.* The preferred approach, according to Harris, is a good one: there is a constant need for international law to “[revise] thinking about some existing rules and [cause] the introduction of new ones.” *Id.*

245 See Lipson, *supra* note 107.

246 See *supra* notes 180-81 and accompanying text; see also Shackelford, *supra* note 3, at 246 (“[t]he fog of identity in cyberspace necessitates the creation of a legal regime that takes into account a level of uncertainty”).

247 See *supra* note 184 and accompanying text.

Secondly, international legal concepts of jurisdiction must also evolve to accommodate the technological innovation that underpins the development of cyber warfare.<sup>248</sup> While the traditional forms of establishing state jurisdiction over internationally unlawful conduct prove inadequate for dealing with instances of cyber warfare,<sup>249</sup> new modes of jurisdiction must be developed by the international community that take into account the unique characteristics of the cyberspace domain.<sup>250</sup>

Finally, the international definition and understanding of what constitutes an unlawful “use of force” under the U.N. Charter and customary international law must also evolve to account for cyber warfare operations.<sup>251</sup> Although a present consideration of cyber warfare as a “use of force” under international law may be inadequate and uncertain, there are developing proposals that call for redefining “use of force” to better accommodate cyber warfare operations by considering both the effects of, and intent behind, a cyber attack.<sup>252</sup>

In the modern world, cyber warfare is reshaping the global community, and laws regulating and defining acceptable global behavior must be created either by adapting the current international legal regime or by building a completely new international legal

---

248 Schaap, *supra* note 22, at 172-73 (“One of the greatest challenges of law is keeping up with the advancement of technology. The international community has often struggled to implement standards of conduct in a timely manner regarding the advancement of weaponry”).

249 *See supra* notes 190-92 and accompanying text (relating the traditional modes of establishing state jurisdiction and why each remains inadequate in the cyber warfare context).

250 *See supra* note 211 and accompanying text.

251 *See* McGavran, *supra* note 25, at 271 (noting that “[i]t is critical, however, that workable definitions be adopted to fit cyber attacks into the ‘use of force’ and ‘armed attack’ context”).

252 *See supra* note 237 and accompanying text. The notion that cyber warfare attacks should be considered in terms of both effect and intent to determine if they fall within the notion of “use of force” may also serve to effectively overcome the problems of over- and under-inclusiveness plaguing traditional “use of force” approaches. *See* McGavran, *supra* note 25, at 272. Consequently, states would be more certain of “how their actions, and actions taken against them, will be judged on the international stage.” *Id.* Further, such an approach would provide a “solid basis on which states could model new international agreements to regulate cyber attacks into existing ‘use of force’ terms.” *Id.*

structure developed specifically to address cyber warfare.<sup>253</sup> The evolution of international legal concepts to mirror the simultaneous developments in cyber warfare technology is a key element in defining and regulating this new field.<sup>254</sup>

### B. Consistency

While the evolution of international legal concepts of attribution, jurisdiction, and “use of force” are all necessary elements to the development of an international legal paradigm capable of dealing with cyber warfare, it is only through the consistent definition and application of such evolving principles that those changes can become truly ingrained within the international community.<sup>255</sup>

At present, the international community lacks consistency regarding even the most basic aspects of cyber warfare; in particular, there is no universally agreed upon definition of what even constitutes “cyber warfare.”<sup>256</sup> This inability to achieve international

---

<sup>253</sup> Harris, *supra* note 130 (there is a constant need for international law to “[revise] thinking about some existing rules and [cause] the introduction of new ones”).

<sup>254</sup> Some commentators make the point that technology may simply be too fast advancing for international law to keep up. See West, *supra* note 154, at 24 (arguing that “[t]he rate of technology will outpace the ability for an international cyber regime to produce responsive policy”). Although such concerns are legitimate, the combination of international agreements and the development of *jus cogens*, customary international legal principles, to dictate the legality of cyber warfare will nonetheless serve to best regulate this advancing technological field. See *infra* note 266-67 (Shackelford’s proposals on regulating cyber warfare call for either creating a new international legal regime specifically tailored to suit cyber warfare, or constructing international agreements that draw on existing international legal principles and introduce new international legal concepts as needed).

<sup>255</sup> See McGavran, *supra* note 25, at 270-71. \

<sup>256</sup> See Schaap, *supra* note 22, at 126 (“there is no widely accepted definition of ‘cyber warfare’”); Shackelford, *supra* note 3, at 199 (arguing that cyber warfare is a misnomer, and instead, “information warfare” is the more appropriate term; although conceding that even that term is susceptible to “definitions and conceptions . . . as numerous as they are complex”); Sinks, *supra* note 16, at 5-6 (noting the various definitions of cyber warfare).

consensus on even the most fundamental aspects of cyber warfare underscores the fact that such uncertainty invites cyber warfare operations during the intermediate flux of legal uncertainty and lack of enforcement against such attacks by the international community.<sup>257</sup>

Further, once internationally consistent definitions and regulations have been formed, the international community must uniformly and strictly enforce those standards.<sup>258</sup> Failure to enforce these standards may create a scenario, familiar in history, where banned weaponry continues to be developed and could eventually be used, despite international prohibitions on such use.<sup>259</sup>

### C. International Agreements

There has been significant debate over whether the international community needs new treaties to deal with the revolutionary problems created by cyber warfare.<sup>260</sup> However, the

---

<sup>257</sup> McGavran, *supra* note 25, at 271 (“As long as nations disagree over the definition of a cyber attack, they will be able to pigeonhole cyber attacks as either uses of force or not to suit their immediate political needs”).

<sup>258</sup> See Malawer, *supra* note 13, at 30-31.

<sup>259</sup> One commentator has compared the consequences of failing to regulate and to enforce regulations against cyber warfare to the development of aircraft carriers following World War I. *Id.* Although general disarmament conferences and treaties were formed to limit the development of new naval technologies after the devastation of WWI, the crucial failure to address and strongly enforce regulations against aircraft carrier development, at the time the most advanced weaponry technology being developed, led inexorably to future wars, with aircraft carriers leading the way. *Id.* The failure of the international community to act quickly to regulate and cohesively enforce regulations against developing military technology made international agreements regarding such technology “‘hallow results’ [that] ‘proved to be a monument to illusion.’” *Id.* To avoid repeating such mistakes with cyber warfare technology, such weaponry must be consistently defined and regulated under international law, and, most critically, those regulations must be enforced by the international community as a united whole.

<sup>260</sup> See Shackelford, *supra* note 83, at 26 (Shackelford proposes that “[g]iven the confused legal regime, the best way to ensure a comprehensive regime is through a new international accord dealing exclusively with cyber security and its status in international law”). *But see* McGavran, *supra* note 25, at 272-73 (noting that many continue to believe that cyber warfare concerns are overblown and international treaties regulating cyber warfare would be a waste of resources and political energies); Julian Ku, *Does the World Need a CyberWarfare Arms*

need for international agreements is critical to realizing the evolutionary changes in international law and the consistency required to afford such changes' staying power amongst the global community.<sup>261</sup> While some have commented that international agreements regulating cyber warfare will not do much in the way of deterring terrorist and criminal organizations from conducting cyber warfare operations,<sup>262</sup> such agreements would nonetheless serve to unite the global community in identifying and holding these groups accountable through a well-defined international prohibition against such activities.

Recently, there have been signs that the international community may be both ready and willing to begin seriously considering the formation of international treaties and binding agreements to regulate cyber warfare operations.<sup>263</sup> Many, apparently

---

*Limitation Treaty?*, OPINIO JURIS (June 7, 2010, 9:26 AM), <http://opiniojuris.org/2010/06/07/does-the-world-need-a-cyberwarfare-arms-limitation-treaty/> (arguing that international agreements to limit cyber warfare operations would impede efforts to battle cyber crime and non-state cyber warfare activities because the investigating state would be bound by the agreements, while the aggressor would not be bound); West, *supra* note 154, at 21-23 (arguing against the creation of an international treaty to deal with cyber warfare).

<sup>261</sup> See Martin Pineda, *International Law Must Adapt to Cyber Warfare*, THE CORD (Feb. 9, 2011, 12:23 AM), <http://cord.hotink.net/articles/42049> ("It is necessary that the international community recognize the importance of collaboration on extensions of international law specific to cyber warfare").

<sup>262</sup> See West, *supra* note 154, at 23. West argues that the creation of international law regulating cyber warfare would actually cripple the efforts to deter and fight terrorist groups who would likely continue to use weapons unaffected by any international legal restrictions. *Id.* However, this is a dangerous reason to decline to limit state use of cyber warfare; if this reasoning were followed, nuclear arms treaties would also be pointless because terrorist groups are not likely to consider international law if afforded the opportunity to utilize such weaponry. The fact that some groups will not feel obligated to follow international laws does not lead to the conclusion that such international regulations should not be created. West also makes the argument that cyber warfare, as a primarily non-lethal weapon technology, may be the lesser of two evils, and that international agreements limiting the use of such weaponry may have the more undesirable effect of increasing the use of more conventional kinetic military weaponry. *Id.* at 22.

<sup>263</sup> See Shackelford, *supra* note 3, at 250 ("There is evidence that at least some subset of countries, namely NATO, have begun international efforts aimed at increasing collaboration to prevent, investigate, and respond to attacks as they occur").

realizing that the presently existing international legal regime is inadequate to cope with the novel legal issues raised by cyber warfare, have come to understand the inherent advantage of definite international agreements on the legality of such activities.<sup>264</sup> The need for international agreements regulating cyber warfare operations has recently been endorsed by groups within the U.N.<sup>265</sup> and Russia.<sup>266</sup>

While there are inherent problems with seeking to formulate agreeable international treaties to address cyber warfare,<sup>267</sup> such agreements remain the best option for dealing with a global threat

---

<sup>264</sup> See David Elliot, *Weighing the Case for a Convention to Limit Cyberwarfare*, ARMS CONTROL ASSOCIATION (Nov. 2009), [http://www.armscontrol.org/act/2009\\_11/Elliot](http://www.armscontrol.org/act/2009_11/Elliot). Although attempts to use traditional international law may be useful in dealing with the legality of cyber warfare, restrictions based on international law precedent would have “an uncertain outcome” and would lack the “normative value of an explicit agreement.” *Id.* See also Shackelford, *supra* note 3, at 250 (noting that the international community must recognize the need for new international legal structures to address cyber warfare, and “to consider cyber attacks as the revolutionary threat that they are to the security and welfare of citizens around the world” in order for “real and lasting progress to be made”).

<sup>265</sup> See AFP, *supra* note 14. The U.N. International Telecommunications Union secretary, Hamadoun Touré, proposed that an international treaty be formed between global powers that addresses the legality of cyber warfare operations and under which States would not use cyber warfare as an offensive, first-strike weapon. *Id.*

<sup>266</sup> See Tom Gjelton, *Shadow Wars: Debating Cyber 'Disarmament'*, WORLD AFFAIRS J. (Nov./Dec. 2010), <http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament>. For over a decade, Russian officials have stressed the need for, and actively advocated for, international treaty agreements limiting cyber warfare operations. *Id.* But see John Markoff & Andrew Kramer, *U.S. and Russia Differ on a Treaty for Cyberspace*, N.Y. TIMES (June 27, 2009), <http://www.nytimes.com/2009/06/28/world/28cyber.html> (the Russian plans for an international treaty agreement to address cyber warfare have been troubled by disagreement with the U.S. over how comprehensive the coverage of the agreement will actually be).

<sup>267</sup> See Shackelford, *supra* note 83, at 26. The “increasingly multipolar state of world affairs and the resultant difficulty of reaching consensus on key issues facing the international community” are certainly challenges that will face any international treaty dealing with cyber warfare. *Id.*



that promises to rapidly grow more problematic.<sup>268</sup> Existing international treaty structures and cybercrime agreements could provide a workable foundation on which cyber warfare treaties could be built,<sup>269</sup> and cooperation amongst the global community is a critical element to the success of any such treaty.<sup>270</sup> Ultimately, serious changes in international law may be required to address the legal issues raised by cyber warfare operations, and it remains likely that a reevaluation of the core, fundamental components of traditional international legal structures will be required.<sup>271</sup> International treaties

---

<sup>268</sup> See Elliot, *supra* note 264, at 22 (noting the importance in “constrain[ing] this form of warfare in the relatively early stages of its development”). See also Scott J. Shackelford, *Estonia Two-an-a-Half Years Later: A Progress Report on Combating Cyber Attacks*, J. INTERNET L. (forthcoming), <http://ssrn.com/abstract=1499849>. An international treaty or agreement likely remains the best option for quickly and effectively dealing with cyber warfare. *Id.* According to Shackelford, such an international treaty would require three key elements to be truly effective: first, it would need to “define when a cyber attack rises to the level of an armed attack;” second, it must “clarify which provisions of international law apply during cyber warfare;” and third, it should “provide for enforcement mechanisms in the event of breach.” *Id.*

<sup>269</sup> See Amit, *supra* note 69, at 7. Amit “foresee[s] a move towards international cyber-treaties which would be based on the lessons learned at the field battling cybercrime.” *Id.* He also considers the possibility that international treaty agreements regulating the use of other kinds of weaponry, such as the U.S. and Russia nuclear arms treaty, may serve as useful blueprints for subsequent cyber warfare treaties. *Id.* Others believe that the 2001 E.U. Council Convention on Cybercrime would be a useful place to begin formulating cyber warfare treaties. Malawer, *supra* note 13, at 30.

<sup>270</sup> See Shackelford, *supra* note 83, at 27. Shackelford, in evaluating the responses of the international community to the need to regulate cyber warfare internationally, especially in the wake of the 2007 attacks on Estonia, notes the following: “Collective action is required. It is that collective action which has been missing over the past three years [since the cyber attacks on Estonia].” *Id.*

<sup>271</sup> See *id.* Shackelford also proposes a “polycentric approach” for addressing cyber warfare under international law. *Id.* Under this approach, regulatory solutions would be addressed at all levels. *Id.* Shackelford proposes that cooperative efforts of major global States and organizations could join together to address cyber warfare attribution and the enforcement of such regulations. *Id.* Specifically, Shackelford pictures a scenario in which a global organization, such as NATO, partners with a system of state-sponsored Cyber Emergency Response Teams (CERTs) to root out state-sponsors of cyber attacks, to pool resources and talent to defend against cyber attacks, and to provide intelligence to solve attribution problems. *Id.*

and agreements present the most direct, effective, and rapid means of implementing these needed changes.<sup>272</sup>

## V. CONCLUSION

Cyber warfare is a burgeoning technology that allows a computer savvy user to disrupt other computer networks and programs in various ways.<sup>273</sup> More advanced forms of cyber warfare can result in destruction of property and State infrastructure equivalent to, if not surpassing, most forms of conventional, kinetic warfare.<sup>274</sup> However, such cyber warfare is unique in that it operates within the borderless domain of cyberspace.<sup>275</sup> As such, cyber warfare remains impervious to many traditional international legal regulations and constraints.<sup>276</sup> While some international laws may be altered, adapted, and enhanced to take cyber warfare operations into account,<sup>277</sup> it may be an inevitable reality that the traditional international legal regime may simply be inadequate to accommodate

---

<sup>272</sup> Ultimately, international treaty agreements may only be the first step towards such a reevaluation and reformation of international laws applicable to cyber warfare operations. However, the first step is the most important, and, as Shackelford has aptly observed, “[t]he status quo strategic ambiguity is unsustainable and is a threat to international peace and security.” Shackelford, *supra* note 83, at 27.

<sup>273</sup> See McGavran, *supra* note 25, at 261. The various ways in which cyber warfare weaponry can be utilized is also outlined in more detail in the section “The Weapons of Cyber Warfare” of this comment.

<sup>274</sup> See McGavran, *supra* note 25, at 261 (a DoS cyber attack could be used to shut down a State’s air traffic control system, causing numerous casualties); Schaap, *supra* note 22, at 147 (noting that cyber attacks may result in physical damage); Shackelford, *supra* note 3, at 193-94 (comparing the effects of a full-scale cyber warfare attack, an “electronic Pearl Harbor,” with the devastation, destruction, and death caused by nuclear weaponry).

<sup>275</sup> See Kanuck, *supra* note 26, at 286 (defining cyberspace as a “borderless realm”).

<sup>276</sup> See *id.* (“Current paradigms of international law focus on a state-based structure that is preoccupied with the notions of sovereignty and territory. Yet tomorrow’s world will require — and, to a certain degree, today’s world already requires — a reformulation of those concepts . . .”).

<sup>277</sup> See Shackelford, *supra* note 3, at 250 (noting that the best approach to defining cyber warfare operations under international law may be to adapt and expand existing international law where possible, and to create new formulations of law when necessary).

the revolutionary issues raised by cyber warfare.<sup>278</sup> Consequently, new international laws may need to be developed, and a new global legal regime introduced, to effectively deal with cyber warfare issues.<sup>279</sup>

Ultimately, while some have argued that extensive renovations to the international legal paradigm are premature,<sup>280</sup> it is critical that such changes not be delayed, as cyber warfare already possesses destructive capabilities approaching that of full-scale nuclear war.<sup>281</sup> Consequently, further delay in the formation of international treaties, limiting the use of and defining the status of cyber warfare under international law, risks devastating global repercussions.<sup>282</sup> In the end, the need for new international legal structures cannot be ignored,

---

<sup>278</sup> As has been observed, cyber warfare represents a new age of military warfare and strategy, and international law must adapt, evolve, and reinvent itself to effectively account for this crucial fact. *See* Kanuck, *supra* note 26, at 290 (lamenting the fact that “international law still seeks to regulate the conflicts of yesterday”).

<sup>279</sup> The proposal regarding terrorism under international law made by Duncan Hollis could also be effectively used as a template upon which international law could deal with legal issues raised by cyber warfare. *See* Hollis, *supra* note 84, at 1026-27. Under Hollis’s proposal, a new international legal framework tailored to deal directly with issues of cyber warfare is likely needed. *Id.* Specifically, Hollis advocates the creation of an ILIO, or international law for information operations, which would be constructed and applied specifically against the backdrop of the emerging problems that cyber warfare have created for traditional international law. *Id.* at 1029.

<sup>280</sup> *See* Sinks, *supra* note 16, at 26 (concluding that the present international laws already in place can sufficiently address the ever-changing nature of warfare, including cyber warfare operations); West, *supra* note 154, at 25 (positing that the creation of a new international law to deal specifically with cyber warfare would do more harm than good).

<sup>281</sup> *See* Schaap, *supra* note 22, at 172-73. Although international law has historically struggled to keep pace with technological weaponry advances, this only evidences the fact that the international community needs to act now to “determine what is and is not permitted under international law in relation to cyber warfare operations.” *Id.* at 173.

<sup>282</sup> *See* Shackelford, *supra* note 3, at 251. Given the current, and constantly advancing, nature of cyber warfare weaponry, the need to regulate this area becomes all the more necessary. As Shackelford observes, failing to address cyber warfare, a militarized warfare potentially equivalent to nuclear weaponry, “risk[s] systematic infrastructure crashes that not only will cripple societies, but also could shake the Information Age to its foundations.” *Id.*

and a reevaluation of traditional legal values, combined with a willingness to completely reinvent the international legal paradigm to make it specifically applicable to cyber warfare issues, is a reality that must be accepted and addressed by the global community as a whole.