THE STUXNET ATTACK: A NEW FORM OF WARFARE AND THE (IN)APPLICABILITY OF CURRENT INTERNATIONAL LAW

Jordan Peagler*

TABLE OF CONTENTS

I. INTRODUCTION

Prior to the twentieth century, the notion of warfare being subject to binding international regulation was virtually nonexistent.[1] At the Hague Convention in October of 1907, the international community attempted to promulgate laws of war.[2] Until then, war had been viewed as a zero-sum game

* J.D., University of Arizona, James E. Rogers College of Law (2014); B.A., Political Science, University of San Diego (2010). Articles Editor, *Arizona Journal of International and Comparative Law*. This Note is dedicated to my friends and family whom I love dearly.

[1] *War and International Law A Brief History of the Law of War*, CONST. RIGHTS FOUND., http://www.crf-usa.org/war-in-iraq/war-and-international-law.html (last visited Mar. 23, 2014).

[2] *See generally Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land*, INT'L COMM. OF THE RED CROSS [hereinafter ICRC *Laws of War*], http://www.icrc.org/applic/ihl/ihl.nsf/INTRO/195 (last visited Feb. 19, 2014); *see also* Hague Convention IV, Respecting the Laws and Customs of War on Land and its Annex, Oct. 18, 1907, 36 Stat. 2277 [hereinafter Hague Convention IV].

with few laws governing its conduct.[3] For its time, the Hague Convention outlined radical principles now viewed as fundamental and unquestionable, such as the treatment of prisoners of war and flags of truce.[4] The Hague Convention was an extremely progressive step in international law, one that has been continuously amended and built upon.[5] With a solid foundation of international conventions in place, it seems warfare began being increasingly addressed as an activity that affected the entire international community, as opposed to just impacting the states directly involved in a conflict.[6] With the carnage and unprecedented level of death caused by World War I weighing heavily on the international community, U.S. President Woodrow Wilson initiated the formation of an international regulatory body that would come to be known as the League of Nations.[7] It was an ambitious attempt to align all of the nations of the world into a collective body, one that would work together to eliminate acts of warfare and belligerence between countries.[8] However, after some initial success in recruiting members, Wilson's idealistic vision for the League floundered; the failure of the United States to ratify the League Covenant coupled with the rise of Nazi Germany doomed the once promising League of Nations.[9]

After World War II drew to a bloody close, the need for such an international body became clear. It came to be that "[a] significant number of the old League's aims and methods were transmitted into [a] new organization in 1945."[10] The establishment of the United Nations (U.N.) solidified the international community's role in preventing conflict and ensuring global security.[11] World War II did more than just bring about the creation of the U.N.; it also fostered the unveiling of the nuclear bomb, a weapon that would forever change modern warfare.[12] In August of 1945, the United States dropped the first atomic bombs used in warfare on the Japanese cities of Hiroshima and Nagasaki.[13]

---

[3] *See generally* Sheng Hongsheng, *The Evolution of Law of War*, 1 CHINESE J. OF INT'L POL. 267, 269 (2006), *available at* http://cjip.oxfordjournals.org/content/1/2/267.full#sec-2 (discussing Carl von Clausewitz' military philosophy).

[4] *See* Hague Convention IV, *supra* note 2, § 1, ch. 2, § 2, ch. 3.

[5] *See generally id.*; *see also More About HCCH*, HAGUE CONF. ON PRIVATE INT'L LAW, http://www.hcch.net/index_en.php?act=text.display&tid=4 (last visited Apr. 5, 2014).

[6] *See* Second Protocol to the Hague Convention of 1954, The Hague, Netherlands, Mar. 15-26, 1999, *Protection of Cultural Property in the Event of Armed Conflict*, art. 5, UNESCO Doc. HC/1999/7 (Mar. 26, 1999) [hereinafter Second Protocol to the Hague Convention].

[7] Charles Townshend, *The League of Nations and the United Nations*, BRIT. BROAD. CO., http://www.bbc.co.uk/history/worldwars/wwone/league_nations_01.shtml (last updated Feb. 17, 2011).

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] U.N. Charter art. 1, para. 1.

[12] *Timeline of World War* II, PUB. BROAD. SERV., http://www.pbs.org/thewar/at_war_timeline_1945.htm (last visited Feb. 24, 2014).

[13] *Id.*

Technological advances, specifically nuclear weapons, and the vast destruction caused by them, fueled the proliferation of international regulatory agencies.[14] The International Atomic Energy Agency (IAEA) is just one of many international agencies designed to regulate sovereign nations that have been created since World War II.[15]

Today, the world is far different than it was post-World War II. The Cold War ended, and the Soviet Union along with it.[16] Technology continues to progress everyday at an unfathomable pace. Computers get faster and faster, while getting smaller and smaller. For example, the Harvard Mark-1 was a five-ton, room-sized computer completed in 1944.[17] Contrast the Harvard Mark-1 with the newest iPad, which weighs less than one pound, and you see the direction technology has taken.[18] The Internet is now one of the primary driving forces of the economy.[19] Computers and telecommunications transmitted through them are integral to countries' infrastructure and national security.[20] Along with the numerous benefits derived from modern computers, many aspects of these technological advances generate the need for international regulation. The United States and other countries have already utilized the military aspect of the Internet, and computer technology in general.[21]

Cyber terrorism and cyber warfare are relatively novel terms. While there is no universal consensus on a definition, cyber warfare has been defined as "the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks."[22] In his most recent State of the Union address, U.S. President Barak Obama stressed the military importance of having firm countermeasures in place to protect the United States

---

[14] DAVID FISCHER, HISTORY OF THE INTERNATIONAL ATOMIC ENERGY AGENCY: THE FIRST FORTY YEARS 1 (1997).

[15] *See generally* International Atomic Energy Agency Statute, Oct. 23, 1956, 8 U.S.T. 1093, 276 U.N.T.S. 4, *available at* http://www.iaea.org/About/statute.html.

[16] *Fall of the Soviet Union*, THE COLD WAR MUSEUM, http://www.coldwar.org/articles/90s/fall_of_the_soviet_union.asp (last visited Feb. 24, 2014).

[17] Paul A. Freiberger & Michael R. Swaine, *Harvard Mark I*, ENCYCLOPEDIA BRITANNICA ONLINE, http://www.britannica.com/EBchecked/topic/44895/Harvard-Mark-I (last visited Feb. 24, 2014).

[18] *iPad Mini*, APPLE, http://www.apple.com/ipad-mini/specs/ (last visited Feb. 24, 2014).

[19] *See* Courteney Palis, *Internet Economy: How Essential Is the Internet to the U.S.?*, HUFFINGTON POST, http://www.huffingtonpost.com/2012/03/20/internet-economy-infographic_n_1363592.html? (last updated Mar. 20, 2012, 4:52 PM).

[20] *See* Mark Memmott, *Grid Failure in India Cuts Power to 370 Million*, NAT'L PUB. RADIO (July 30, 2012, 8:02 AM), http://www.npr.org/blogs/thetwo-way/2012/07/30/157583464/grid-failure-in-india-cuts-power-to-370-million.

[21] *See* James P. Farrell & Rafal Rohozinski, *Stuxnet and the Future of Cyber War*, 53 SURVIVAL 23, 24 (2011).

[22] *See Cyber Warfare*, RAND CORP., http://www.rand.org/topics/cyber-warfare.html (last visited Feb. 24, 2014).

from the growing threat posed by cyber warfare.[23] In June 2010, the Islamic Republic of Iran felt the effects of what would become known as the "Stuxnet Virus."[24] Iran's nuclear ambitions suffered a setback resulting from the Stuxnet attack on its facilities in Natanz.[25] Many believe cyber warfare is the wave of the future,[26] but the law has been slow to address its use, misuse, and what degree of retaliation it warrants. [27]

II. OVERVIEW OF CYBER WARFARE

In this Note, I will apply existing international law to the Iranian attack, and examine a new U.N. agreement that would elevate cyber-attacks to the level of conventional belligerence on a nation's sovereignty. In section A, I will discuss the advent of ARPANET, the precursor to the Internet, and its roots as a military tool. After discussing the groundwork for what has become known as the Internet, I will examine its application as a military weapon in the recent South Ossetia conflict between Russia and Georgia, along with NATO's reaction to the cyber-attack. This Note will then attempt to find a more refined definition of cyber warfare. Section E will examine the U.N. Charter's broad prohibition against the use of force, and examine several definitions of "force" (e.g., force as coercion, armed violence, and interference) and how they relate to cyber warfare. Section F of this Note addresses the current international regulatory framework surrounding cyber warfare, and then, in Part III, I will begin my analysis regarding the Stuxnet attack on the Iranian nuclear facilities at Natanz. Next, in Part IV, I will examine the implications and potential likelihood of creating a new treaty or convention that clearly defines and regulates cyber warfare. Finally, I will summarize the findings and analysis of this Note in the conclusion section.

---

[23] Christina Gagnier, *White House Cybersecurity Order Accompanies State of the Union Address*, HUFFINGTON POST (Feb. 12, 2013, 10:53 PM), http://www.huffingtonpost.com/christina-gagnier/obama-cybersecurity-executive-order_b_2674283.html?.

[24] Farrell & Rohozinski, *supra* note 21, at 23.

[25] *Id.* at 29.

[26] *See Cyber-Warfare: Hype and Fear*, ECONOMIST (Dec. 8, 2012, 4:03 PM), http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may.

[27] Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 134 (2005).

A. The Foundation Laid by ARPANET

While Al Gore may claim to have invented the Internet,[28] he surely was not alone.[29] The Internet and computers as we know them today would be almost unrecognizable to the scientists and technicians who began the groundbreaking research in the 1960s.[30] The Advanced Research Projects Agency Network (ARPANET) established the foundation for what has become the modern day Internet.[31] Created by the U.S. Department of Defense,[32] ARPANET involved some uses of the first use of a packet-switching network.[33] Packet-switching is the:

> [D]ividing of messages into packets before they are sent, transmitting each packet individually, and then reassembling them into the original message once all of them have arrived at the intended destination. Packets are the fundamental unit of information transport in all modern computer networks . . . .[34]

Engineers envisioned that a packet-switching network would connect diverse computers into a communal network.[35] Packet-switching, while still unproven, promised a more efficient use of a network's long-range communications links and a boost to a network's ability to recover from equipment failures.[36] ARPANET was born with Cold War implications squarely in mind.[37] Cold War defense analysts considered durable communications networks as a necessity in the event of a nuclear confrontation.[38] Prior to packet-switching, the switching involved in conventional communications networks was concentrated in a single local or regional facility.[39] The need for durable communications increased as the two Cold War foes exponentially increased their nuclear arsenals:

> Both the US and USSR were building hair-trigger nuclear ballistic missile systems . . . If the strategic weapons command and control systems could be more survivable, then the country's

---

[28] *Internet Hall of Fame: Al Gore and Craig Newmark Inducted, Google Founders Snubbed*, HUFFINGTON POST (Apr. 24, 2012), http://www.huffingtonpost.com/2012/04/24/internet-hall-of-fame-al-gore-craig-newmark_n_1449048.html.

[29] *See* JANET ABBATE, INVENTING THE INTERNET 7 (MIT Press ed., 2000).

[30] *See id.* at 40.

[31] *See id.* at 113.

[32] *Id.* at 2.

[33] *Id.* at 46.

[34] *Packet Switching Definition*, THE LINUX INFO. PROJECT (Nov. 4, 2005), http://www.linfo.org/packet_switching.html.

[35] ABBATE, *supra* note 29, at 46.

[36] *Id.* at 39.

[37] *Id.* at 77.

[38] *Id.* at 9.

[39] *Id.* at 11.

> retaliatory capability could better allow it to withstand an attack and still function . . . . But this was not a wholly feasible concept, because long distance communications networks at that time were extremely vulnerable and not able to survive attack. That was the issue. Here a most dangerous situation was created by the lack of a survivable communication system.[40]

Due to the lack of long-range communications networks, the development of ARPANET became a national security concern of the highest importance.[41] This communication vulnerability prompted the U.S. government to allocate a large amount of funding to ARPANET researchers.[42] In sum, "packet-switching [was appealing] because it seemed to meet the requirements of a survivable military system . . . . Efficient transmissions made it possible for commanders to have higher communications capacity . . . [it] made perfect sense in the Cold War context."[43]

B. Cyber Warfare's Involvement in the South Ossetia Conflict

In the summer of 2008, the international community was rattled by the sudden outbreak of fighting in the Georgian territory of South Ossetia in Eastern Europe.[44] After escalating tensions came to a boiling point, the Russian military crossed the sovereign borders of another nation for the first time since 1979.[45] As tanks, fighter jets, and other conventional military forces poured into Georgian territory, they were accompanied by cyber-attacks launched from the Russian mainland.[46] However, it was not the first time Russia had used cyber warfare.[47] Estonia, a country heavily reliant on the Internet, endured a crippling barrage of cyber-attacks after it decided to remove a Soviet World War II monument from

---

[40] Interview by Judy O'Neill with Paul Baran, employee, RAND Corp., in Menlo Park, Cal. (Mar. 5, 1990).

[41] *Id.*

[42] ABBATE, *supra* note 29, at 75.

[43] *Id.* at 20 (alteration in original).

[44] SVANTE E. CORNELL & S. FREDERICK STARR, at *Introduction*, *in* THE GUNS OF AUGUST 2008: RUSSIA'S WAR IN GEORGIA 3 (Svante E. Cornell & S. Frederick Starr eds., 2009).

[45] *Id.*

[46] JOHANNA POPJANEVSKI, *From Sukhumi to Tskhinvali: The Path to War in Georgia*, *in* THE GUNS OF AUGUST 2008: RUSSIA'S WAR IN GEORGIA, *supra* note 44, at 143, 152.

[47] *See Marching off to Cyberwar*, ECONOMIST (Dec. 4, 2008, 12:00 PM), http://www.economist.com/node/12673385?story_id=12673385&CFID=34793589&CFTOKEN=83946352.

the nation's downtown capital of Tallinn.[48] The Distributed Denial of Service attack (DDoS) targeted Estonia's essential electronic infrastructure, including the government's communications network, banks, and corporate websites.[49]

> [B]otnets . . . made up of hundreds of thousands of individual computers from around the world . . . known as zombies, could be made to repeatedly flood designated Internet addresses with a variety of useless network-clogging data. It was the digital version of carpet bombing and is referred to as a distributed denial of service . . . ."[50]

These DDoS attacks overwhelmed the Estonian networks with bogus requests causing them to become unusable.[51] The Russian government denied the attacks, and eventually a small group of activists associated with the pro-Kremlin youth group, Nashi, claimed responsibility for the attacks.[52]

Russia's successful DDoS attack against Estonia likely served as the template for its attack on Georgia the following year.[53] What distinguished the Georgian attacks from their Estonian predecessor was that the Georgian cyber-attacks were coordinated, alongside Russian land and air attacks on its sovereign territory.[54] As Russian tanks engaged Georgian forces in Ossetia, the Russian government was well aware that it needed to frame its actions as being necessary to protect Russian citizens.[55] Initially the worldwide press appeared to accept Russia's justifications, which were "facilitated by Russia's . . . . ongoing cyber-attacks against Georgian governmental and media websites, which hampered [the Georgian capital's] ability to disseminate information during the first days of hostilities."[56] The DDoS attack crippled Georgia's civil administration and ability to communicate with its population during a national emergency.[57] While several Georgian websites that distribute information, from both governmental and media

---

[48] *A Look at Estonia's Cyber Attack in 2007*, NBCNEWS.COM, http://www.msnbc.msn.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.UIBIsxilmHs (last updated July 8, 2009, 2:24 PM).

[49] *Id.*

[50] 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.

[51] *Marching off to Cyberwar*, *supra* note 47.

[52] *A Look at Estonia's Cyber Attack in 2007*, *supra* note 48.

[53] Davis, *supra* note 50 (quoting Denis Bilunov, the executive director of the United Civil Front: "There is a specific department within the FSB—the successor to the KGB—that specializes in coordinating Internet campaigns against those they consider a threat[.]").

[54] POPJANEVSKI, *supra* note 46, at 154; *see also* PAVEL FELGENHAUER, *After August 7: The Escalation of the Russia-Georgia War*, *in* THE GUNS OF AUGUST 2008: RUSSIA'S WAR IN GEORGIA, *supra* note 44, at 166.

[55] POPJANEVSKI, *supra* note 46, at 154.

[56] *Id.*

[57] Farrell & Rohozinski, *supra* note 21, at 26.

agencies, were rendered inaccessible, the actual damage inflicted upon Georgia as a result of the cyber-attacks was minimal.[58]

The most acute feature of the Georgian cyber-attack was its lack of traceability; Georgia was left with only fragments from which to patch together where the attack originated.[59] Such attacks are cheap, effective, and easily concealed: "It costs about 4 cents per machine, [y]ou could fund an entire cyberwarfare [sic] campaign for the cost of replacing a tank tread."[60] It seems likely that the Russian strategy employed against Georgia, a cyber-attack as a first-strike weapon preceding a conventional military campaign, will serve as the template for future cyber-attacks.[61] So, while there was significant circumstantial proof of Russia's involvement in the DDoS attacks, there was no direct link, allowing the Russian government to deny culpability.[62]

C. Reaction to the Georgian Conflict by NATO

Estonia is a member of the North Atlantic Treaty Organization (NATO),[63] but Georgia's membership to the alliance is not yet finalized.[64] Following the 2008 attacks by Russia, heads of state met at the Bucharest Summit and agreed to assist Georgia.[65] The ramifications of the Estonian attack prompted NATO to create the Cooperative Cyber Defense Center of Excellence in Tallinn to address the myriad novel issues implicated by cyber warfare.[66] The Center conducts research and has specialists to train officials on cyber defense.[67] NATO now recognizes that the growing sophistication of cyber-attacks is a real threat

---

[58] *See Marching off to Cyberwar*, *supra* note 47. For example, some e-mail communication was disrupted. *Id.*

[59] *See* Farrell & Rohozinski, *supra* note 21, at 26-27.

[60] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1 (quoting Bill Woodcock), *available at* http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=2&.

[61] Press Release, Eur. Network & Info. Sec. Agency, EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats & Critical Info. Infrastructure Prot. (Oct. 7, 2010).

[62] *See* Markoff, *supra* note 60.

[63] *See Marching off to Cyberwar*, *supra* note 47.

[64] *NATO's Relations with Georgia*, NATO, http://www.nato.int/cps/en/natolive/topics_38988.htm (last visited Feb. 24, 2014).

[65] *Id*.

[66] *See NATO Opens a New Centre of Excellence on Cyber Defence*, NATO, http://www.nato.int/docu/update/2008/05-may/e0514a.html (last visited Mar. 11, 2014).

[67] *See Mission and Vision*, CCDCOE, http://www.ccdcoe.org/11.html (last visited Mar. 2, 2014).

that needs to be addressed.[68] On November 20, 2010, various heads of state met in Lisbon at a meeting of the North Atlantic Council.[69] The Council stated:

> Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance. We will strive in particular to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralised cyber protection. We will use NATO's defence planning processes in order to promote the development of Allies' cyber defence capabilities.[70]

The Lisbon Summit brought cyber warfare to the forefront of NATO's agenda, highlighting the need for accelerated efforts to improve its ability to detect, assess, prevent, defend, and recover from cyber-attacks.[71] As of February 2012, NATO had committed over U.S. $75,000,000 to the NATO Computer Incidence Response Capability (NCIRC) to enhance intelligence sharing and situational awareness.[72] NATO cited the Estonian and Georgian conflicts as outlining the growing sophistication of cyber warfare and its potential to become a major component of conventional warfare.[73] After the Lisbon Summit in 2010, NATO leaders met again in 2012, this time in Chicago, to reaffirm their commitment to developing its cyber defense capabilities in order to meet the evolving threat of cyber warfare.[74]

As stated previously, the agreements reached at the Lisbon Summit emphasized the importance of the NCIRC.[75] The NCIRC has two tiers.[76] The first tier comprises the Technical Center, which is NATO's primary technical and operational body charged with responding with countermeasures to "any cyber

---

[68] *NATO and Cyber Defence*, NATO, http://www.nato.int/cps/en/natolive/topics_78170.htm (last visited Feb. 24, 2014).

[69] Press Release, North Atlantic Council, Lisbon Summit Declaration ¶ 1, PR/CP(2010)0155 (Nov. 20, 2010).

[70] *Id.* ¶ 40.

[71] *Id.*

[72] *NATO and Cyber Defence*, *supra* note 68. The amount in the source, which listed the commitment at € 58,000,000, was converted to U.S. dollars.

[73] *See id.*

[74] *Id.*

[75] Lisbon Summit Declaration, *supra* note 69, ¶ 40.

[76] *NATO and Cyber Defence*, *supra* note 68.

aggression against the Alliance."[77] The second tier of the NCIRC is the Coordination Center, which is responsible for coordinating cyber defense activities and exercises within the Alliance as well as with other international organizations (e.g., the European Union).[78] In summation, prior to the cyber-attacks on Estonia and Georgia, the Alliance's defense efforts were primarily aimed at protecting members' communication systems, but since then NATO has broadened its focus.[79]

D. Attempting to Define Cyber Warfare

While its evolution continues to increasingly impact the international community, cyber warfare remains essentially undefined.[80] As computer-security specialist Bruce Schneier points out, "[o]ne problem is that there is no clear definition of 'cyberwar.' What does it look like? How does it start? When is it over? Even cybersecurity [sic] experts don't know the answers to these questions . . . ."[81] Part of the difficulty in establishing firm parameters as to what constitutes an act of cyber warfare is the fact that the Internet, unlike tanks and jets, is not owned or controlled by any one nation; it is available to all entities private and public.[82] While often fairly nebulous, "the definition of cyber warfare has been expanded to include government-sponsored espionage, potential terrorist attacks in cyberspace, large-scale criminal fraud, and even hacker kids attacking government networks and critical infrastructure."[83] The U.S. National Research Council's Committee on Offensive Information Warfare (NRC Committee) defines cyber-attacks as referring to, "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[84] The NRC Committee's definition differs from other definitions in that it distinguishes between cyber-attacks and cyber exploitation, which it refers to as an intelligence-

---

77 *Id.*

78 *Id.*

79 *Id.*

80 Bruce Schneier, Comment to *Wire Opinion: Cyber War is the New Yellowcake*, SCHNEIER ON SEC. (Feb. 28, 2012, 7:52 AM), https://www.schneier.com/blog/archives/2012/02/cyberwar_is_the.html; *see also* Jerry Brito & Tate Watkins, *Wire Opinion: Cyber War is the New Yellowcake*, WIRED (Feb. 14, 2012, 6:30 AM), http://www.wired.com/threatlevel/2012/02/yellowcake-and-cyberwar/.

81 Bruce Schneier, *The Threat of Cyberwar Has Been Grossly Exaggerated*, SCHNEIER ON SEC. (Jul. 7, 2010, 12:58 PM), http://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html.

82 *See* Bruce Schneier, *Cyberwar Treaties*, SCHNEIER ON SEC. (June 14, 2012, 6:40 AM), http://www.schneier.com/blog/archives/2012/06/cyberwar_treati.html.

83 *Id.*

84 NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009) [hereinafter NRC COMMITTEE REPORT].

gathering function rather than a destructive function.[85] Schneier is of the belief that for an attack to be considered cyber warfare, "it must first be war."[86] This seems to imply that a cyber-attack on a nation's power grid, independent of any mobilization of conventional forces, would fall short of qualifying as cyber warfare. The definition of cyber warfare I will be using is warfare that alters, disrupts, or destroys computer systems or networks, or information and programs on them.[87]

The technical aspect of a cyber-attack involves accessing and exploiting a vulnerability in order to deliver a payload.[88] The term "payload" is used to describe the things that can be done once a vulnerability has been exploited (e.g., uploading the Stuxnet virus).[89] A remote-access cyber-attack is one that "is launched at some distance from the adversary computer or network of interest" (e.g., accessing an adversary computer through a wireless network); a close-access cyber-attack is one that "takes place through the local installation of hardware or software functionality in close proximity to the computer or network of interest."[90] Exploitable vulnerabilities refers to service providers, hardware, software, or even users and operators.[91]

Some have posited that the law of war only applies to cyber warfare by analogy.[92] Because cyber-attacks and information operations do not constitute armed attacks, analogies seem appropriate. It would not be the first time that an emerging field of warfare was regulated by means of analogizing between it and an existing form of combat.[93] After World War II came to an end, diplomats from around the world met to create additional protocols regarding the laws of war because the existing framework insufficiently covered air warfare; the new rules concerning air warfare were largely derived from the rules of land warfare.[94] Another roadblock to defining cyber warfare is that the law of war is state-centric, meaning that the existing regulatory framework primarily controls how states interact with other states.[95] However, as the Russian attacks in Estonia demonstrated, cyber-attacks can be orchestrated by private citizens devoid of state action, which causes analytical problems for the state-centric approach to

---

[85] *Id.*

[86] Bruce Schneier, *Cyberwar: Myth or Reality?*, SCHNEIER ON SEC. (Nov. 2007), https://www.schneier.com/essay-201.html.

[87] This definition is based heavily on the one used in the NRC COMMITTEE REPORT, *supra* note 84, at 10-11.

[88] *Id.* at 83.

[89] *Id.*

[90] *Id.* at 87.

[91] *Id.* at 79.

[92] *See, e.g.*, Wolfgang McGavran, *Intended Consequences: Regulating Cyber Attacks*, 12 TUL. J. TECH. & INTELL. PROP. 259, 268 (2009).

[93] *See generally* Hague Convention IV, *supra* note 2.

[94] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1037 (2007).

[95] *Id.* at 1047-48.

emerging informational operations.[96] While attacks by individual criminals are predominately motivated by profit, terrorist groups and foreign governments pose a more serious threat because their motives are destruction and disruption.[97]

> Compared to the military forces and weapons that have threatened Western societies in the past, modern technology has made the tools of [cyber warfare] cheap, readily available and easily obtainable. The ubiquity of Internet access and the easy availability of hacker tools on underground Internet sites have significantly reduced both financial and intellectual barriers to launching attacks against critical computer systems. Little equipment is needed to launch such attacks. The basic attack tools consist of computers, modems, telephones and software, essentially the same tools used by hackers and cyber-criminals. [Cyber warfare], unlike nuclear warfare, is not just the province of the industrial nation-state. Terrorist groups, whether state-sponsored or independent, domestic or international, as well as organized crime syndicates and individuals, have cyber-technologies at their disposal to launch these attacks.[98]

Because of these complex, multifaceted aspects of cyber warfare, any attempt to define and regulate cyber warfare must be broader than the restrictive, state-centric view that dominates the current analysis.

There have been several attempts to fit cyber warfare into the current international regulatory framework. The first is known as the "instrumentality" approach.[99] Proponents of the instrumentality approach argue cyber warfare does not qualify as an armed use of force because it "lacks the physical characteristics traditionally associated with military coercion. The text of the U.N. Charter offers some support for this view; Article 41 lists 'measures not involving the use of armed force' to include 'complete or partial interruption of . . . telegraphic, radio, and other means of communication.'"[100] Another approach to bring cyber-attacks under the existing international regulatory framework of Article 2(4) is known as the "target-based" approach.[101] This approach holds that a cyber-attack rises to the equivalent of an Article 41 use of armed force whenever it penetrates the

---

[96] *Id.* at 1049.

[97] ANTHONY H. CORDESMAN & JUSTIN G. CORDESMAN, CYBER-THREATS, INFORMATION WARFARE, AND CRITICAL INFRASTRUCTURE PROTECTION: DEFENDING THE U.S. HOMELAND 8 (2001).

[98] Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. OF INT'L L. 825, 832 (2001).

[99] Hollis, *supra* note 94, at 1041.

[100] *Id.* (quoting U.N. Charter art. 41).

[101] *Id.*

critical infrastructure of a nation.[102] The target-based approach substantially branches off from the traditional interpretation of force in that a cyber-attack would fall under Article 2(4)'s governance, i.e., the prohibition on the use of force, even absent destruction or casualties.[103] Another approach to fitting cyber-attacks into the current international regulatory framework is known as the "consequentiality" approach.[104] This approach, which focuses on the consequences of a cyber-attack, is favored by the U.S. Department of Defense; the consequentiality approach holds that whenever the effects of a cyber-attack are equivalent to those produced by a traditional attack (death or destruction of property) it would constitute the use of force in an armed attack.[105]

E. Interpretation of "Force" Under the U.N. Charter

The U.N. Charter fails to outline what constitutes "use of force" in cyberspace, a deficiency that must be addressed by the International Community.[106] Harold Koh, the U.S. State Department's former chief legal advisor, has stated that international law does apply to activities in cyberspace, and that in order to constitute "use of force" under Article 2 of the U.N. Charter a cyber-attack would have to "proximately result in death, injury or significant destruction."[107] Koh's statement was significant because the United States is one of the "few governments believed to have engaged in cyber warfare, in particular the Stuxnet attack against Iran's nuclear centrifuge infrastructure. Koh's announcement of a legal doctrine on cyber warfare comes just months after new reports surfaced about the Obama administration's alleged central role in deploying the Stuxnet worm.[108] While Koh's statement is illustrative of the United States' developing stance toward cyber warfare, "the U.S. government has not formalized a definitive public position on the issue or articulated clear lines or standards."[109] Whether or not a cyber-attack meets the definition of "use of force" is the determinative issue when analyzing the current legal implications of such operations.[110]

---

[102] *Id.*

[103] Hollis, *supra* note 94, at 1041.

[104] *Id.*

[105] *Id.*

[106] *See* U.N. Charter art. 2, para. 4. Article 51 carves out a self-defense exception to "armed" attacks set out in Article 2, paragraph 4.

[107] Aram Roston, *U.S.: Laws of War Apply to Cyber Attacks*, ARMY TIMES (Sept. 18, 2012, 8:18 PM), http://www.armytimes.com/article/20120918/NEWS/209180311/U-S-Laws-of-war-apply-to-cyber-attacks.

[108] *Id.*

[109] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 432 (2011) (internal citations omitted).

[110] McGavran, *supra* note 92, at 270.

1. Force as Armed Violence

The traditional law of armed conflict, the one most accepted by the United States and its allies, is that the Article 2(4) prohibition of force and the related right to self-defense outlined in Article 51 apply to armed attacks.[111] This seems to be supported by the plain meaning of the text and the likely intent of the articles' drafters to protect territorial sovereignty.[112] In addition to the U.N. Charter's preamble, Article 51 specifically states the right to self-defense against an "armed attack."[113] However:

> While textual analysis is often telling, it is based on the somewhat suspect premise that a diverse group of diplomatic teams was thoroughly aware of the subtle nuances of language. This is so despite the fact that many members of the teams do not share English . . . as their first language.[114]

By focusing on an attack's consequences and not its means, this approach seems to restrict unlawful uses of force to conventional military attacks that result in destruction and human injury, meaning Stuxnet's disruptive attack on the Natanz facilities would be deemed lawful.[115] Defining force as armed violence opens the door to a wider array of permissive cyber operations: "Computer-based espionage, intelligence collection, or even preemptive cyber-operations or countermeasures designed to disable an adversary's threatening capabilities, for example, would not constitute prohibited force because these attacks do not produce destructive consequences."[116] However, defining the legality of a cyber-attack based on its consequences, the predominant paradigm, is not without its flaws: "[Cyber warfare] challenges the prevailing paradigm, for its consequences cannot easily be placed in a particular area . . . . The dilemma lies in the fact that [cyber warfare] spans the spectrum of consequentiality. Its effects freely range from mere inconvenience . . . to physical destruction . . . ."[117] Thus, defining force as violence would be an incompatible and overbroad standard when applied to cyber warfare.

---

111 *See* NRC COMMITTEE REPORT, *supra* note 79, at 253.

112 U.N. Charter preamble includes the word "armed" when mentioning the goals of the charter.

113 U.N. Charter art. 51.

114 *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 905 (1999).

115 *See* Joyner & Lotrionte, *supra* note 98, at 855.

116 Waxman, *supra* note 109, at 434-35.

117 Schmitt, *supra* note 114, at 912.

2. Force as Coercion

A more expansive view of Article 2(4) is one that reads it as a general prohibition against coercion. While the United States has pushed for a narrower definition focused on military attacks, developing nations have argued for an expansive view of "force" including other forms of pressure such as political or economic coercion.[118] The U.N. Charter clearly prohibits "armed" uses of force, but "withholds comment on other, more subtle forms of 'subversive' coercion that do not involve, at the very least, a perceived threat of armed force. The age of [cyber warfare] invites reconsideration of the restrictive scope of this prohibition."[119] Prior to the advent of cyber warfare, "most coercion could be handily categorized into one of several boxes, for few coercive options existed that could not be typed as political, economic, or armed in nature."[120] One example of force as coercion is an information embargo: "While a naval blockade is a violation of international law, the intentional deprivation . . . of a nation's communications channels (via satellite or otherwise) does not apparently constitute aggression."[121]

Some argue that cyber warfare, with its inherently complex and multifaceted nature, can sometimes constitute force and sometimes not.[122] For example, a cyber-attack that disrupts a nation's air traffic control system resulting in human death can logically be deemed a use of force; however, an attack that disrupts financial institutions but results in no human casualties does not seem to breach the prohibition of force.[123] However it is still possible that the fact that "computer-based information operations in one state could destroy lives and damage property in other states points up the legal rationale for concluding that such activities should be prohibited as a 'use of force' under UN Charter law."[124] Consequently, cyber warfare operations represent a new form of coercion that is distinct from those that were previously available, which necessitates the emergence of new laws and international customs to restrict its use.

The consequentiality paradigm is so dominant that it also seeps into and permeates the analysis of interstate coercion that falls short of armed violence.[125] The starting point in considering non-forceful coercion is whether it amounts to a prohibited intervention; it seems apparent that armed coercion readily qualifies as unlawful intervention.[126] For example, the Declaration on the Inadmissibility of

---

[118] *See* JULIUS STONE, CONFLICT THROUGH CONSENSUS: UNITED NATIONS' APPROACHES TO AGGRESSION 115-36 (1977).

[119] Joyner & Lotrionte, *supra* note 98, at 846.

[120] Schmitt, *supra* note 114, at 908.

[121] Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 289 (1996) (internal citations omitted).

[122] *See* Joyner & Lotrionte, *supra* note 98, at 850.

[123] *See id.* at 855; Schmitt, *supra* note 114, at 916-17.

[124] *See* Joyner & Lotrionte, *supra* note 98, at 850.

[125] Schmitt, *supra* note 114, at 918.

[126] *Id.*

Intervention states that "[n]o State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind."[127] By focusing on the advantages of an act of coercion, the coercion approach, like the armed force approach, is consequentiality-based, leading to more gray area cases.[128]

3. Force as Interference

The third definitional approach to the U.N. Charter's prohibition against "use of force" is focused on interferences with a state's right to sovereign control over its territory. The notion of national sovereignty is one of the most fundamental concepts in international law, and has been well established by the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty.[129] The pertinent part of the resolution states:

> No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned.[130]

While it seems immediately apparent that a cyber-attack on a nation's nuclear facilities undoubtedly constitutes interference, one must first weigh other considerations before reaching such a conclusion.[131] It is often difficult to separate legitimate from illegitimate interferences, and "though perhaps not 'armed force' in the literal sense, resort[ing] to cyber-force may be viewed as a form of intervention that can produce certain harmful or coercive effects in other states."[132] In 1987, the U.N. General Assembly attempted to refine what constitutes a prohibited use of force in its Declaration on the Enhancement on the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations.[133] There, the U.N. stated that an "armed intervention" is connected to "interference or attempted threats against the personality of the State

---

[127] Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131 (XX), U.N. GAOR, 20th Sess. Supp. No. 14, U.N. Doc. A/RES/2131, at 12 (Dec. 21, 1965).

[128] *See* Schmitt, *supra* note 114, at 918-19.

[129] G.A. Res. 2131, *supra* note 120, at 12.

[130] *Id.*

[131] Joyner & Lotrionte, *supra* note 98, at 847.

[132] *Id.* at 848-49.

[133] *See* G.A. Res. 42/22, U.N. Doc. A/RES/42/22 (Nov. 18, 1987).

or against its political, economic, and cultural elements."[134] Thus, the critical question becomes how to locate the point of demarcation between coercion and interference and the use of armed force.[135]

Professor Michael Schmitt, one of the leading sources on characterizing cyber operations, developed a multifactor test for analyzing when a cyber-attack falls under the U.N. Charter's prohibition against the use of force.[136] The so-called "Schmitt Analysis" considers several factors when characterizing the legality of cyber-attacks, which include: severity, immediacy, directness, invasiveness, measurability, and preemptive legitimacy.[137] The Schmitt analysis focuses on permissible and impermissible forms of coercion: "When applying these factors, the more closely the attributes of a cyber operation approximate the attributes of armed force, the more likely states are to characterize the operation as a prohibited use of force."[138] The Schmitt factors consist of the following:

> 1) Severity: Armed attacks threaten physical injury or destruction of property to a much greater degree than other forms of coercion. Physical well-being usually occupies the apex of the human hierarchy of need.
>
> 2) Immediacy: The negative consequences of armed coercion, or threat thereof, usually occur with great immediacy, while those of other forms of coercion develop more slowly. Thus, the opportunity for the target state or the international community to seek peaceful accommodation is hampered in the former case.
>
> 3) Directness: The consequences of armed coercion are more directly tied to the *actus reus* than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition on force precludes negative consequences with greater certainty.
>
> 4) Invasiveness: In armed coercion, the act causing the harm usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the rights of the target state and, therefore, is more likely to disrupt international stability.

---

134 *Id.*

135 Schmitt, *supra* note 114, at 914.

136 Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use of Force" Debate*, 67 JOINT FORCE Q. 40, 42 (2012).

137 *Id.* at 43.

138 *Id.* at 42-43.

> 5) Measurability: While the consequences of armed coercion are usually easy to ascertain (e.g., a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This fact renders the appropriateness of community condemnation, and the degree of vehemence contained therein, less suspect in the case of armed force.
>
> 6) Presumptive Legitimacy: In most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exception such as self-defense.[139]

According to Professor Schmitt, this analysis allows the "force box" to expand.[140] By measuring the consequences of a cyber-attack against the Schmitt factors one can determine whether they fall within the ambit of the Article 2 prohibition on the use of force, or whether they fall outside of the "box."[141]

4. Customary International Law Regarding "Use of Force"

The prohibition on the use of force extends beyond its U.N. Charter context in also constituting customary international law.[142] In an important case, *Nicaragua v. United States*, the International Court of Justice held that a prohibition on the use of force existed in customary law, and that the United States had violated it.[143] In that case, the United States claimed it acted in collective self-defense in supporting the *Contra* guerillas; the Court, however, was not persuaded by the United States' arguments, holding that the United States had violated international law.[144] The court:

> Imposed high bars on the level of violence necessary to constitute an 'armed attack'[145] . . . . But, while these doctrinal approaches may have made sense to a court trying to articulate standards that would constrict opportunities for states to militarily escalate conflict, they did little to address the underlying challenges of contemporary interstate conflict being

---

139 Schmitt, *supra* note 114, at 914-15.

140 *Id.* at 915.

141 *Id.* at 914-15.

142 *See* Statute of the International Court of Justice art. 38, ¶ 1(b), June 25, 1945, 59 Stat. 1055, 3 Bevans 1179.

143 On the issue of customary nature of the prohibition, see Military & Paramilitary Activities in & Against Nicar. (Nicar. v. United States), 1986 I.C.J. 14, 98-101 (June 27).

144 *Id.* at 35.

145 *See* W. Michael Reisman, *Assessing Claims To Revise the Laws of War*, 97 AM. J. INT'L L. 82, 83-84 (2002).

> waged through surrogates and unconventional means[.][146]

It has been said that "treaty law is both more and less flexible than its customary law counterpart."[147] Treaty law is flexible in the sense that it is susceptible to interpretation in an evolving context; it is inflexible in the sense that the prescription itself "is frozen beyond interpretation thereof; new norms require new consent. Customary law, by contrast, is unlimited in scope, but limited by the fact that it cannot react to evolving context[.]"[148] The absence of any extended, significant cyber warfare practice renders analysis of customary international law inappropriate; one may develop over time but does not currently exist:

> [However,] [t]hat is not to say that [cyber warfare] exists wholly beyond the customary international law governing the use of force . . . application of the customary norm to [cyber warfare] would require it to be characterized as a new technique of armed force. In order to rise to this level, it must cause not analogous consequences, but identical results, specifically direct human injury or physical damage to tangible property. Thus, it must fall within the narrow category of computer network attacks that are appropriately characterized as an application of armed force.[149]

The U.N. Charter seems to have been built for a different era of international conflict.[150]

> Efforts to draw clear lines between . . . efforts regarded as short of 'force' and prohibited offensive attacks raise tough questions of how to measure and judge the consequences . . . of hostile intrusions, as well as tough technical questions of distinguishing intelligence collection . . . from initiation of offensive operations . . . . In cyberspace, these activities may look identical, especially in real time.[151]

While arguably outdated, the U.N. Charter is not completely devoid of any and all applicability to cyber warfare. Classifying cyber warfare as a lawful act of espionage could have the effect of making it a permitted use of force under Article 2(4) of the Charter.[152]

---

146 Waxman, *supra* note 109, at 446-47.

147 Schmitt, *supra* note 114, at 921.

148 *Id.*

149 *Id.* at 922.

150 Waxman, *supra* note 109, at 443.

151 *Id.* at 435 (citing NRC COMMITTEE REPORT, *supra* note 84, at 121-26, 135-42).

152 James P. Terry, Book Review, *Cyberspace and the Use of Force*, 9 DUKE J. COMP. & INT'L L. 491, 493 (1999).

> [U]nder international law, the intruding state may be conducting lawful acts of espionage that may not be considered a use of force in violation of Article 2(4) of the Charter. [Walter Gary Sharp] carefully explains that espionage conducted by the nonconsensual penetration of another state's computer systems is lawful under existing international law when it does not violate systems so vital that their incapacity or destruction would have a critical destabilizing effect on the national security of a state.[153]

As Sharp points out, espionage is considered an essential part of a state's fundamental right to self-defense.[154] The 1907 Hague Convention explicitly recognizes the lawfulness of espionage.[155] In light of this, "[c]omputer-based espionage, intelligence collection, or even some preemptive cyber-operations or countermeasures designed to disable an adversary's threatening capabilities, for example, would generally not constitute prohibited force because these activities do not produce destructive consequences analogous to a kinetic military attack."[156] Sharp states that the threshold question of when a cyber-attack or cyber-espionage activity constitutes a "threat or use of force" under the U.N. Charter is a subjective one:

> Computer espionage [and] computer network attacks . . . may all constitute a use of force in CyberSpace [sic]. Although a use of force does not always rise to the scope, duration, and intensity threshold of an armed conflict that invokes a state's right of self-defense, international law clearly permits a state to respond in self-defense when attacked through CyberSpace [sic].[157]

While espionage during times of armed conflict is almost universally accepted under customary international law, it is, however, unlawful under the domestic law of most nations during peacetime.[158]

---

153 *Id.*
154 WALTER GARY SHARP SR., CYBERSPACE AND THE USE OF FORCE 123 (1999).
155 *See* Hague Convention IV, *supra* note 2, arts. 24, 29-31.
156 Waxman, *supra* note 109, at 434-35.
157 SHARP SR., *supra* note 154, at xiv.
158 *Id.* at 123-24.

F. Existing International Regulatory Framework

The Geneva Convention established most of the existing international laws regarding warfare.[159] The Geneva Convention is a series of treaties that was first aimed at establishing international regulations governing the treatment of the wounded and prisoners of war.[160] In 1977, nations met to reaffirm the existing Geneva Convention.[161] The nations also ratified an amendment, Additional Protocol 1, which added provisions and clarifications to accommodate the developments in modern international warfare that had occurred since the end of World War II.[162] Article 36 of Additional Protocol 1 pertains to novel methods and means of war.[163] It also records the affirmative duty of states that develop or acquire "a new weapon, [or] means or method of warfare . . . to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable."[164] The drafters of Protocol 1 seemed to have had the Internet, or its equivalent, in mind despite not fully understanding its future implications in saying, "in short, all predictions agree that if man does not master technology, but allows it to master him, he will be destroyed by technology."[165]

While NATO and individual nation-states have taken it upon themselves to address the growing concerns posed by cyber warfare, the U.N. has been slower to address cyber warfare.[166] In 2009, President Obama appointed Howard Schmidt to head the new position of "cyber czar" to handle cyber warfare issues and developments.[167] In January 2010, the Secretary General of the U.N. International Telecommunications Union spoke at a World Economic Forum where he pushed for an international treaty to prevent cyber war.[168] The treaty framework would mirror a peace treaty before a war: "He proposed a treaty in which countries would engage not to make the first cyber strike against another

---

159 *See* ICRC *Laws of War*, *supra* note 2.

160 *Id.*

161 *See Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts*, MILITARY LEGAL RESOURCES, http://www.loc.gov/rr/frd/Military_Law/RC-dipl-conference-records.html (last visited Apr. 6, 2014).

162 *See* Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 36, June 8, 1977, at Part III [hereinafter ICRC Protocol 1].

163 *Id.*

164 *Id.*

165 *See id.* at *General Remarks 1476(22)*.

166 *See UN Chief Calls for Treaty to Prevent Cyber War*, AM. FREE PRESS (Jan. 30, 2010), http://www.google.com/hostednews/afp/article/ALeqM5h8Uvk-jpSvCWT-bqYSg1Ws4I4yAA.

167 *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.

168 *See UN Chief Calls for Treaty to Prevent Cyber War*, *supra* note 166.

nation. 'A cyber war would be worse than a tsunami – a catastrophe,' the UN official said, . . . highlighting examples such as attacks on Estonia last year."[169] Despite the fact that Secretary General Hamadoun Touré's proposals have yet to be adopted as the official stance of the U.N., it seems to be evident that the principal international body has begun to consider cyber warfare as a pertinent issue.

In 2001, the Council of Europe met in Budapest to hold the Convention on Cybercrime.[170] It was the first international meeting governing Internet crime, and it covered a broad range of activities.[171] Article 4 of the Convention stated, "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right."[172] This broad description seems to encompass most types of information operations that comprise cyber warfare. The terms "alteration" and "suppression" would apply to the DDoS cyber-attacks suffered by Estonia and Georgia because the intentional flooding of computer networks definitely suppressed and altered the victims' technological capabilities.[173]

The U.N. Charter allows for only two situations where the use of force is permitted: Security Council authorized operations pursuant to Chapter VII and acts of self-defense in accordance with Article 51.[174] Under Chapter VII, the U.N. Security Council has the authority to "determine the existence of any threat to peace, breach of peace, or act of aggression."[175] In such an instance, the Council can call upon U.N. member nations to apply measures "not involving the use of armed force . . ."[176] to resolve the situation, and should those measures fail or be futile, it may "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security."[177] It must be stated that techniques of cyber warfare seem to fall under Article 41 of the Charter in that "complete or partial interruption of . . . telegraphic, radio, or other means of communication" are "measure[s] not involving the use of armed force . . . ."[178] Article 51 states that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an *armed attack* occurs against a

---

169 *Id.*

170 *See Summary of the Convention on Cybercrime*, COUNCIL OF EUR., http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm (last visited Mar. 3, 2014); *see also* Convention on Cybercrime, Nov. 23, 2001, E.T.S No. 185.

171 *Summary of the Convention on Cybercrime*, *supra* note 170.

172 Convention on Cybercrime, *supra* note 170, art. 4.

173 *See A Look at Estonia's Cyber Attack in 2007*, *supra* note 44; *see also Marching off to Cyberwar*, *supra* note 46.

174 Schmitt, *supra* note 109, at 924.

175 U.N. Charter art. 39.

176 *Id.* art. 41.

177 *Id.* art. 42.

178 *Id.* art. 41.

Member of the United Nations . . . ."[179] However, the question remains of when a cyber-attack amounts to a "threat to peace, breach of peace, or act of aggression such that the Council may authorize a response by armed force?"[180]

In 1974, well before cyber-attacks were on diplomats' radar, the General Assembly defined aggression as **"**the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any manner inconsistent with the Charter of the United Nations. . . ."[181] This definition of aggression would seemingly only cover cyber warfare to the extent that a cyber-attack is intended to cause direct damage or injury.[182] Others have defined aggression as a threat to or breach of peace, which begs the question of what is "peace"?[183] If "peace" were defined as the absence of force, which in turn is used as the standard for characterizing aggression, then the U.N. Security Council would be able to react forcefully to any cyber-attack that might provoke a breach of peace.[184]

The other situation in which use of force is permitted by the U.N. charter, outside of Security Council authorized operations under Chapter VII, is an act of self-defense pursuant to Article 51.[185] Article 51 addresses the reality that often the international community will not be able to react quickly enough to prevent or forestall armed aggression on a victim state.[186] A state's right to self-defense is qualified and restricted to situations involving an armed attack.[187]

> Although coercion not involving armed force may violate Article 2(4) and result in action under Article 39, it does not follow that states may react unilaterally pursuant to Article 51 . . . . Thus faced with [cyber warfare] that does not occur in conjunction with, or as a prelude to, conventional military force, a state may only respond with force in self-defense if the [cyber-attack] constituted armed force . . . i.e., that is intended to directly cause physical destruction or injury . . . . The victim state . . . could not respond forcefully thereto on its own accord.[188]

However, this analysis only applies to cyber-attacks that occur in isolation, and the prevailing standard holds that an attack must be imminent before the right to

---

[179] *Id.* art. 51 (emphasis added).
[180] Schmitt, *supra* note 109, at 925.
[181] Definition of Aggression, G.A. Res. 3314 (XXIX), art. 1, U.N. GAOR, 29th Sess., Supp. No. 31, U.N. Doc. A/9631, at 142 (Dec. 14, 1974).
[182] Schmitt, *supra* note 109, at 925.
[183] *See id.* at 926.
[184] *Id.* at 927.
[185] U.N. Charter art. 51.
[186] Schmitt, *supra* note 114, at 928.
[187] *See* U.N. Charter art. 51.
[188] Schmitt, *supra* note 114, at 928-29.

self-defense matures.[189] Former U.S. Secretary of State Daniel Webster approached the right to self-defense from a different angle, articulating an "anticipatory" right to self-defense in the *Caroline* incident.[190] Under this anticipatory approach, cyber-attacks may be used lawfully as a means of preemptive self-defense, or in other words, self-defense can be either a preventative or responsive measure.[191] The basic premise underlying the principle of anticipatory self-defense is "that the use of force by one state against another is permissible . . . if the use of force to respond is both really necessary and not excessive in relation to the perceived threat."[192] There has been no international consensus on the merits of anticipatory self-defense, but there has also been no universal consensus opposing the concept so long as the threat is real and immediate.[193]

> Defense in advance of the attack is legitimate if the potential victim must immediately act to defend itself in a meaningful way and if the potential aggressor has irrevocably committed itself to attack . . . . A wide array of computer network attack operations executed to prepare the battle space may meet this standard. By the anticipatory self-defense standard, the right of the state to respond forcefully to them would depend not so much on the nature of the information operation, as on its significance vis-à-vis the coming armed attack.[194]

Schmitt states that the right to respond forcefully in self-defense to a cyber-attack that, by itself, does not constitute an armed attack depends on three factors: whether the cyber-attack is part of an overall operation culminating in an armed attack, whether the cyber-attack is an irrevocable step in an imminent and probably unavoidable attack, and whether the defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack.[195]

---

189 *Id.* at 930.

190 *Id.*

191 Joyner & Lotrionte, *supra* note 98, at 857.

192 *Id.*

193 For a discussion of the various views of international scholars regarding the legitimacy of anticipatory self-defense under Article 51, see ANTHONY C. AREND ET AL., INTERNATIONAL LAW AND THE USE OF FORCE: BEYOND THE UN CHARTER PARADIGM 73 (Psychology Press ed., 1993).

194 Schmitt, *supra* note 114, at 932.

195 *Id.* at 933.

III. ANALYSIS

One of the basic premises underlying the law of war is proportionality; the collateral damage caused must be proportional to the military advantage gained.[196] However, determining proportionality is almost impossible when the attack suffered cannot be classified as an act of war under existing international law. How far can a nation go in using conventional warfare to avenge itself from a cyber-attack? This is the question this Note undertakes to answer. Applying current international law to the Stuxnet attack in Iran leaves one with few definitive answers. It is true that often the law cannot keep pace with the rapid advancements in technology that are being made on a daily basis.[197] However, I believe proposing a clear-cut definition of cyber warfare and the military responses it warrants is difficult yet necessary. One of the fundamental limitations on the use of force in self-defense is the principle of proportionality, which "balances positive consequences (military advantage) against harmful ones (collateral damage and incidental injury)."[198]

> [A]ttacks that are not linked to physical conflict or traditional forms of war are difficult to categorize . . . . Furthermore, retaliation becomes a problem because some interpret the present rules of engagement as forbidding any response that might produce collateral damage affecting actors other than those directly engaged in the conflict. The problem is that because there is no blueprint of the Internet . . . it is very difficult to gauge what the unintended consequences of a cyber-attack would be.[199]

Proportionality and reasonableness are the main requirements in justifying armed force as self-defense.[200] Basically, a given level of cyber-force is appropriate as self-defense by a victim state if it is necessary and proportional to the force used by the aggressor state in the initial attack.[201]

Modern infrastructure relies heavily on telecommunications and computer networking.[202] Traffic lights, bridges, radio transmissions, nuclear facilities and many other critical components of a nation's infrastructure are

---

196 Thomas Hurka, *Proportionality in the Morality of War*, 33 PHIL. & PUB. AFFS. 34, 35 (2005) (discussing the fundamental principles of just war theory).

197 *See generally* LEON L. FOSTER, LEGAL ISSUES AND RISKS ASSOCIATED WITH BUILDING INFORMATION MODELING TECHNOLOGY 21(2008).

198 Schmitt, *supra* note 114, at 917-18.

199 CORDESMAN & CORDESMAN, *supra* note 97, at 6-7.

200 Joyner & Lotrionte, *supra* note 98, at 857.

201 *Id.*

202 *See Marching off to Cyberwar*, *supra* note 47.

intertwined with computer networks.[203] Banking institutions, with the growth of wired transactions in modern years, would be crippled by a similar DDoS attack that stymied Estonia.[204] Due to information itself being a valuable asset, "enemy command and control systems have actually become the primary targets in modern warfare . . . . Against a technologically competent adversary, information will be the principal determinant of victory."[205] The proliferation of cyber warfare is logically correlated to the increasing governmental and financial reliance on telecommunications.

Whether Iran is still attempting to design and build an atomic bomb is uncertain.[206] The Islamic Republic has continuously stated whatever nuclear program they do maintain is for peaceful purposes.[207] Recently, Director General of the International Atomic Energy Agency (IAEA), Yukiya Amano, confirmed that a large portion of Iran's nuclear facilities under IAEA supervision are conducted for peaceful purposes.[208] One of Iran's nuclear facilities is located in Natanz, where it has "constructed both a pilot and commercial gas centrifuge-based uranium enrichment facility[.]"[209] Enriching uranium produces fuel for nuclear reactors, but uranium enrichment can also produce fissile material to be used in nuclear weapons;[210] "[c]entrifuges are finely calibrated cylindrical devices that spin at supersonic speed to increase the fissile element in uranium so that it can serve as fuel for nuclear power plants or, if refined to a much higher degree, for atomic bombs."[211] While Stuxnet did disrupt operations at the Natanz facilities, as of November 2010, the facilities' enrichment operations had been resumed.[212] The United States and Israel have repeatedly maintained that Iran is

---

[203] PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROT., CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 12 (1997), *available at* http://www.fas.org/sgp/library/pccip.pdf.

[204] *See A Look at Estonia's Cyber Attack in 2007*, *supra* note 47; *see also* Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1.

[205] Kanuck, *supra* note 121, at 282.

[206] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&.

[207] Al Pessin, *UN Airs New Concerns After Iran Says Nuclear Program Peaceful*, VOICE OF AMERICA (Aug. 30, 2012), http://www.voanews.com/content/iran-khamenei-rules-out-nuclear-bomb/1498406.html.

[208] *Iran Nuclear Program Peaceful: IAEA Chief*, PRESSTV (Nov. 11, 2012), http://www.presstv.ir/detail/2012/11/11/271619/iran-nuclear-energy-program-pea ceful/.

[209] PAUL K. KERR ET AL., CONG. RESEARCH SERV., R41524, THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY 4 (2010).

[210] *Id.*

[211] Fredrik Dahl & Sylvia Westall, *Technical Woes Halt Some Iran Nuclear Machines – Dips*, REUTERS (Nov. 23, 2010), http://www.reuters.com/article/2010/11/23/us-nuclear-iran-problems-idUSTRE6AM1L520101123.

[212] *See* U.N. Director General, *Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran:*

pursuing military objectives in its nuclear energy program.[213] This fear of Iran possessing a nuclear weapon culminated in one of the most well-known cyber-attacks to date, the Stuxnet attack, on Iran's Natanz facilities.[214]

The cyber worm named "Stuxnet" was discovered in June 2010.[215] When the murky waters of cyberspace finally cleared, Stuxnet infected over 60,000 computers, half of which were Iranian; other countries infected by the virus included: the United States, India, the United Kingdom, Germany, Australia, China, Indonesia, and Finland.[216] Stuxnet is a form of malicious software (malware) designed to disrupt a Microsoft Windows-based application employed by an Iranian industrial control system.[217] Industrial control systems (ICS) assist in the management of equipment used in critical infrastructure facilities, in this case the nuclear facility in Natanz.[218] One expert, Ralph Langner, described Stuxnet as "a military-grade cyber missile that was used to launch an 'all-out cyber strike against the Iranian nuclear program.'"[219] The worm was uploaded not by accessing computers connected to the public Internet, but through the use of intermediate devices such as thumb drives.[220] Stuxnet targeted computer systems that were used to control the functioning of a nuclear power plant, and "[o]nce inside the system, Stuxnet had the ability to degrade or destroy the software on which it operated."[221] Stuxnet's ability to manipulate system controls to the point of causing long-term damage or rendering them inoperable makes these cyber worms very attractive to military strategists.[222] Specifically, "Stuxnet [changed] the output frequencies and thus the speed of the motors for short intervals over a period of months. Interfering with the speed of the motors sabotages the normal operation of the industrial control process."[223] Stuxnet's potential to damage a nation's critical infrastructure, infrastructures that are becoming increasingly interconnected, threatens a government's ability to protect national security interests.[224]

Rep. of the Director General, U.N. Doc. GOV/2010/62 (Nov. 23, 2010).

213 *Iran Nuclear Program Peaceful: IAEA Chief*, *supra* note 208.

214 *See generally* Farrell & Rohozinski, *supra* note 20, at 29.

215 *Id*. at 23.

216 *Id.*

217 KERR ET AL., *supra* note 209, at 1.

218 KEITH STOUFFER ET AL., U.S. DEP'T OF COMMERCE, GUIDE TO INDUSTRIAL CONTROL (ICS) SYSTEMS 1 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

219 Farrell & Rohozinski, *supra* note 21, at 23.

220 KERR ET AL., *supra* note 209, at 1 (stating that a thumb drive is a data storage device).

221 *Id.* at ii.

222 *Id.*

223 Farrell & Rohozinski, *supra* note 21, at 24-25 (quoting Symantec researcher Eric Chien).

224 KERR ET AL., *supra* note 209, at ii.

While Stuxnet was disruptive, its overall impact on Iran's nuclear facilities is unclear.[225] Iranian President Mahmoud Ahmadinejad stated that the cyber-attacks "were able to cause minor problems with some of our centrifuges by installing some software in electrical parts . . . . They misbehaved but fortunately, our experts discovered it."[226] However, this statement could easily be seen as damage control, and Western diplomats believed the ramifications of the Stuxnet attack were greater than Iran let on.[227]

IV. IMPLICATIONS

A U.N. treaty classifying cyber-attacks as conventional military belligerence, while unlikely to be agreed upon, gives the state subject to such attacks the necessary right to defend its national sovereignty to the utmost extent. While there is uncertainty over what a "use of force" is in cyberspace under the U.N. Charter,[228] such a treaty would clearly define what constitutes an act of cyber warfare. There are several ways in which such a treaty could be crafted, one of which is a no-first-strike agreement.

Stuxnet has raised concerns about the vulnerabilities in crucial U.S. infrastructures.[229] Former U.S. President Bill Clinton established the President's Commission on Critical Infrastructure Protection in 1997, one of the first major threat assessments and characterizations.[230] The Commission on Critical Infrastructure Protection identified five major types of possible acts, including espionage and shutting down service amongst others.[231] The U.S. Department of Homeland Security has since labeled sixteen infrastructure sectors as "essential to the nation's security, public health and safety, economic vitality, and way of life."[232] Some major ICSs are controlled by computers that can be accessed from remote locations connected to the ICS, and can also be accessed through the ever-growing use of mobile-wireless devices.[233] One such ICS that can be accessed wirelessly is the Supervisory Control and Data Acquisition (SCADA) system, which controls industrial processes and infrastructure operations.[234] This is particularly worrisome because "unclassified reports suggest that the Stuxnet worm was specifically developed to seek out and exploit vulnerabilities in

---

225 *Id.* at 5.

226 *Id.* (quoting statement of Iranian President Mahmoud Ahmadinejad).

227 *See* Dahl & Westall, *supra* note 211.

228 SHARP SR., *supra* note 96, at 7.

229 KERR ET AL., *supra* note 209, at 6.

230 CORDESMAN & CORDESMAN, *supra* note 97, at 13.

231 *Id.*

232 *Critical Infrastructure Sectors*, U.S. DEPT. OF HOMELAND SEC., http://www.dhs.gov/critical-infrastructure-sectors (last visited Mar. 3, 2014).

233 KERR ET AL., *supra* note 209, at 6.

234 *Id.*

software that manages ICSs found in most critical infrastructure facilities."[235] Shutting down the power grid on Wall Street, for example, would result in a crippling blow to the already precarious global financial market.[236] In 2009, the Department of Homeland Security conducted an experiment known as the Aurora Project. [237] The Aurora Project was a simulated cyber-attack on SCADA, and it demonstrated the system's vulnerabilities. [238] Aurora attacked the SCADA systems that control power generators and grids, causing them to shut down and cease operations. [239] These vulnerabilities could exist in other critical infrastructure.[240]

Several commentators have noted that it may be difficult to identify the point at which a successful attack would be serious enough to justify federal intervention.[241]

> From the perspective of any given business or [non-governmental organization], a catastrophic attack on its information systems could be crippling or have massive consequences. However, from a national perspective, businesses . . . fail or suffer crippling damage for many reasons and the nation has survived. Major temporary failures in the operation of communications systems, commerce, utility services, stock transactions, et cetera are an ongoing fact of life.[242]

The federal government has conducted only a limited number of similar tests and exercises to evaluate cyber vulnerabilities, leading some to argue for an annual cyber assessment to determine when and where federal intervention is necessary.[243] That is not to say the U.S. federal government has not taken measures to protect critical infrastructure: "Total funding for critical infrastructure protection has risen from [U.S.] $1.4 billion in [1998] to [U.S.] $2.03 billion in [2001], and the U.S. is steadily improving its intelligence and law enforcement efforts."[244] However, U.S. law enforcement's jurisdiction ends at the national borders while cyber-attacks and cyber-crime do not.[245]

Some commentators disagree that new treaties or conventions are necessary, arguing that the existing U.N. Charter provisions adequately address

---

235 *Id.*
236 *See id.*
237 *Id.*
238 KERR ET AL., *supra* note 209, at 6.
239 *Id.*
240 *Id.*
241 CORDESMAN & CORDESMAN, *supra* note 97, at 4.
242 *Id.*
243 *Id.* at 5.
244 *Id.*
245 *Id.* at 8.

cyber warfare implications.[246] In Gary Sharp's book, *Cyberspace and the Use of Force*, the editor of the U.N. Peace Operations stated that certain activities in cyber space constitute armed attacks and are therefore subject to customary international law and U.N. provisions regarding the illegal use of force.[247] The NRC Committee concluded that the current framework provided by the U.N. Charter does apply to cyber warfare:

> Prior to the outbreak of an acknowledged armed conflict, if the effects (including both direct and indirect effects) produced by a cyberattack [sic] would, if produced by other means, constitute an armed attack in the sense of Article 51 of the UN Charter, the cyberattack [sic] would likely be treated as an armed attack. Similarly, if a cyberattack [sic] has the same effects and is otherwise similar to governmentally initiated coercive or harmful actions that are traditionally and generally not treated as the "use of force" (e.g., economic sanctions . . .), such a cyberattack [sic] would likely not be regarded as an action justifying a use of force in response.[248]

Like many proposed international conventions and treaties, such as a new convention that expressly characterizes cyber-attacks as a "use of force," those affected most by it will have objections, as evidenced by the statement of former director of U.S. intelligence John Negroponte, that intelligence agencies in the major powers would be the first to "express reservations" about such an accord.[249] That being said, in 2003 the ICRC stated that the existing legal framework is sufficient to deal with present day conflicts.[250] Professor Schmitt argues for a presumption operating in favor of inclusivity of cyber warfare under the existing prohibition of "use of force" under Article 2 of the U.N. Charter.[251] It can be said that the issue "is not legality, but rather illegality by what standard."[252] Schmitt believes that such a presumption would foster shared community values within the security framework of the Charter.[253] The counterargument is that a presumption

---

[246] Dondi S. West, *A Survey and Examination of the Adequacy of the Laws Related to Cyber Warfare*, DEF CON 24, www.defcon.org/images/defcon-18/dc-18-presentations/West/DEFCON-18-West-Laws-Cyber-Warfare-WP.pdf (last visited Mar. 3, 2014) (arguing that the current rules of international law, embodied within the U.N. Charter, are sufficient to address the emerging issues of cyber warfare).

[247] *See* SHARP SR., *supra* note 154, at ix.

[248] NRC COMMITTEE REPORT, *supra* note 84, at 4.

[249] *See UN Chief Calls for Treaty to Prevent Cyber War*, *supra* note 159.

[250] 28th International Conference on the Red Cross and Red Crescent, Geneva, Switzerland, Dec. 2-6, 2003, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, at 4, Doc. 03/IC/09 (2003).

[251] Schmitt, *supra* note 114, at 919.

[252] *Id.*

[253] *Id.*

"labeling uncertain cases as a use of force would be destabilizing, for the victim would be likely to respond forcefully. However . . . it is not the use of force, but rather [an] 'armed attack' which gives a state the right to respond in self-defense."[254]

It may be the case that, due to the politicking that would surround any new proposal to amend the U.N. Charter to include cyber warfare as a "use of force," a new treaty or convention would be simply impossible to pass. Consequently, an arms control treaty that bans or restricts the development and use of cyber weaponry seems unlikely to come to fruition. Should such a treaty somehow be passed, it could have a harmful effect on domestic cyber security; also, it would be seemingly unenforceable due to difficulties in detecting the production of cyber weapons and the aforementioned problem of attribution.[255] So where does this leave international law regulating cyber warfare? Would an international treaty regulating cyber warfare even be desirable? Many commentators have answered the latter question in the negative.[256] One commentator believes cyber capabilities are evolving too fast, preventing such a treaty from being enforceable or workable,[257] while another believes such a treaty would prevent nations from using a non-violent weapon, thus resulting in more human casualties.[258] Are these difficulties and concerns enough to preclude even an attempt to bring cyber warfare in line with current international treaties?

Bruce Schneier believes an international cyber warfare treaty is not only workable, but necessary.[259] The first step to any effective treaty is to start negotiations. The international community recognizes the growing threat posed by cyber warfare, and simply needs to get the ball rolling: "The very act of negotiating limits the arms race and paves the way to peace."[260] Schneier proposes that one approach to creating a cyber warfare treaty would involve a no-first-use policy and outlawing broadly targeted weapons aimed at civilian infrastructure.[261] A no-first-use policy would mirror the one nations have already

---

[254] *Id.* at 919-20.

[255] *See Cyber Warfare*, *supra* note 22.

[256] Jon Lindsay, *International Cyberwar Treaty Would Quickly Be Hacked to Bits*, U.S. NEWS (June 8, 2012), http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/international-cyberwar-treaty-would-quickly-be-hacked-to-bits.

[257] *Id.*

[258] Lawrence Muir Jr., *Cyberwarfare a Viable Nonviolent Alternative to Military Strikes*, U.S. NEWS (June 8, 2012), http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/cyberwarfare-a-viable-nonviolent-alternative-to-military-strikes.

[259] *See* Bruce Schneier, *An International Cyberwar Treaty Is the Only Way to Stem the Threat*, U.S. NEWS (June 8, 2012), http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/an-international-cyberwar-treaty-is-the-only-way-to-stem-the-threat.

[260] *See* Schneier, *supra* note 77.

[261] *Id.*

pledged to uphold in regards to nuclear weapons [262] in that nations would agree not to engage in cyber warfare unless it was first attacked by an adversary using cyber warfare tactics. Again, I doubt whether nations would agree to such a pledge considering that NATO has already rejected the no-first-use policy in regards to nuclear weapons. Additionally, an attempt to use conventional ground and air forces to respond to a cyber-attack would seemingly violate the proportionality requirement underlying the right to self-defense.

After cutting through the red-tape and politics that engulf any proposed international treaty or convention, the possibility of bringing cyber warfare under a workable international regulatory framework seems to come back to how one interprets the U.N. Charter's meaning of "force."[263] As of this writing, under both customary international law and the existing regulatory framework, it seems that nations are free to conduct cyber warfare activities, "perhaps even in peacetime, without significant legal repercussions."[264] The current paradigm, or lack thereof, seems to suit the United States fairly well as it is a world leader in cyber warfare development, as evidenced by the attack on the Natanz facilities in Iran.

> In the absence of conclusive authority indicating, say, that particular information warfare attacks are 'armed attacks,' . . . or 'force,' the United States can act with some confidence that its acts will not be held to be so. Given its position in the world, the United States will have the opportunity to be in the state practice that can establish international norms and, perhaps, customary international law . . . . [However,] [j]ust as the United States can attack, it can be attacked, and its actions in conducting attacks may provide precedent for attacks against it and its allies.[265]

However, enduring hegemonic domination in cyberspace is neither realistic nor achievable by the United States.[266]

The U.N. Charter's provisions regarding the use of "force" are a reasonable starting point for creating an international regulatory framework for cyber warfare.[267] While a logical starting point, the Charter is not without its deficiencies; the first step in reconciling cyber warfare and international law would be to "clarify the [ambiguities] of such terms as 'armed attack,' 'force,' and others, so that the status of information warfare attacks under international

---

[262] Richard H. Ullman, *No First Use of Nuclear Weapons*, COUNCIL ON FOREIGN AFFAIRS (July 1972), http://www.foreignaffairs.com/articles/24355/richard-h-ullman/no-first-use-of-nuclear-weapons (subscription publication).

[263] West, *supra* note 246, at 8.

[264] LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 34 (1998).

[265] *Id.*

[266] NRC COMMITTEE REPORT, *supra* note 84, at 5.

[267] *Id.*

law is understood."[268] The current framework underpinning Article II also fails to account for non-state actors, and for the technical characteristics of many cyber warfare attacks.[269]

It is my suggestion that Iran, as a prominent and powerful victim of cyber warfare, propose a convention that clearly constitutes cyber warfare as a "use of force," with force being defined in terms of interference, that extends equally to both state and non-state actors alike. To get the proverbial ball rolling, Iran could move for declarations of the U.N. General Assembly interpreting the Charter's applicability to cyber warfare. This convention would not be an attempt to draft a new U.N. Charter, or a novel arms-control treaty, but rather a method of bringing cyber warfare under, and in harmony with, existing international treaties and conventions. One way to do so would be to pursue an "international [understanding] that the financial or other intangible damages caused by certain types of nonlethal information attacks are, indeed, the types of injuries against which humanitarian law should protect noncombatants."[270]

The utilization of cyber warfare tactics by private individuals and other non-state actors would serve as a hindrance to the efficacy of any new, potential international regulation, primarily due to attribution difficulties.[271] One way to extend this proposed convention's reach to non-state actors would be for nations seeking to regulate cyber warfare to use diplomatic pressure to promote the criminalization of computer-based attacks in countries that have yet to recognize such attacks as crimes.[272] This criminalization on a national scale would serve two functions: "[T]o encourage other countries to discourage such behavior by individuals within their borders, and to enable extradition of offenders."[273] Development of an extradition agreement would contribute to an international norm obligating states to cooperate in resisting and punishing such attacks by non-state actors.[274]

The option of pursuing some arms control ban on cyber warfare attacks or control of cyber warfare weaponry seems to be both unlikely and ineffective.

> An information weapons ban would pose problems because not only do many information weapons have dual military and civilian uses, but their applications are predominately civilian. Because of technological diffusion, the small size of much information technology, and its primary incorporation into consumer goods, an arms control regime would seem difficult to enforce.[275]

---

268 GREENBERG ET AL., *supra* note 264, at 34.
269 NRC COMMITTEE REPORT, *supra* note 84, at 5.
270 GREENBERG ET AL., *supra* note 264, at 35.
271 Waxman, *supra* note 109, at 456.
272 *Id.*
273 *Id.*
274 *Id.* at 36.
275 *Id.* at 36-37.

As stated earlier, a total cyber warfare arms control ban would be unworkable due to the complications that arise from attributing the attack to another nation, and its inapplicability to non-state actors. Actions taken in cyberspace are conducted in milliseconds, which complicate potential regulations.[276] Additionally, "many arms controls treaties are built upon inspection, verification, and compliance regimes. As nefarious activities in cyberspace defy geographical boundaries and often attribution, how would such activities be conducted in a cyber arms control treaty?"[277] "Proliferation is a real problem, and no country is prepared to deal with it," said Melissa Hathaway, a former U.S. national cyber-security coordinator; "[t]he widespread availability of the attack techniques revealed by current software has set off alarms among industrial control specialists, she said: 'All of these guys are scared to death.'"[278] As previously mentioned, the U.N. Charter seems to have been created for a different era of international conflict. Like the earlier proxy conflicts in Nicaragua:

> [C]yber-conflict is likely to feature disputed facts about what exactly occurred, including who committed the electronic disruption and on whose behalf they did it. In some respects, those problems will likely be vastly exacerbated in the cyber-context because of the participant's greater ability to mask or anonymize [sic] their identity and because the 'movements' and 'terrain' of cyber-warfare can be dispersed across global information networks and will often be carried out on private infrastructure.[279]

The dissipated nature of cyber warfare, and cyberspace in general, seems to be a conceptual hindrance when applied to existing and proposed international regulatory frameworks.[280]

V. CONCLUSION

The emergence of cyber warfare, as made especially evident by the Stuxnet attack on Iran's nuclear facilities at Natanz, has necessitated a shift in the international paradigm regarding "use of force" and national security law. The dissipated nature of and anonymity afforded by the cyber-attacks "undermines deterrence and limits a state's ability to use force in self-defense. Maintaining a credible ability to use force in CyberSpace [sic] is, however, lawful and a

---

[276] *See* KERR ET AL., *supra* note 209, at 8.

[277] *Id.*

[278] John Markoff, *A Silent Attack, but Not a Subtle One*, N.Y. TIMES (Sept. 26, 2010), http://www.nytimes.com/2010/09/27/technology/27virus.html?_r=0.

[279] Waxman, *supra* note 109, at 447.

[280] *Id.* at 443-44.

fundamentally important aspect of deterrence and the maintenance of international peace and security."[281] While its military usefulness is readily apparent, the question this Note sought to answer is whether the Stuxnet attack constituted a "use of force" under the U.N. Charter, and if so what retaliatory measures are legally available to Iran.

Much of the legal analysis surrounding the Stuxnet attack centers on the prohibition against the "use of force." There are three commonly accepted interpretations of "force": force as armed violence, force as coercion, and force as interference. Most scholars and experts on the subject agree that the use of cyber-attacks will generally not constitute armed violence, but the waters become murkier when the definition of "force" becomes broader. By focusing largely on an attack's consequences, defining force as armed violence allows for too permissive of a standard. Defining force as coercion would lead to an unacceptable number of gray area cases. While the first two interpretations have significant incompatibilities with cyber warfare, the third definitional approach to the U.N. Charter's prohibition against "use of force," force as interference/disruption, is focused on the interference with a state's right to sovereign control over its territory. Disruption of a nation's critical infrastructure, in Stuxnet's case the interference of system controls at nuclear centrifuging facilities, can cause significant property and fiscal damage. Should a nation overcome the complexities of attributing an attack to a specific belligerent, and "even if such intentional [disruptive] activities are an unlawful use of force that unequivocally invokes a victim state's right to self-defense, that right of self-defense does not necessarily justify a use of force in response."[282] It is for this reason that the principle of proportionality is a limiting principle in regards to how Iran can legally respond to the Stuxnet attack. In summation, violations of international law can constitute a use of force within the meaning of Article 2 of the U.N. Charter if they involve an exercise of power in the territory of another sovereign, even without the use of arms, but the response in self-defense must be necessary and proportional.[283]

While amending the current U.N. Charter or ratifying a new international treaty is highly unlikely, in order to vindicate its rights as a national sovereign, Iran should seek a new international convention that clearly delineates lawful cyber-attacks from unlawful cyber-attacks. By defining force as intervention, such an international convention would be an attempt to bring cyber warfare into harmony with existing international treaties and conventions. However, any measure beyond a convention seems unworkable; any arms control ban is unlikely to be signed by stronger nations that already possess cyber warfare capabilities. An arm's control ban would likewise prove unworkable due to the difficulties in attributing cyber-attacks to any one nation with certainty. Cyber-attacks take just seconds to occur, and most informational weapons have both civilian and military

---

281 SHARP SR., *supra* note 154, at xiv.
282 *Id.* at 103.
283 *Id.* at 100.

purposes. While informational weapons have both civilian and military aspects/purposes, any such ban would be nearly impossible to enforce since cyber space is predominately incorporated into legal consumer goods.

Until a nation with the requisite international authority and power becomes adversely affected by the use of cyber warfare, the use of cyber weaponry will continue to be highly unregulated and will only fall sparsely under a patchwork of the existing international regulations. Unless customary international law and interpretation of the U.N. Charter's use of force are altered, elevating cyber warfare to an act of conventional belligerence against a nation's sovereignty, Iran seems to be stuck without further recourse to the damage inflicted by the Stuxnet virus.