1-1-2013

The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors

Christopher D. DeLuca
Pace University School of Law, cdeluca@law.pace.edu

PACE UNIVERSITY
SCHOOL OF LAW

PACE INTERNATIONAL
LAW REVIEW
ONLINE COMPANION

Volume 3, Number 9 Winter 2013

THE NEED FOR INTERNATIONAL LAWS OF WAR TO INCLUDE CYBER ATTACKS INVOLVING STATE AND NON-STATE ACTORS

Christopher D. DeLuca*

* Articles Editor, Pace International Law Review, 2012-2013; J.D. Candidate, Pace University School of Law (expected May 2013); B.A., New York University, 2008. I would like to thank and dedicate this work to my family for their willingness to read every draft of this article and their guidance and support over the years.

I. INTRODUCTION

> Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both *states and non-states* and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication.[1]

> One of the most prominent features of the global political system . . . is the significant surge in numbers and importance of non-state entities. . . . The rise of these . . . non-state actors and their growing involvement in world politics challenges the assumptions of traditional approaches to international relations which assume that states are the only important units of the international system.[2]

Within the past fifteen to twenty years, the international community has witnessed the rise of a new style of warfare. Attacks are no longer limited to soldiers firing their weapons at clearly defined targets on the ground, nor are they limited to traditional forms of air and naval operations. Today, through cyberspace, enemies can target government agencies, industries, and domestic infrastructure from thousands of miles away. This new form of warfare turns a state's and non-state's own technology against it in order to bring down vital infrastructure.[3] These "cyber attacks" have the potential to cause mass physical and economic destruction. Their ability to be carried out anonymously, coupled with the low cost and wide availability of computers, are making cyber attacks an attractive method of warfare.[4]

In recent years, there has been a dramatic increase in the

---

[1] U.S. JOINT FORCES COMMAND, THE JOINT OPERATING ENVIRONMENT 36 (2010) (emphasis added).

[2] Gustaaf Geeraets, *Analyzing Non-State Actors in World Politics*, 1 POLE PAPERS, NO. 4 (1996), *available at* http://poli.vub.ac.be/publi/pole-papers/pole0104.htm.

[3] *See* Lesley Swanson, The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, 32 L.A. INT'L & COMP. L. REV. 303, 304 (2010).

[4] *See id.*

number of cyber attacks, both by nations and non-state actors.[5] However, currently, there are no provisions in the international laws of war that explicitly outlaw or even regulate cyber warfare.[6] Furthermore, given the rise of the non-state actor's importance and influence in the international community,[7] it is quite odd/troubling that these international laws of war only apply to state actors.[8]

This article argues that existing international laws of war are inadequate and need to be adjusted and clearly defined to include cyber attacks involving state and non-state actors. Part II of this article describes the different forms and increasing use of cyber attacks in international conflicts. Part III focuses on the importance and relevance of non-state actors in the international community and today's asymmetric battlefield. Part IV discusses the applicability of current international laws of war to cyber attacks. Part V of this article suggests ways in which current international law can be improved to include and regulate cyber attacks involving state and non-state actors.

II. CYBER ATTACKS AND THEIR INCREASING USE IN INTERNATIONAL CONFLICTS

A. What is a Cyber Attack?

Definitions of cyber attacks vary, and the range of hostile activities that constitute cyber attacks are spread across a very wide spectrum.[9] According to the U.S. Army's Cyber Operations and Cyber Terrorism Handbook, a cyber attack is:

> The premeditated use of disruptive activities, or the threat there-

---

[5] Swanson, *supra* note 3.

[6] *Id.* at 305.

[7] *See* Geeraets, *supra* note 2.

[8] *See* U.N. Charter art. 2, para. 4 (only applying the prohibition of the use or threat of force to state actors); Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 2, Aug. 12, 1949. 6 U.S.T. 3114, 75 U.N.T.S. 31 (only applying Geneva Law to "high contracting parties") [hereinafter Geneva Convention for the Wounded and Sick].

[9] 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, 422 (2011).

> of, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives.[10]

More generally, Matthew Waxman defines cyber attacks as "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them."[11] Harm from these attacks can be inflicted either on a computer network, or physical facilities and persons. Cyber attacks range from "malicious hacking and defacement of websites to large-scale destruction of the military or civilian infrastructures that rely on those networks."[12]

Cyber attacks are thus distinguishable from what domestic law enforcement has deemed "cyber crimes." Cyber crimes, like fraud or posting obscene and offensive content on the Internet, are governed by national criminal laws.[13] The intentions of those that commit cyber crimes are also very different from those who initiate cyber attacks.[14]

Cyber attacks are initiated in what is called "cyberspace." Today, the most common definition for cyberspace refers to the internet, and usually consists of some sort of information-sharing environment between computers.[15] In the United States, the National Military Strategy for Cyberspace Operations defines cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated

---

[10] U.S. ARMY TRAINING & DOCTRINE COMMAND, DCSINT HANDBOOK NO. 1.02, CRITICAL INFRASTRUCTURE THREATS AND TERRORISM, at VII-2 (2006).

[11] Waxman, *supra* note 9, at 422.

[12] *Id.*

[13] *See* Natasha Solce, *The Battlefield of Cyber Space: The Inevitable New Military Branch – The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293 (2008).

[14] *See id.* at 301 (explaining that those who commit cyber crimes exhibit personal desires like stealing money whereas a cyber attack's purpose can be to take out a military target).

[15] *See* Michael A. Sinks, Cyber Warfare and International Law 3 (Apr. 2008) (unpublished research paper) (on file with Air University, Air Command and Staff College), *available at* https://www.afresearch.org/skins/RIMS/display.aspx?moduleid=be0e99f3-fc56-4ccb-8dfe-670c0822a153&mode=user&action=researchproject&objectid=1120f215-38a9-4829-bb7a-33de2e42ec12.

physical infrastructure."[16] Furthermore, "joint doctrine has adopted a computer-centric definition where cyberspace is the 'notional environment in which digitized information is communicated over networks.'"[17] In essence, "cyberspace is the sum of electronic networks including, but not limited to, the Internet, where various information operations occur."[18]

B. Types of Cyber Attacks

Cyber attacks can take many shapes and forms. This article will focus on attacks that are used quite frequently in cyberspace: viruses, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, worms, and Trojan horses.

1. Viruses

A virus (quite possibly the "simplest" type of cyber attack according to Jason Barkham) is a code fragment, intentionally written and launched, that attaches itself to a program, and only operates when the host program begins to run.[19] A virus's "most common trait is its ability to (1) attach itself to a host program and execute when the host is operated and (2) replicate itself."[20] The intended goal of the virus is "to impact the data or integrity of the computer without the owner's knowledge."[21] A well-executed and written virus has the potential to inflict serious damage. For example, "the 'I Love You' virus, released in the spring of 2000, caused an estimated $6.7 billion in damage."[22]

2. Denial of Service (DoS)/Distributed Denial of Service (DDoS) Attacks

In a DoS attack, an attacker, hacker, etc. seeks to prevent

---

[16] *Id.*

[17] *Id.*

[18] Swanson, *supra* note 3, at 307.

[19] Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 62-63 (2001).

[20] Sharon R. Stevens, *Internet War Crimes Tribunals and Security in an Interconnected World,* 18 TRANSNAT'L L. & CONTEMP. PROBS. 657, 663 (2009).

[21] *Id.*

[22] Barkham, *supra* note 19, at 62-63.

legitimate users from accessing information or services.[23] An attacker will either target a computer and its network connection, or the computers and networks of sites, in order to prevent the user from accessing email, websites, online accounts, or any other service that relies on the affected computer.[24] "The most common and obvious type of DoS attack occurs when an attacker 'floods' a network with information."[25] For example, an individual may seek to cripple a website or a computer network by sending it an overwhelming amount of data requests.[26] Since the server can only process a certain amount of requests at a time, when an attacker sends an exorbitant amount of data requests, the server will be unable to respond to legitimate data requests, thus disallowing access to the site.[27]

Distributed denial of service (DDoS) attacks, on the other hand, use many computers that "are pre-infected with a virus that hijacks another computer to attack Web sites, making it exponentially more powerful than a standard DoS attack."[28] For instance, an attacker may take control of another computer or system, and then force the infected computer to send large amounts of data to a website. The attack is "distributed" because the attacker is using multiple computers to launch the denial of service attack.[29]

3. Worms

A worm is an independent program that, once infected on one computer, copies itself onto other machines, but usually does not change the makeup of other programs.[30] "Worms can cause damage merely by eating up network resources or by de-

---

[23] Mindi McDowell, *National Cyber Alert System,* US-CERT.GOV (Nov. 4, 2009), http://www.us-cert.gov/cas/tips/ST04-015.html.

[24] *Id.*

[25] *Id.*

[26] Wolfgang McGavran, *Intended Consequences: Regulating Cyber Attacks,* 12 TUL. J. TECH. & INTELL. PROP. 259, 262 (2009).

[27] McDowell, *supra* note 23.

[28] McGavran, *supra* note 26, at 262.

[29] McDowell, *supra* note 23.

[30] Barkham, *supra* note 19, at 63.

stroying data, and are particularly effective over networks."[31] And, unlike a computer virus, the worm does not need to attach itself to an existing program.

The first Internet worm was unleashed upon the Massachusetts Institute of Technology's computer network on November 2, 1988, from a twenty-three year-old Cornell University graduate student's computer terminal in Ithaca, New York.[32] After infecting a single computer, the worm copied itself to other machines, and in the span of one day, infected an estimated five to ten percent of all Internet-connected machines at MIT.[33]

4. Trojan Horses

Derived from the "Trojan Horse" story in Greek mythology, Trojan horses are one of the easiest weapons that hackers can use to "wreak havoc on the internet."[34] A Trojan horse is a destructive tool that operates under the guise of a valuable or otherwise entertaining computer program.[35] They can be viruses or remote control programs that provide complete access to a victim's computer, and can be installed on a host computer in a number of ways, including, for instance, through an email attachment intended to be opened by the victim.[36] As the user enjoys or uses the email attachment, infection occurs simultaneously and silently.[37] In essence, a Trojan horse either replaces a legitimate program, or simulates a legitimate program.[38] When a user runs a Trojan horse, it executes detrimental commands that are unknown to the user.[39] "For example, a Trojan horse hidden in a random program downloaded from the Internet may read any file on a user's system, and then e-mail

---

[31] *Id.*

[32] JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 37 (2008).

[33] *Id.*

[34] John Crapanzano, *Deconstructing SubSeven, the Trojan Horse of Choice*, SANS INSTITUTE (2003), http://www.sans.org/reading_room/whitepapers/malicious/deconstructing-subseven-trojan-horse-choice_953.

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] Kristen M. Koepsel, *Methods and Tools for Cyber Attacks – Trojan Horse*, *in* DATA SEC. & PRIVACY LAW § 1.44 (2011).

[39] *Id.*

it anywhere in the world."[40] Furthermore, "if a remote control Trojan [horse] is installed and initiated on a system, that computer is now completely open to anyone who knows to connect to it using the Trojan horse as a server."[41] A remote control Trojan horse differs from a traditional computer virus in that it does not spread throughout an infected system; it is thus a contained program designed to invisibly execute commands issued by a remote user.[42]

C. Recent Cyber Attacks Used in International Conflicts

Cyber attacks are not a new phenomenon in the international community. In 1996, a congressional report given by the General Accounting Office of the United States projected that the Department of Defense may have experienced as many as 250,000 cyber attacks during that year, and further estimated that the attacks were successful 65% of the time.[43] The report also found that only about one in 150 attacks were actually detected and reported.[44] These cyber attacks have evolved exponentially, from small hacker attacks against government computers to large-scale distributed denial of service attacks that can ultimately disrupt a single nation's infrastructure, bringing it to its knees.

1. Cyber Attacks on the Estonian Infrastructure

On April 27, 2007, a massive series of cyber attacks crippled main components of Estonia's essential electronic infrastructure. The attacks were allegedly initiated when Estonian officials moved a statue commemorating Russians who perished while driving the Nazis out of the country at the end of World War II.[45] In only a few hours, the online portals of Estonia's leading banks were flooded with data requests and crashed. All of the principal newspaper websites stopped work-

---

[40] *Id.*

[41] Crapanzano, *supra* note 34.

[42] *Id.*

[43] U.S. GEN. ACCOUNT. OFFICE, GAO/AIMD-96-84, COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS 2 (1996).

[44] *Id.* at 3.

[45] *Id.*

ing, affecting circulation, and government communications were largely blacked out.[46] Throughout this onslaught, dozens of targets were assaulted across the country.[47] Because of Estonia's wired "e-government," its infrastructure was an enormous target for cyber attackers. In the end, government websites, newspapers, universities, hospitals, banks, and fire and paramedic services were all victims of the attacks orchestrated by allegedly one million computers operated by third parties working together to bring down the Estonian government.[48]

These cyber attacks ultimately lasted for weeks.[49] They caused social unrest and rioting, resulting in property damage, 150 people injured, and one Russian dead.[50] The Estonia incident displayed the full potential of well-executed cyber attacks. It was the first time cyber attacks threatened the security of an entire nation.[51] To this day, it remains unknown whether state or non-state actors were responsible for this offense.[52]

2. The Russian-Georgian Cyber Conflict

When war broke out between Russia and Georgia in August 2008 over the disputed territory of South Ossetia, Russian bombers sought to destroy Georgia's economic infrastructure. Targets included the country's largest port on the Black Sea and an important road connecting southern Georgia with the East.[53] As well, in the two months prior to the physical conflict, Georgia's "Internet Infrastructure" was hit with massive DDoS attacks:

> [M]ajor Georgian website servers were brought down, hindering communication and causing confusion throughout the country. . . . These cyber attacks mainly hindered the Georgian government's ability to communicate with its citizens, as well as other nations, both before and during the physical invasion by Russia.[54]

---

[46] Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKLEY J. INT'L L. 192, 193 (2009).

[47] *Id.*

[48] Stevens, *supra* note 20, at 666.

[49] *Id.*

[50] Shackelford, *supra* note 46, at 193.

[51] *Id.*

[52] *See id.* at 205.

[53] Swanson, *supra* note 3, at 303.

[54] *Id.*

Media, communications, and transportation companies were also attacked, along with the National Bank of Georgia's website.[55] The attacks further spread to computers throughout the government, even after Russian troops entered South Ossetia.[56] What is important to note about this attack is that it was the first time a known cyber attack had coincided with traditional military action.[57]

3. Stuxnet

"Stuxnet is the world's first cyber-weapon of geopolitical significance; it enables a military attack using a computer program tailored to a specific target."[58] First discovered in 2010, Stuxnet was a computer worm that infiltrated Siemens's (a German engineering company) industrial software and equipment, spreading via Microsoft Windows.[59] Initiated via a removable memory stick, Stuxnet was the first worm to exploit a Microsoft Windows vulnerability in order to spread:

> Stuxnet was the first piece of malware to exploit the Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability (BID 41732) in order to spread. The worm drops a copy of itself as well as a link to that copy on a removable drive. When a removable drive is attached to a system and browsed with an application that can display icons, such as Windows Explorer, the link file runs the copy of the worm. Due to a design flaw in Windows, applications that can display icons can also inadvertently run code, and in Stuxnet's case, code in the .lnk file points to a copy of the worm on the same removable drive.[60]

"It then sent detailed production information through the In-

---

[55] John Markoff, *Before the Gunfire, Cyberattacks,* N.Y. TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&th=&adxnnl=1&oref=%20slogin&emc=th&adxnnlx=1218651509sGZ4ZcPX+1J8D844weNClw.

[56] *Id.*

[57] *Id.*

[58] Holger Stark, *Stuxnet Virus Opens New Era of Cyberwar,* SPIEGEL ONLINE INTERNATIONAL (Aug. 08, 2011), http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html.

[59] *Building a Cyber Secure Plant,* SIEMENS TOTALLY INTEGRATED AUTOMATION (Sept. 30, 2010), http://www.totallyintegratedautomation.com/2010/09/building-a-cyber-secure-plant/.

[60] Jarrad Shearer, *W32.Stuxnet,* SYMANTEC.COM (JUL. 13, 2010), http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

ternet to a set of servers in Malaysia."[61] Stuxnet was thus able to provide cyber attackers with the valuable ability to remotely control the infection process, and to hide the existence of their changes to a system.[62] Furthermore, the worm was not designed to instantly cause damage or inconvenience, but to inflict destruction over a substantial period of time.[63] "As long as the worm remained undetected, the attackers could steal information, halt production, compromise safety systems or even cause equipment to be damaged or people injured whenever they choose."[64]

Along with other countries around the world, the worm repeatedly targeted five industrial facilities in Iran over a ten-month period.[65] On November 23, 2010, it was announced that uranium enrichment at the Natanz nuclear facility had ceased on several occasions because of a series of severe technical problems caused by the Stuxnet worm.[66] The worm first infected an Iranian IR-1 centrifuge, causing it to increase its operating speed for about fifteen minutes before returning to its normal frequency.[67] Almost one month later, the worm went back into action, further slowing the infected centrifuges for a total of fifty minutes.[68] The stresses from the shift in speeds caused the aluminum centrifugal tubes to expand, often forcing parts of the centrifuges into sufficient contact with each other, destroying the machine.[69] Even though destruction of the centrifuges was by no means total, Stuxnet displayed to the world the ever-growing destructive capabilities of cyber worms. According to General Michael Hayden, former Director of the CIA, "Stuxnet is the first time where we've seen significant

---

[61] *Building a Cyber Secure Plant*, *supra* note 59.

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] Jonathan Fildes, *Stuxnet Virus Targets and Spread Revealed*, BBC NEWS (Feb. 15, 2011, 8:51 PM), http://www.bbc.co.uk/news/technology-12465688.

[66] Yossi Melman, *Iran Pauses Uranium Enrichment at Natanz Nuclear Plant*, HAARETZ.COM (Nov. 23, 2010), http://www.haaretz.com/news/international/iran-pauses-uranium-enrichment-at-natanz-nuclear-plant-1.326276.

[67] Stark, *supra* note 58.

[68] *Id.*

[69] *Id.*

physical damage created by a cyber attack."[70]

4. Alleged Government Cyber Attacks on WikiLeaks

Hosted on various servers across the globe, the whistle-blowing organization WikiLeaks is no stranger to cyber attacks. The organization's founder, Julian Assange, claims that WikiLeak's servers and computers are attacked in cyberspace on a daily basis.[71] What is particularly interesting about the WikiLeaks cyber attacks is the alleged involvement of government institutions.

In 2010, WikiLeaks distributed, or "leaked," United States diplomatic cables to The New York Times, revealing that China's Politburo directed the cyber intrusion of Google's computer systems in China.[72] This situation came to be known as "CableGate." The Google cyber attack "was part of a coordinated campaign of computer sabotage carried out by government operatives, private security experts and Internet outlaws recruited by the Chinese government."[73] According to Julian Assange, after the cables detailing the Chinese attacks on Google were released, the Chinese government retaliated by launching a series of DDoS attacks on WikiLeak's servers.[74]

Around the same time, armies of "zombie" computers in Europe, Russia, and Asia flooded the WikiLeaks servers, sending massive data requests, forcing WikiLeaks to look for other

---

[70] *60 Minutes: Stuxnet* (CBS television broadcast Mar. 4, 2012) (emphasis added) (transcript *available at* http://www.cbsnews.com/8301-18560_162-57390124/stuxnet-computer-worm-opens-new-era-of-warfare/).

[71] *Julian Assange and How He Sees the World*, SUEDDEUTSCHE ZEITUNG (Sept. 9, 2011), http://www.scribd.com/doc/64417045/Julian-Assange-and-How-He-Sees-the-World.

[72] Scott Shane & Andrew W. Lehren, *Leaked Cables Offer Raw Look at U.S. Diplomacy*, N.Y. TIMES (Nov. 28, 2010), http://www.nytimes.com/2010/11/29/world/29cables.html.

[73] *Id.* This was not the first time China was involved in cyber attacks. "In late August 2011, a state television documentary appeared to capture an in-progress DDoS attack by the Chinese military on a Falun Gong website based in Alabama. Not long after, the McAfee cyber security-company reported that a state actor – widely believed to be China – had been engaged in a year-long cyber attack program aimed at governments, U.S. corporations, and United Nations groups." Oona A. Hathaway et al., *The Law of Cyber-Attack,* 100 CALIF. L. REV. 817, 819 (2012).

[74] *Julian Assange and How He Sees the World*, *supra* note 71.

servers to help fight off the massive attack.[75] Assange's lawyer, Mark Stephens, also claimed that a "state actor" was most likely behind some of these attacks.[76] Even Senators and various officials in Washington called for the United States and hackers to launch a full-scale attack on the whistleblowing organization.[77]

WikiLeaks continues to be hit by massive DDoS attacks, making the site completely inaccessible for various periods.[78] Although the identity of the attackers is unknown, Assange remains steadfast in his assumption that that these attacks are backed by many foreign governments, including the United States.[79] Assange has gone so far as to classify governmental cyber attacks on WikiLeaks as "war crimes," by declaring "[a]ttacks on websites by governmental institutions however are a war crime, same as assaults on every other civilian infrastructure."[80]

III. NON-STATE ACTORS IN THE INTERNATIONAL COMMUNITY

A. The Importance of Non-State Actors

In the past, principal actors in world politics and international relations were nation-states.[81] However, in the years fol-

---

[75] Ashlee Vance, *WikiLeaks Struggles to Stay Online After Attacks*, N.Y. TIMES (Dec. 03, 2010), http://www.nytimes.com/2010/12/04/world/europe/04domain.html.

[76] Agence France-Presse, *Assange Lawyer Blames 'State Actor' for Cyber Attacks,* THE RAW STORY (Dec. 03, 2010, 7:16 PM), http://www.rawstory.com/rs/2010/12/03/assange-lawyer-blames-state-actor-cyberattacks/.

[77] Declan McCullagh, *Has WikiLeaks Landed in Cyberattack Crosshairs?,* CNET (Oct. 27, 2010, 4:00 AM), http://news.cnet.com/8301-13578_3-20020835-38.html.

[78] *WikiLeaks Site Comes Under Cyber Attack,* THE GUARDIAN (Aug. 30, 2011, 10:18 PM), http://www.guardian.co.uk/world/2011/aug/31/wikileaks-site-cyberattack-cable-release.

[79] *See* McCullagh, *supra* note 77; *WikiLeaks Says Website Was Target of Cyber Attack*, REUTERS (Aug. 31, 2011), http://www.reuters.com/article/2011/08/31/us-wikileaks-cyberattack-idUSTRE77U17920110831.

[80] *Julian Assange and How He Sees the World*, *supra* note 71.

[81] Muhittin Ataman, *The Impact of Non-State Actors on World Politics: A Challenge to Nation-States,* 2 ALTERNATIVES: TURKISH J. OF INT'L RELATIONS (2003), *available at* http://www.alternativesjournal.net/volume2/number1/

lowing World War II, there has been a proliferation of non-state actors ("i.e. organizations lacking formal or legal status as a state or as an agent of a state") in the international community that have become principal actors in world politics and international relations.[82] The growth of non-state actors challenges and weakens the "state-centric" concept of international politics and replaces it with a "transnational" system, where relationships and interactions are significantly more complex.[83] This phenomenon has led scholars of international relations to conclude that states are declining in importance, while non-state actors are gaining great influence.[84]

Today, non-state actors play an important role in foreign policy making and can pit one state against another.[85] For example, terrorist organizations shape entire nations' security policies. Non-governmental organizations, like WikiLeaks and spinoffs, open the eyes of the public to injustices, and can not only destroy reputations, but can drastically shape policy and international relations. Moreover, these non-state actors are beginning to notice that cyber attacks can be a useful tool in accomplishing their respective goals.

B. Cyber Attacks and Non-State Actors

It can be argued that non-state actors are involved in cyber attacks almost daily. As previously mentioned, these attacks can include alleged governmental attacks on non-state organizations, and can range from the everyday hacker targeting governmental websites, to sophisticated "cyber terrorists" launching massive DDoS attacks on private companies like Google. Terrorist organizations have also been identified as having the capability to launch *destructive* cyber attacks.

Recently, Al Qaeda has been building its cyber skills to attack Western nations.[86] In 2006, it was reported that Al Qaeda may have called for cyber attacks against U.S. financial insti-

---

ataman2.htm.

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] Solce, *supra* note 13, at 299.

tutions during December of that year.[87] In April 2010, court records from the case of terrorism suspect, Mohamedou Ould Slahi, revealed that the organization initiated *successful* cyber attacks, including one against government computers in Israel in 2001.[88] "This was the first public confirmation that the terrorist group has mounted an offensive cyber attack."[89] Slahi informed interrogators that Al Qaeda "used the Internet to launch . . . computer attacks," and that the organization "also sabotaged other websites by launching denial of service attacks, such as one targeting the Israeli prime minister's computer server."[90]

Other international terrorist groups like the Armed Islamic Group, Aum Shinrikyo, Hezbollah, and Hamas have been heightening their computer expertise as well.[91] "Furthermore, four domestic [U.S.] terrorist organizations – Hammerskin Nation, Stormfront, Aryan Nation, and National Alliance – are recognized as potentially having the technology to engage in cyber terrorism."[92] British authorities are also bracing for an increase in cyber attacks as a result of Al Qaeda calling for a cyber jihad following the death of Osama bin Laden.[93]

> There will be more cyber terrorism. Groups will continue to benefit from the off-the-shelf technology in planning and conducting attacks, making operations more secure and potentially more lethal. The Internet and virtual space will be strategically vital.[94]

However, even though non-state actors are extremely important in international relations and have the capability to launch destructive cyber attacks, attacks involving these par-

---

[87] *Id.*

[88] Alex Kingsbury, *Documents Reveal Al Qaeda Cyberattacks,* U.S. NEWS (Apr. 14, 2010), http://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks.

[89] *Id.*

[90] *Id.*

[91] Solce, *supra* note 13, at 299.

[92] *Id.*

[93] Gerry Smith, *UK Authorities Brace for 'Cyber Jihad' By Al Qeada after Bin Laden Death*, THE HUFFINGTON POST (Jul. 12, 2011, 1:17 PM), http://www.huffingtonpost.com/2011/07/12/al-qaeda-cyber-jihad_n_895579.html.

[94] SECRETARY OF STATE FOR THE HOME DEP'T, CONTEST: THE UNITED KINGDOM'S STRATEGY FOR COUNTERING TERRORISM, 2011, Cm 8123, at 41 (U.K.).

ties are not governed by current international laws.

> By definition, terrorists who engage in the interstate use of force do not observe the laws of war. Therefore, they are not entitled to an elevated status that would grant them protections under *jus in bello*. As such, members of terror groups are entitled to fewer rights than protected persons and lawful combatants.[95]

These existing rules have little to say, if anything at all, about non-state actors that will most likely be at the center of these future cyber conflicts.[96]

IV. CURRENT INTERNATIONAL LAWS OF WAR AND CYBER ATTACKS

The laws of war are split into two principle divisions: *jus ad bellum* and *jus in bello. Jus ad bellum,* or the "law to war," "governs the legality of resorting to armed force,"[97] whereas *jus in bello* means the "law in war."[98] For purposes of *jus ad bellum,* when analyzing whether an international conflict, cyber or otherwise, is governed by the international laws of war, it must be determined whether the attack violates the United Nations Charter.[99] In other words, does the attack constitute a level of force that is prohibited by Article 2(4) of the U.N. Charter?[100] Or, does the attack rise to the level of an armed attack justifying self-defense under Article 51 of the U.N. Charter?[101] If the attack satisfies the principles of *jus ad bellum,* and can be viewed as an armed attack under the U.N. Charter, then we must look to laws governing the conduct of war. Such laws are known as *jus in bello* laws, which are comprised of both Geneva and Hague law.[102]

---

[95] Norman G. Printer, Jr., *The Use of Force Against Non-State Actors Under International Law: An Analysis of the U.S. Predator Strike in Yemen*, 8 UCLA J. INT'L L. & FOREIGN AFF. 331, 334 (2003).

[96] *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1093 (2007).

[97] Swanson, *supra* note 3, at 312

[98] *Id.*

[99] *See* U.N. Charter art. 2, para. 4; art. 51.

[100] *See* Oona A. Hathaway et al., *The Law of Cyber-Attack,* 100 CALIF. L. REV. 817, 841 (2012).

[101] *Id.* at 845.

[102] U.K. MINISTRY OF DEFENSE, THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT 3 (2004) [hereinafter JOINT SERVICE MANUAL OF THE LAW OF

A. Jus ad Bellum

Legal regulation of the use of force in the international community begins with Article 2(4) of the U.N. Charter.[103] The provision states that "[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[104] However, the meaning of the "use of force" has been debated ever since the Charter went into effect.[105]

Many view "use of force" to be interpreted in three possible ways: force as armed violence, force as coercion, and force as interference.[106] Advocates of the "force as armed violence view" argue that "use of force" strictly applies to military attacks or armed violence.[107] This view mainly analyzes the instrument used to inflict force, rather than its general effect.[108] Under the "force as coercion" interpretation, force is viewed in a more expansive way.[109] Proponents of this interpretation view force as including forms of pressure other than just armed force, i.e. political and economic coercion threatening state autonomy.[110] The third approach, or "force as interference" approach, "ties the concept of force to improper interference with the rights of other states, focusing on the object and specific character of a state's actions rather than a narrow set of means or their coercive effect."[111] Weaker nation states and some scholars defend the "force as coercion" and "force as interference" views.[112] However, the general consensus, and the dominant view in the international community, is that Article 2(4) prohibits only physical armed force.[113]

ARMED CONFLICT].

[103] Waxman, *supra* note 9, at 426.

[104] U.N. Charter art. 2, para. 4.

[105] Waxman, *supra* note 9, at 427-29.

[106] *Id.* at 427-30.

[107] *Id.* at 427-28.

[108] *Id.* at 428.

[109] *Id.*

[110] *Id.* at 428-29.

[111] *Id.* at 429.

[112] *See id.* at 429-30.

[113] Hathaway, *supra* note 100, at 842.

One exception to the blanket rule of Article 2(4) prohibiting the threat or use of armed force is articulated in Article 51 of the U.N. Charter. Article 51 stands for the proposition that nations can use force as a means of self-defense: "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[114] Lawful self-defense is very difficult to define.[115] However, the critical question in determining the lawfulness of self-defense is whether or not an "armed attack" has actually occurred.[116]

It is also widely understood that the definition of "armed attack" is much narrower than the definition of "force" under the U.N. Charter.[117] For example, there may be acts that violate Article 2(4)'s prohibition on the use or threat of force, but do not constitute an "armed attack." In *Nicaragua v. The United States,* the International Criminal Court (ICJ) found that

> [A]n armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by . . . a State of armed bands . . . which carry out acts of armed force against another State. . . ." The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State to the territory of another State, if such an operation, *because of its scale and effects*, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.[118]

According to the ICJ, armed attacks are those that constitute the "most grave forms of the use of force."[119]

---

[114] U.N. Charter art. 51.

[115] Hathaway, *supra* note 100, at 844.

[116] *Id.*

[117] *Id.*

[118] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 103 (June 27) (emphasis added) (quoting Article 3, paragraph (g), of the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX)).

[119] *Id.* at 101.

1. Application of Jus ad Bellum to Cyber Attacks

In order for the U.N. Charter to apply to cyber attacks, the attacker must be a nation-state.[120] If a situation existed where a non-state actor (i.e. a terrorist organization) launched a cyber attack against a state actor (and vice-versa), the Charter would not apply. Since there are no specific provisions in the U.N. Charter addressing cyber attacks, scholars have looked to many approaches in interpreting the Charter in order to pinpoint when a cyber attack constitutes a use or threat of force, or when they rise to the level of an armed attack.

Duncan Hollis utilizes three approaches in order to determine when a cyber attack constitutes a use or threat of force under Article 2(4).[121] However, according to Hollis, there are major problems with each approach used in a modern context.[122] The first approach is the traditionalist "instrumentality" approach, which argues that a cyber attack cannot constitute an "armed attack" under Article 2(4) because it lacks the physical characteristics traditionally associated with a military attack.[123] According to Hollis, the text of the U.N. Charter offers some support for this view in Article 41, which "lists 'measures not involving the use of armed force' to include 'complete or partial interruption of . . . telegraphic, radio, and other means of communication."[124] Since the object of most cyber attacks is to interrupt or disrupt some means of communication (i.e. a massive DDoS attack aimed at a website in order to stop it from displaying information), "more or different forms of aggression must be shown in order [for the cyber attack] to constitute an 'armed attack' under the U.N. charter."[125]

The second approach, the "target-based" approach,[126] suggests that cyber attacks constitute a use of force or an armed attack whenever the attack "penetrates 'critical national infrastructure' systems, even absent significant destruction or casu-

---

[120] *See* U.N. Charter art. 2, para. 4; art. 51.
[121] Hollis, *supra* note 96, at 1041.
[122] *Id.* at 1041-42.
[123] *Id.* at 1041.
[124] *Id.*
[125] Stevens, *supra* note 20, at 675.
[126] Hollis, *supra* note 96, at 1041.

alties."[127] Hollis argues that this approach tends to be too over-inclusive, since cyber attacks can produce wide-ranging effects, from merely informational (distributing propaganda), to inconvenient (disrupting systems temporarily via a denial-of-service attack), to potentially dangerous (implanting a logic bomb doing no immediate harm, but with the potential to cause future injury), to immediately destructive (disabling a system permanently via a virus).[128]

The third and final approach, the "consequentiality" approach, focuses on the consequences of the cyber attack.[129] Whenever the cyber attack intends to cause effects normally produced by kinetic force (death and destruction of property), the attack constitutes a use of force, and an armed attack.[130] Sharon Stevens argues that the real problem with the "consequentiality" approach is that it does not account for the damage a cyber attack can inflict even with a lack of physical effects:

> A cyber attack that shuts down any part of a nation's critical infrastructure may have an effect that is much more debilitating than a traditional military attack. The threat in such a situation may be more terrorizing and harmful than a traditional armed attack. Certainly, a country that is unable to use its banking system, or whose power grid has gone off-line due to a cyber attack, possesses legitimate claims for reparation, justice, and security. Because the consequentiality approach focuses on the same type of physical damage caused by a kinetic attack, it does not sufficiently protect critical infrastructure.[131]

But, given these possible approaches, is it possible that the current law of *jus ad bellum* could apply to the recent cyber attacks mentioned in Part II of this article?

3. Current Jus ad Bellum Laws are Inadequate in Regulating Recent Cyber Attacks

Since cyber attacks lack the physical characteristics of a traditional military attack, the "instrumentality" approach would not

---

[127] *Id.*
[128] *Id.* at 1042.
[129] *Id.* at 1041.
[130] *Id.*
[131] Stevens, *supra* note 20, at 676.

apply to the cyber attacks on Estonia's infrastructure, the Russia-Georgian conflict, the Stuxnet worm, the alleged governmental attacks on WikiLeaks, the Chinese cyber attacks, and cyber attacks involving terrorists. As a result, these attacks would not constitute force or an armed attack under the U.N. Charter.

With regards to the "target-based" approach, it may be possible that current *jus ad bellum* laws apply to the Estonian cyber attacks, but not the Russian-Georgian conflict, or the Stuxnet worm. As previously stated, Estonia's infrastructure was under a massive DDoS attack in 2007. Fire services, hospitals, newspapers, and banks were all victims of the attack. It can be argued that Estonia's critical infrastructure was attacked, and under the "target-based" approach, this attack could be seen as a use or threat of force, or an armed attack. However, since the attack caused mere confusion and unrest rather than any direct deaths or destruction of property, is it reasonable that these cyber attacks be labeled as a use of force or an armed attack under the U.N. Charter? The current laws of force and armed attack do not specify or answer this question.

In applying the "target-based" approach to the Russia-Georgian cyber attack and the Stuxnet worm, one needs to examine what constitutes "critical national infrastructure," since it is unclear whether government websites actually constitute "critical national infrastructure." One could argue that government websites that affect a nation's ability to communicate are part of its "critical national infrastructure." However, the current law does not incorporate this definition. Also, what about cyber attacks against nuclear facilities, as in the case of the Stuxnet worm? Do these facilities constitute "critical national infrastructure" under Hollis's "target-based" approach? Again, one can only speculate.

In all of the cyber attacks mentioned, with the exception of the Estonian situation, there were no civilian casualties. Nonetheless, in all of these cases, it can be argued that there was a destruction of property. In the case of the Stuxnet worm, parts of nuclear centrifuges in Iran were destroyed. Regarding Estonia, Russia, and the WikiLeaks DDoS attacks, it can be inferred that massive amounts of data were likely destroyed as a result of the cyber attacks. However, it is unlikely that this

type of property destruction would amount to a use of force or an armed attack under a formalist analysis of the U.N. Charter, given the fact that the Charter was written decades ago. As a result, it is unlikely that the "consequences" approach would apply to any of the cyber cases cited.

Lastly, since cyber attacks involving WikiLeaks and terrorists involve non-state actors, current *jus ad bellum* laws would not apply in these situations, no matter what approach is used or how much damage is inflicted. However, "in today's world, non-state actors may inflict damages tantamount to a state-sponsored military attack. Non-state aggressors may also gain sophisticated technological skills that parallel the type of attack that Estonia faced in 2007."[132]

It is clear to see that the current *jus ad bellum* laws accomplish little in categorizing recent cyber attacks as a use or threat of force or an armed attack. However, the cases mentioned demonstrate major flaws in current *jus ad bellum* laws, and demonstrate that current laws must adapt to this new style of combat.

B. Jus in Bello (International Humanitarian Law)

As previously stated, *jus in bello* or "law in war," also known as International Humanitarian Law (IHL) or the Law of Armed Conflict (LOAC), is a set of rules that seek to limit the effects of armed conflicts.[133] IHL also "protects persons who are not or are no longer participating in the hostilities and *restricts the means and methods of warfare*."[134]

IHL is comprised of both Geneva and Hague law.[135] Geneva law refers to the laws created in the Geneva Conventions.[136] A major part of IHL is contained in the four Geneva Conventions of 1949,[137] which nearly every nation-State in the world

---

[132] Stevens, *supra* note 20, at 676.

[133] *What is International Humanitarian Law?*, INT'L COMMITTEE OF THE RED CROSS, (July 2004), http://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf.

[134] *Id.* (emphasis added).

[135] Swanson, *supra* note 3, at 312.

[136] *Id.*

[137] *Id.*

has agreed to be bound by.[138] The Conventions have been further developed and supplemented by two agreements know as the Additional Protocols I and II of 1977, which relate to the protection of victims of armed conflicts.[139] "These treaties are particularly concerned with the protection of the victims of armed conflict, with Additional Protocol I focusing on the means and methods of warfare."[140] Conversely, Hague law refers to the 1899 and 1907 Hague Conventions, and is mainly concerned with the methods and means of warfare, tactics and the general conduct of hostilities.[141]

In order for IHL to govern a cyber attack, the attack must constitute an "armed conflict."[142] According to the International Committee of the Red Cross (ICRC), there are only two types of armed conflicts under IHL: "[i]nternational armed conflicts, opposing two or more States, and non-international armed conflicts between governmental forces and non-governmental armed groups, or between such groups only."[143] Regarding international armed conflicts (IAC), Common Article 2 of the Geneva Conventions provides that:

> In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation

---

[138] *Id.*

[139] *See id.*; Protocol Additional to the Geneva Conventions of 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II].

[140] Swanson, *supra* note 3, at 312; *see* Additional Protocol II, *supra* note 139, art. 1.

[141] Swanson, *supra* note 3, at 313; *see* Convention With Respect to the Laws and Customs of War on Land (Hague II), July 29, 1899, 32 Stat. 1803; Convention With Respect to the Laws and Customs of War on Land (Hague II), Oct. 18, 1907**,** 36 Stat. 2277.

[142] JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT, *supra* note 102.

[143] *Id.*

> meets with no armed resistance.[144]

Additional Protocol I also relies on this same "armed conflict" language. Article 1(3) of Additional Protocol I states "this Protocol, which supplements the Geneva Conventions of 12 August 1949 for the protection of war victims, shall apply in the situations referred to in Article 2 common to those Conventions."[145] In the words of the Conventions, "High Contracting Parties" are nation-States.[146] The Commentary of the Geneva Conventions of 1949 also states:

> Any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place.[147]

The International Criminal Tribunal for the Former Yugoslavia (ICTY) in *The Prosecutor v. Dusko Tadic* further defined an IAC by holding that "an armed conflict exists whenever there is a resort to armed force between States."[148]

In defining non-international armed conflicts, it is appropriate to consult Common Article 3 to the Geneva Conventions and Article 1 of the Additional Protocol II.[149] Additionally, the ICTY determined the existence of a non-international armed conflict "whenever there is . . . protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[150] The court further confirmed that NIAC's exist in situations where "several factors [confront] each other without involvement of the government's armed forces."[151] Since the ruling in *Tadic*, each judgment of the ICTY has taken this definition as a starting

---

144 Geneva Convention for the Wounded and Sick, *supra* note 8, art. 2.

145 Additional Protocol I, *supra* note 139, art. 1, para. 3.

146 *How is the Term 'Armed Conflict Defined in International Humanitarian Law?* INT'L COMMITTEE OF THE RED CROSS, 1 (Mar. 2008), http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf [hereinafter ICRC Opinion Paper].

147 Geneva Convention for the Wounded and Sick, *supra* note 8, art. 2.

148 Prosecutor v. Tadic, Case No. IT-94-1-A, Opinion and Judgment, ¶ 561 (May 7, 1997).

149 ICRC Opinion Paper, *supra* note 146, at 3.

150 Tadic, IT-94-1-A , ¶ 561.

151 ICRC Opinion Paper, *supra* note 146, at 4.

point.[152]

1. Application of Current IHL to Cyber Attacks

Assuming a cyber attack does meet the definition of force and armed attack under the U.N. Charter, the next step in the analysis would be to determine if the attack is governed by current *jus in bello* principles or International Humanitarian Law (IHL). As previously stated, in order for IHL to govern a cyber attack, an armed conflict must exist. Some have argued that IHL cannot govern cyber attacks because there is nothing physical or kinetic about these operations.[153] Under this theory, a cyber attack is not an armed conflict because it does not embody traditional aspects of military attacks; therefore, cyber attacks are beyond the scope of current IHL.

However, commentaries to the Geneva Conventions and the Additional Protocols have implied that "armed conflict" can be viewed in an expansive way.[154] "[S]ome degree of intensity and duration must be considered, as underlying principles of IHL make clear."[155] IHL contained in Hague Law and the Geneva Conventions is based on the idea that victims of an armed conflict are entitled to protection.[156] This protection is usually framed in terms of injury, death, or property damage or destruction.[157] "Therefore, fundamental principles of IHL provide that armed conflict occurs when a group takes measures that injure, kill, damage, or destroy."[158]

As a result, a cyber attack could constitute an armed conflict, as long as certain consequences result from the attack. Moreover, the language of Additional Protocol I indicates that the drafters anticipated change, and that Geneva law would

---

[152] *Id.*

[153] Swanson, *supra* note 3, at 314*; see* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, 84 INT'L REV. OF THE RED CROSS 365, 368-69 (2003) (describing the arguments against the applicability of IHL to computer network attacks).

[154] U.K. MINISTRY OF DEFENCE, THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT 3 (2004).

[155] Swanson, *supra* note 3, at 314.

[156] *Id.*

[157] *Id.* (quoting Schmitt, *supra* note 153, at 366).

[158] *Id.*

have to apply to new methods of warfare.[159] Article 36 of Additional Protocol I requires that:

> In the study, development, acquisition, or adoption of a new weapon, means or methods of warfare, a High Contracting Party is under an obligation 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 to the High Contracting Party.[160]

IHL can also be viewed as anticipating technological change.[161] The "Martens Clause" in the Preamble to the Hague Convention IV of 1907 provides:

> [E]ven in cases not explicitly covered by specific agreements, civilians and combatants remain under the protection and authority of principles of international law derived from established custom, principles of humanity, and from the dictates of public conscience."[162]

In other words, attacks should essentially be judged largely by their effects, rather than by how they are employed.[163]

When applying IHL to cyber attacks, the attack must follow some guidelines. For instance, the attack must not produce "unnecessary suffering."[164] Article 35 of Additional Protocol I thus serves to place some limits on the range of means and weapons that are available in today's modern society. The attack must also follow the principle of proportionality as stated in Additional Protocol I, which requires that the losses resulting from the attack should not be excessive in relation to the expected military advantage.[165] "These principles are important to cyber [attacks] because they require that the attacker refrain from attacks that may be expected to cause excessive collateral damage."[166]

---

[159] Knut Dormann, *Applicability of the Additional Protocols to Computer Network Attacks,* INT'L COMMITTEE OF THE RED CROSS (Nov. 19, 2004), http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.

[160] Additional Protocol I, *supra* note 139, art. 36.

[161] Swanson, *supra* note 3, at 315.

[162] *Id.* (quoting LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 11 (1998)).

[163] *Id.*

[164] Additional Protocol I, *supra* note 139, art. 35.

[165] *Id.*, art. 51, para. 5(b)

[166] Swanson, *supra* note 3, at 316.

Where armed conflict exists, IHL governs once kinetic weapons are used in combination with cyber attacks.[167] However, the law is unclear when cyber attacks are the first or only hostile attacks in the conflict. Yet, it is agreed that in this situation, the key to assessing the attack is in analyzing the effects or consequences of the attack.[168] "Based on this framework, IHL applies whenever cyber attacks, attributed to a state are more than simply sporadic in nature and are intended to, and actually do, cause injury, death, damage, or destruction or such consequences are foreseeable."[169] Therefore, IHL most likely would not apply to cyber attacks where the actual, foreseeable, or intended consequences do not include injury, death, damage, or destruction.[170] However, a lone cyber attack might fall under current IHL if these consequences would result.[171]

2. Current IHL is Inadequate in Regulating Recent Cyber Attacks

In applying current IHL to recent cyber attacks - i.e. the attacks on Estonia's infrastructure, the Russian-Georgian conflict, the Stuxnet worm, the alleged governmental attacks on WikiLeaks, and Chinese cyber attacks - one may conclude that these conflicts did not result in the kinds of consequences necessary to rise to the level of an armed conflict under current IHL. During the cyber conflict between Russia and Georgia, major servers were brought down, resulting in confusion throughout the country and hindering certain communications. In Estonia, the nation's infrastructure was hit, affecting many key societal components. The same could be said for the WikiLeaks attacks and the Stuxnet worm. An argument could be made that damage or destruction was done to property in these situations, even if death or injury were not present. Yet, since it appears that the main results of these cyber attacks were confusion, inconvenience, and possible data destruction, IHL would not govern these situations.

Nevertheless, while the cyber attacks resulting in the types of consequences discussed above were implemented by

---

[167] Dormann, *supra* note 159.
[168] Swanson, *supra* note 3, at 316.
[169] *Id.* at 317.
[170] *Id.*
[171] *Id.*

non-state actors, which are not covered by current IHL, they do pose serious problems, and can be potentially harmful in many indirect ways. Consider the outcomes if the governmental attacks on WikiLeaks or the Chinese cyber attacks caused massive data destruction or massive property destruction to computers or servers; or if Al Qaeda launched a massive cyber attack against the United States military or the United States infrastructure, causing a major dam to be destroyed, resulting in widespread flooding. Or, suppose a third party was behind the Stuxnet worm, or the Estonia or Russian-Georgian conflict. Assuming these cyber attacks did produce the necessary consequences to make IHL applicable, IHL still would not apply because it only applies to states or "High Contracting Parties." Though, as non-state actors have the potential to cause massive destruction via a cyber attack, the laws must address them.

V. IMPROVING CURRENT INTERNATIONAL LAW

A. International Laws vs. Domestic Criminal Laws

Before discussing ways in which to expand or amend current international laws to include cyber attacks between state and non-state actors, it must be determined whether international laws are in fact the most effective tool in regulating cyber attacks between state and non-state actors. Perhaps separate domestic laws might better serve this purpose? Although some may believe domestic laws are the best means to address the cyber attack issue, given the nature of cyber attacks, the confusion and lack of clarity created by conflicting domestic laws and policies, and the global trend of nations coming together to form multilateral agreements regarding similar areas of cyberspace, utilizing international laws seems to be the best solution.

Cyber attacks are global in nature.[172] Changes in domestic law and policy criminalizing cyber attacks, while valuable legal responses, cannot adequately and effectively curb an action that is truly an international concept.[173] Cyber attacks occur in

[172] Hathaway, *supra* note 100, at 880.
[173] *Id.*

cyberspace, and "cyberspace is a network of networks that includes thousands of Internet service providers across the globe: no single state or organization can maintain effective cyber defenses on its own."[174] "An effective solution to this global challenge cannot be achieved by individual states acting alone. It will require global cooperation."[175]

International laws further establish uniformity and clarity where numerous domestic laws may not. Many countries, including the United States and China, have recognized the serious threat posed by cyber attacks.[176] In 2011, the Department of Defense established "five strategic initiatives" to cyber security.[177] The Pentagon further stated that a cyber attack by a foreign state could be considered a traditional act of war, in that "any computer attack that threatens widespread civilian casualties – for example, by cutting off power supplies or bringing down hospitals and emergency-responder networks – could be treated as an act of aggression."[178] However, the Pentagon's policy fails to mention how the United States might respond to a cyber attack from a non-state actor,[179] "nor does it establish a threshold for what level of cyber attack merits a military response."[180]

China, on the other hand, seems to take a more expansive approach to cyber attacks. The Shanghai Cooperation Organization, a security cooperation group headed by China and Rus-

---

[174] *Id.*

[175] *Id.* at 822.

[176] *See id.*

[177] DEP'T. OF DEFENSE, STRATEGY FOR OPERATING IN CYBERSPACE (2011) [hereinafter STRATEGY FOR OPERATING IN CYBERSPACE], *available at* http://www.defense.gov/news/d20110714cyber.pdf (describing the initiatives: 1. Treat cyberspace as an operational domain to organize, train, and equip, so that DoD can take full advantage of cyberspace's potential; 2. Employ new defense operating concepts to protect DoD network and systems; 3. Partner with other U.S. government departments and agencies in the private sector to enable a whole-of-government cybersecurity strategy; 4. Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity; 5. Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation).

[178] David E. Sanger & Elisabeth Bumiller, *Pentagon to Consider Cyberattacks Acts of War*, N.Y. TIMES (June 1, 2011), http://www.nytimes.com /2011/06/01/us/politics/01cyber.html.

[179] *Id.*

[180] *Id.*

sia, adopted more of a means-based approach to cyber attacks.[181] The agreement between the parties cites and defines an "information war" (basically a "cyber war") as "mass psychologic [sic] brainwashing to destabilize society and state, as to force the state to take decisions in the interest of an opposing party."[182] The agreement further states that the "dissemination of information harmful to the spiritual, moral, and cultural spheres of other states" should be viewed as a "security threat."[183]

These policies initiated by the United States and China obviously lack clarity and uniformity. An attack initiated against China may not be considered a cyber attack under United States policies, but may be deemed one under Chinese cyber attack principles. A singular cyber attack definition under international law, such as the U.N. Charter, can accomplish uniformity as well as clarity, and therefore makes international law the more effective tool for regulating cyber attacks.

In recent years, there has been somewhat of a trend towards countries signing multilateral agreements in order to establish uniform laws regarding cyberspace and cyber crimes. One such agreement, besides the Shanghai Cooperation Organization, is the Convention on Cybercrime. The Convention was adopted in 2001 by the Council of Europe.[184] Since its adoption, forty-three countries have signed the treaty, but only sixteen have ratified it.[185] The Convention's main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.[186] In other words, the basic purpose of the Convention was to create a vehicle that

---

[181] Hathaway, *supra* note 100, at 865.

[182] Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, Annex I, at 209 (Dec. 2, 2008) [hereinafter Shanghai Cooperation Agreement].

[183] *Id.* at 203.

[184] Stevens, *supra* note 20, at 685.

[185] *Id.*

[186] Council of Europe, Convention on Cybercrime, pmbl, Nov. 23, 2001, C.E.T.S. No. 185 [hereinafter Cybercrime Convention], *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

would facilitate the creation of uniform domestic laws relating to Internet crime.[187]

> The interest in harmonizing cyber laws stemmed from the chaotic and impossible dilemma presented to anyone intending to do international business via the Internet. The web of varied and conflicting criminal sanctions was overwhelming and burdensome. Not only was it difficult to understand what law applied to a given situation, but even if one could manage that feat, in order to act lawfully, that actor would have to sink to the lowest common denominator, i.e., to follow the most restrictive law in the world. This situation was unfair and too restrictive on the Internet itself.[188]

In creating the Convention, the drafters understood that the only way to effectively regulate cyberspace is through a multilateral set of uniform laws.[189] The drafters recognized it was simply too difficult to accomplish this goal any other way.[190]

B. Amendments and Expansion Suggestions

1. Inclusion of Non-State Actors

First, and arguably most importantly, international laws like the U.N. Charter and the Geneva Conventions must be amended to include conflicts involving non-state actors. Although non-state actors are not traditionally subject to *jus ad bellum* and *jus in bello* principles, the current international legal construct needs to evolve in order to include these principle actors.[191] In regards to the U.N. Charter, Norman Printer describes two reasons why non-state actors should not escape the Charter's provisions:

> First, an entity that elects to use force on the international plane should be treated as an international actor and should be bound by accepted international norms . . . . Second, it would be inconsistent with the purpose of the Charter to allow terrorist groups that engage in transnational armed conflict against a state to fall

---

[187] Stevens, *supra* note 20, at 686.
[188] *Id.*
[189] *See generally* Cybercrime Convention, *supra* note 186.
[190] *Id.*
[191] Printer, *supra* note 95, at 334.

outside the Charter.[192]

In order for non-state actors to be covered under these laws, they would need to be granted some sort of international legal status.[193] Printer suggests that although non-state actors do not typically enjoy international legal status, actors like non-governmental organizations (NGOs) have increasingly become recognized as subjects of international law "with some incidents of international legal status."[194] Printer further argues, "a terrorist network that operates on a global basis, insofar as it is an association of persons with a common purpose not affiliated with a state, arguably attributes similar to an NGO."[195] Yet, Printer suggests that terrorist groups should not enjoy the same legitimacy as an NGO.[196] Instead, terrorist groups should receive a limited form of international legal status, focusing on the rights of states in the international community to hold such organizations accountable for violations of international laws of force.[197]

In addition, if the principles of *jus ad bellum* outlined in the U.N. Charter were applied to non-state actors, the purpose of the Charter to maintain international peace and security would be furthered.[198] Conversely, the Charter's principles would be ill-served if the activities of rogue groups fell outside the principles of *jus ad bellum*, since non-state actors such as terrorist organizations have the capacity to greatly threaten international peace and security.[199]

A similar argument can be made that *jus in bello* principles, outlined in the Geneva Conventions, should apply to non-state actors. Since the purpose of the Conventions and its Additional Protocols is to limit the effects of armed conflicts and conduct of actors within these armed conflicts, the principles of *jus in bello* would be ill-served if non-state actors were not included, as their conduct would not be limited in any way. Fur-

---

[192] *Id.* at 345.
[193] *Id.* at 348.
[194] *Id.* at 347.
[195] *Id.*
[196] *Id.* at 348.
[197] *Id.*
[198] *Id.*
[199] *Id.*

thermore, conduct of state actors involved in conflicts with non-state actors would be murky and unclear.

2. A Clear Cyber Attack Definition

As previously stated, currently a cyber attack can be defined in many ways. Accordingly, a specific, codified definition is needed. A singular definition would provide clarity on whether a state or non-state actor is initiating an armed conflict and whether retaliation in self-defense is warranted.[200] Specific codification of international criminal provisions for cyber attacks also creates greater deterrence because actors know what is specifically forbidden.[201] The legitimacy gained by cyber attack codification increases cyber attack law's deterrence value since actors are more likely to follow rules and regulations that carry the authority of legitimacy.[202] As a result, the U.N. Charter should be amended to include a clear and comprehensive definition of cyber attacks.

Davis Brown proposed a singular definition of a cyber attack – calling it an information attack - in his "Draft Convention Regulating the Use of Information Systems in Armed Conflict":

> The term "information attack" means the use of computer and/or other information or communications systems to destroy, alter, or manipulate data or images, engage in denial of service attacks, transmit malicious code, or perpetrate similar attacks, or do physical damage to any target for the purpose of inflicting injury or degrading the enemy's ability or will to fight.[203]

Brown's definition is a good starting point. However, the proposed amendment should define the various types of cyber attacks, while at the same time should be broad enough to incorporate the idea that new methods of cyber attacks are likely to be discovered.

---

[200] Hathaway, *supra* note 100, at 881-82.

[201] Stevens, *supra* note 20, at 704.

[202] *Id.* 704-05.

[203] Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 215 (2006).

3. Cyber Attacks as a Use of Force

Since the general consensus in the international community is that Article 2(4) of the U.N. Charter prohibits only physical armed force,[204] the U.N. Charter must be changed to clearly indicate when a cyber attack would be a use of force. In expanding the U.N. Charter, cyber attacks should be considered an act of force by a state or a non-state actor based on a "consequentiality" approach described in Part IV of this article, regardless of the instrumentality used or the type of actor.[205] This definition would further include damage that cyber attacks can inflict, even with a lack of physical effects. A recent publication from the Department of Defense Office of General Counsel, agrees that the consequences of a cyber attack are extremely important:

> If a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack.[206]

So, if there is a certain level of death and property destruction caused by the cyber attack, this attack should be viewed as an act of force under the U.N. Charter. Regarding property destruction, the threshold should ultimately include the type of traditional physical destruction produced by kinetic force (building collapse, bomb detonations, destruction caused by flooding, etc.), as well as some substantial threshold level of data destruction, to ensure attacks that target and affect a nation's infrastructure (i.e. banking systems, emergency response, and power grids) are covered.

This "consequentiality" approach should also address the type of cyber attacks that lack traditional physical effects. For instance, the U.N. Charter definition of force should include cyber attacks whose consequences are economic and political,

---

[204] *See supra* Part IV.A.

[205] *See supra* Part IV.A.1.

[206] DEP'T. OF DEFENSE, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION SYSTEMS 18 (1999).

instead of applying only in situations where there are foreseeable or intended consequences from the attacks including injury, death, damage, and destruction.[207] Sharon Stevens argues "cyber attacks which result in economic losses or inconvenience to civilians . . . could be used by an enemy country to target certain ethnic groups, gain economic advantage in international trade, or influence international exchange rates."[208] These types of attacks could cause massive destruction, albeit not physical. As a result, attacks similar to the DDoS attacks that briefly shut down Estonia's infrastructure in 2007, as well as those relating to the Russian-Georgian Cyber Conflict, could arguably fall within this category. Furthermore, these types of attacks can be potentially more debilitating than a traditional military attack. Given these guidelines, a cyber attack that only affected free speech would not be included in this definition of force, nor would an attack that only destroyed a small network of electronic data. Consequently, cyber attacks like the Stuxnet worm, which caused minimal property and data destruction, would probably not fall under this proposed expanded definition of the use of force. Lastly, cyber attacks that simply cause confusion among the populace, or amongst the non-state actors' members, would not specifically be covered by the Charter as an act of force. This expanded definition of force would apply equally to state *and* non-state actors.

Targets should also be more clearly defined. For instance, instead of utilizing the term "critical national infrastructure," perhaps the Charter should include a definition of the term "critical infrastructure" so as to ensure that non-state actors are covered, since their infrastructure is not in a sense "national." The definition should include power grids, banking systems, water supply systems, nuclear facilities, etc. Attacks against critical infrastructure would thus be an act of force under Article 2(4) of the U.N. Charter if certain consequences occurred. The term "critical infrastructure" should not only mean the actual physical infrastructure, but also websites or computer systems of these agencies or non-state actors, so as to ensure that potentially vulnerable computer networks are protected.

---

[207] *See* Stevens, *supra* note 20, at 704.

[208] *Id.* at 708.

4. Cyber Attacks in IHL

Since IHL can only govern attacks that rise to the level of an armed conflict as defined in the Geneva Conventions and its Additional Protocols, and since it is questionable whether cyber attacks can ever be governed by existing IHL principles, the definition of armed conflict under IHL needs to be expanded to include cyber attacks involving state and non-state actors. Since the law of armed conflict outlined in IHL mainly focuses on the effects of an armed attack or use of force, or when an attack causes "injury, death, damage, or destruction, or when such consequences are foreseeable,"[209] the definition of armed conflict should be expanded to include cyber attacks between states and non-states that exhibit these type of consequences, as well as political and economic consequences previously discussed. The definition should further include cyber attacks that result in massive property and data destruction in order to include attacks on a nation's central infrastructure. In sum, IHL regarding cyber attacks should give substantial consideration to non-lethal consequences.

IHL should also be expanded to specifically address cyber attacks against non-military objectives which would foreseeably cause non-traditional results. Specifically, Article 48 of Additional Protocol I provides:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[210]

Based on the language of Article 48, IHL would prohibit cyber attacks directed against non-military objectives that are intended to, or would foreseeably, cause injury, death, destruction, or damage.[211] However, an attack aimed against a non-military objective that is not likely to result in these consequences would be permissible.[212] Therefore, an attack involv-

---

[209] Swanson, *supra* note 3, at 316.
[210] Additional Protocol I, *supra* note 139, art. 48.
[211] Swanson, *supra* note 3, at 317.
[212] *Id.*

ing a cyber attack on a nation's power grid, banking or trading systems, or other aspects of infrastructure such as the DDoS attacks involved in the Estonia and Russian-Georgian conflicts would not be covered. Nor would a virus initiated by a non-state actor aimed at these locations be covered. However, as noted earlier, these types of cyber attacks against non-military targets could have non-traditional destructive consequences[213] and should be accounted for in current IHL.

The IHL principles regarding cyber attacks must also address proportionality and unnecessary suffering outlined in Part IV.[214] However, regarding proportionality, under current IHL, specifically Article 51(5)(b)[215] of Additional Protocol I:

> It is difficult to evaluate whether an attack would be proportional according to the relevant categories of "loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof," as the typical direct effects of cyber attacks may be non-lethal or temporary, yet severe.[216]

Consequently, the current language of proportionality needs to be changed in order to expressly give more weight to temporary or non-lethal consequences.[217] For instance, regarding countermeasures, if the United States were attacked by a virus that destroyed massive amounts of data, it would only be able to respond with a similar cyber attack that would cause a proportional amount of destruction; nothing more. This proportionality would also apply if a non-state actor was attacked by a state actor in a similar fashion.

VI. CONCLUSION

Current international laws of war are inadequate, as they do not define or regulate many instances of cyber attacks.

---

[213] *See supra* Part II.C.1-2.

[214] *See supra* Part IV.B.1.

[215] "Among others, the following types of attacks are to be considered as indiscriminate . . . an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated." Additional Protocol I, *supra* note 139, art. 51, para. 5(b).

[216] Hathaway, *supra* note 100, at 851.

[217] *See id.*

They must be changed to include cyber attacks involving state and non-state actors. A new frontier is before us. Gone is the day when nation-states dominated international relations. Gone is the day when kinetic warfare was the only way to cause massive destruction. Cyberspace is the new battlefield, state and non-state entities are the soldiers, and the weapons are computer-generated. "The very technologies that empower us to lead and create also empower those who would disrupt and destroy."[218] Cyber attacks and cyber warfare are here to stay, and if the international community does not regulate this new style of combat, the consequences could be unfathomable.

[218] STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 177, at 2.